Contract Abstract

Contract Information

Contract & Solicitation Title: Various Hosting Application and Products

Contract Summary: CONTRACTOR agrees to provide Acquia hosting and security services for Nashville.gov as well as Salesforce licensing and support for HubNashville, MAC Hope, Metro Clerk's PRR, Finance PRR and HR Benefits CRM system and related products including but not limited to TIBCO, Nintex, FormAssembly, OwnBackup, File Storage and Community Logins. Additionally, CONTRACTOR agrees to provide their entire catalog of then current products and services throughout the term of this contract

Contract Number: 6508243 Solicitation Number: N/A Requisition Number: SS2022034

Replaces Expiring or Expired Contract? (Enter "No" or Contract No and Expiration Date): N/A

Type of Contract/PO: IDIQ Contract **Requires Council Legislation: Yes**

High Risk Contract (Per Finance Department Contract Risk Management Policy): Yes

Sexual Harassment Training Required (per BL2018-1281): Yes

Estimated Start Date: 11/15/2023 Estimated Expiration Date: 11/14/2028 Contract Term: 60 Months

Estimated Contract Life Value: $25,000,000.00 Fund:* 51137 BU:* 14521017

(*Depending on contract terms, actual expenses may hit across various departmental BUs and Funds at PO Levels)

Payment Terms: Net 30 Selection Method: Sole Source

Procurement Staff: Terri Ray BAO Staff: Jeremy Frye

Procuring Department: **Information Technology** Department(s) Served: **Metro Wide**

Prime Contractor Information

Prime Contracting Firm: Carahsoft Technology Corporation ISN#: 17362

Address: 11493 Sunset Hills Road, Suite 100 City: Reston State: VA Zip: 20190

Prime Contractor is a Uncertified/Unapproved: SBE ☐ SDV ☐ MBE ☐ WBE ☐ LGBTBE ☐ (select/check if applicable)

Prime Company Contact: Colby Bender Email Address: contracts@carahsoft.com Phone #: 703-673-3635

Prime Contractor Signatory: Kristina Smith **Email Address:** **contracts@carahsoft.com**

Business Participation for Entire Contract

Small Business and Service Disabled Veteran Business Program: N/A

Amount: N/A Percent, if applicable: N/A

Equal Business Opportunity (EBO) Program: Program Not Applicable

MBE Amount: N/A MBE Percent, if applicable: N/A

WBE Amount: N/A WBE Percent, if applicable: N/A

Federal Disadvantaged Business Enterprise: No

Amount: N/A Percent, if applicable: N/A

Note: Amounts and/or percentages are not exclusive.

B2GNow (Contract Compliance Monitoring): No

Summary of Offer

Offeror Name	MBE	WBE	SBE	SDV	LGBTBE	Score (RFP Only)	Evaluated Cost	Result
	(check as applicable)							
Carahsoft Technology Corp	☐	☐	☐	☐	☐	N/A	N/A	Approved Sole Source Form

Terms and Conditions

1. GOODS AND SERVICES CONTRACT

1.1. Heading

This contract is initiated by and between **The Metropolitan Government of Nashville and Davidson County** (METRO) and **Carahsoft Technology Corporation** (CONTRACTOR) located at **11493 Sunset Hills Road, Suite 100, Reston, VA 20190** resulting from an approved sole source signed by Metro's Purchasing Agent (made a part of this contract by reference**)**. This Contract consists of the following documents:

- ***Any properly executed contract amendment*** *(most recent with first priority),*
- ***This document, including exhibits,***
  - ***Exhibit A - Pricing***
  - ***Exhibit B - MISA Terms and Conditions***
  - ***Exhibit C -Affidavits***
  - ***Exhibit D - Service Agreements***
- ***Purchase Orders (and PO Changes),***

  In the event of conflicting provisions, all documents shall be construed in the order listed above.

2. THE PARTIES HEREBY AGREE TO THE FOLLOWING TERMS AND CONDITIONS:

2.1. Duties and Responsibilities

CONTRACTOR agrees to provide Acquia hosting and security services for Nashville.gov as well as Salesforce licensing and support for HubNashville, MAC Hope, Metro Clerk's PRR, Finance PRR and HR Benefits CRM system and related products including but not limited to TIBCO, Nintex, FormAssembly, OwnBackup, File Storage and Community Logins. Additionally, CONTRACTOR agrees to provide their entire catalog of then current products and services throughout the term of this contract.

2.2. Delivery and/or Installation.

All deliveries (if provided by the performance of this Contract) are F.O.B. Destination, Prepaid by Supplier, Inside Delivery, as defined by METRO.

METRO assumes no liability for any goods delivered without a purchase order. All deliveries shall be made as defined in the solicitation or purchase order and by the date specified on the purchase order.

Installation, if required by the solicitation and/or purchase order shall be completed by the date specified on the purchase order.

3. CONTRACT TERM

3.1. Contract Term

The Contract Term will begin on the date this Contract is approved by all required parties and filed in the Metropolitan Clerk's Office. The Contract Term will end sixty (60) months from the date of filing with the Metropolitan Clerk's Office. This Contract may be extended by letter signed by Metro's Purchasing Agent for up to an additional sixty (60) months. However, in no event shall the term of this Contract exceed one hundred twenty (120) months from the date of filing with the Metropolitan Clerk's Office.

4. COMPENSATION

4.1. Contract Value

This Contract has an estimated value of $25,000,000.00. The pricing details are included in Exhibit A and are made a part of this Contract by reference. CONTRACTOR shall be paid as work is completed and METRO is accordingly, invoiced.

4.2. Other Fees

There will be no other charges or fees for the performance of this Contract. METRO will make reasonable efforts to make payments within 30 days of receipt of invoice but in any event shall make payment within 60 days. METRO will make reasonable efforts to make payments to Small Businesses within 15 days of receipt of invoice but in any event shall make payment within 60 days.

4.3. Payment Methodology

Payment in accordance with the terms and conditions of this Contract shall constitute the entire compensation due CONTRACTOR for all goods and/or services provided under this Contract.

METRO will compensate CONTRACTOR in accordance with Exhibit A of this Contract. Subject to these payment terms and conditions, CONTRACTOR shall be paid for delivered/performed products and/or services properly authorized by METRO in accordance with this Contract. Compensation shall be contingent upon the satisfactory provision of the products and/or services as determined by METRO.

4.4. Escalation/De-escalation

This Contract is not eligible for annual escalation/de-escalation adjustments.

4.5. Electronic Payment

All payments shall be effectuated by ACH (Automated Clearing House).

4.6. Invoicing Requirements

CONTRACTOR shall submit invoices for payment in a format acceptable to METRO and shall submit invoices no more frequently than monthly for satisfactorily and accurately performed services. CONTRACTOR shall be paid as work is completed and invoices are approved by METRO. Invoices shall detail this Contract Number accompanied by any necessary supporting documentation as required by METRO. CONTRACTOR shall submit all invoices no later than ninety (90) days after the services have been delivered/performed.

Payment of an invoice by METRO shall not waive METRO's rights of revocation of acceptance due to non-conformity or the difficulty of discovery of the non-conformance. Such revocation of acceptance shall occur within a reasonable time after METRO discovers or should have discovered the non-conforming product and/or service but prior to any substantial change in condition of the products and/or services caused by METRO.

4.7. Subcontractor/Subconsultant Payments

When payment is received from METRO, CONTRACTOR shall within fourteen (14) calendar days pay all subcontractors, subconsultants, laborers, and suppliers the amounts they are due for the work covered by such payment. In the event METRO becomes informed that CONTRACTOR has not paid a subcontractor, subconsultant, laborer, or supplier as provided herein, METRO shall have the right, but not the duty, to issue future checks and payments to CONTRACTOR of amounts otherwise due hereunder naming CONTRACTOR and any such subcontractor, subconsultant, laborer, or supplier as joint payees. Such joint check procedure, if employed by METRO, shall create no rights in favor of any person or entity beyond the right of the named payees to payment of the check and shall not be deemed to commit METRO to repeat the procedure in the future. If persistent, this may be determined to be a material breach of this Contract.

5. TERMINATION

5.1. Breach

Should CONTRACTOR fail to fulfill in a timely and proper manner its obligations under this Contract or if it should violate any of the terms of this Contract, METRO shall identify the breach and CONTRACTOR shall cure the performance within thirty (30) days. If CONTRACTOR fails to satisfactorily provide cure, METRO shall have the right to immediately terminate this Contract. Such termination shall not relieve CONTRACTOR of any liability to METRO for damages sustained by virtue of any breach by CONTRACTOR.

5.2. Lack of Funding

Should funding for this Contract be discontinued, METRO shall have the right to terminate this Contract immediately upon written notice to CONTRACTOR.

5.3. Notice

METRO may terminate this Contract at any time upon thirty (30) days written notice to CONTRACTOR. Should METRO terminate this Contract, CONTRACTOR shall immediately cease work and deliver to METRO, within thirty (30) days, all completed or partially completed satisfactory work, and METRO shall determine and pay to CONTRACTOR the amount due for satisfactory work.

6. NONDISCRIMINATION

6.1. METRO's Nondiscrimination Policy

It is the policy of METRO not to discriminate on the basis of race, creed, color, national origin, age, sex, or disability in its hiring and employment practices, or in admission to, access to, or operation of its programs, services, and activities.

6.2. Nondiscrimination Requirement

No person shall be excluded from participation in, be denied benefits of, be discriminated against in the admission or access to, or be discriminated against in treatment or employment in METRO's contracted programs or activities, on the grounds of race, creed, color, national origin, age, sex, disability, or any other classification protected by federal or Tennessee State Constitutional or statutory law; nor shall they be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of contracts with METRO or in the employment practices of METRO's CONTRACTORs. **CONTRACTOR certifies and warrants that it will comply with this nondiscrimination requirement**. Accordingly, all offerors entering into contracts with METRO shall, upon request, be required to show proof of such nondiscrimination and to post in conspicuous places that are available to all employees and applicants, notices of nondiscrimination.

6.3. Equal Business Opportunity (EBO) Program Requirement

The Equal Business Opportunity (EBO) Program is not applicable to this Contract.

6.4. Covenant of Nondiscrimination

All offerors have committed to the Covenant of Nondiscrimination when registering with METRO to do business. To review this document, go to METRO's website.

6.5. Americans with Disabilities Act (ADA)

CONTRACTOR assures METRO that all services provided shall be completed in full compliance with the Americans with Disabilities Act ('ADA') 2010 ADA Standards for Accessible Design, enacted by law March 15, 2012, as has been adopted by METRO. CONTRACTOR will ensure that participants with disabilities will have communication access that is equally effective as that provided to people without disabilities. Information shall be made available in accessible formats, and auxiliary aids and services shall be provided upon the reasonable request of a qualified person with a disability.

7. INSURANCE

7.1. Proof of Insurance

During the term of this Contract, for any and all awards, CONTRACTOR shall, at its sole expense, obtain and maintain in full force and effect for the duration of this Contract, including any extension(s), the types and amounts of insurance identified below. Proof of insurance shall be required naming METRO as additional insured and identifying Contract number on the ACORD document.

7.2. Automobile Liability Insurance
In the amount of one million ($1,000,000.00) dollars.

7.3. General Liability Insurance
In the amount of one million ($1,000,000.00) dollars.

7.4. Worker's Compensation Insurance (if applicable)
CONTRACTOR shall maintain workers' compensation insurance with statutory limits required by the State of Tennessee or other applicable laws and Employer's Liability Insurance with limits of no less than one hundred thousand ($100,000.00) dollars, as required by the laws of Tennessee.

7.5. Technological Errors and Omissions, including Cyber Liability, Insurance
Technological Errors and Omissions Insurance in the amount of one million ($1,000,000.00) dollars and Cyber Liability Insurance in the amount of four million ($4,000,000.00) dollars for a combined limit of five million ($5,000,000) dollars.

7.6. Such insurance shall:

Contain or be endorsed to contain a provision that includes METRO, its officials, officers, employees, and volunteers as additional insureds with respect to liability arising out of work or operations performed by or on behalf of CONTRACTOR including materials, parts, or equipment furnished in connection with such work or operations. The coverage shall contain no special limitations on the scope of its protection afforded to the above-listed insureds.

For any claims related to this Contract, CONTRACTOR's insurance coverage shall be primary insurance with respects to METRO, its officers, officials, employees, and volunteers. Any insurance or self-insurance programs covering METRO, its officials, officers, employees, and volunteers shall be in excess of CONTRACTOR's insurance and shall ot contribute with it.

Automotive Liability insurance shall include vehicles owned, hired, and/or non-owned. Said insurance shall include coverage for loading and unloading hazards. Insurance shall contain or be endorsed to contain a provision that includes METRO, its officials, officers, employees, and volunteers as additional insureds with respect to liability arising out of automobiles owned, leased, hired, or borrowed by or on behalf of CONTRACTOR.

CONTRACTOR shall maintain Workers' Compensation insurance (if applicable) with statutory limits as required by the State of Tennessee or other applicable laws and Employers' Liability insurance. CONTRACTOR shall require each of its subcontractors to provide Workers' Compensation for all of the latter's employees to be engaged in such work unless such employees are covered by CONTRACTOR's Workers' Compensation insurance coverage.

7.7. Other Insurance Requirements

Prior to commencement of services, CONTRACTOR shall furnish METRO with original certificates and amendatory endorsements effecting coverage required by this section and provide that such insurance shall not be cancelled, allowed to expire, or be materially reduced in coverage except on 30 days' prior written notice to:

PROCUREMENTCOI@NASHVILLE.GOV (preferred method) OR
DEPARTMENT OF FINANCE
PROCUREMENT DIVISION
730 2ND AVE SOUTH, STE 101
P.O. BOX 196300
NASHVILLE, TN 37219-6300

Provide certified copies of endorsements and policies if requested by METRO in lieu of or in addition to certificates of insurance.

Replace certificates, policies, and/or endorsements for any such insurance expiring prior to completion of services.

Maintain such insurance from the time services commence until services are completed. Failure to maintain or renew coverage and to provide evidence of renewal may be treated by METRO as a material breach of this Contract.

Said insurance shall be with an insurer licensed to do business in Tennessee and having A.M. Best Company ratings of no less than A-. Modification of this standard may be considered upon appeal to the METRO Director of Risk Management Services.

Require all subcontractors to maintain during the term of this Contract, Commercial General Liability insurance, Business Automobile Liability insurance, and Worker's Compensation/ Employers Liability insurance (unless subcontractor's employees are covered by CONTRACTOR's insurance) in the same manner as specified for CONTRACTOR. CONTRACTOR shall require subcontractor's to have all necessary insurance and maintain the subcontractor's certificates of insurance.

Any deductibles and/or self-insured retentions greater than $10,000.00 must be disclosed to and approved by METRO **prior to the commencement of services.**

If CONTRACTOR has or obtains primary and excess policy(ies), there shall be no gap between the limits of the primary policy and the deductible features of the excess policies.

8. GENERAL TERMS AND CONDITONS

8.1. Taxes

METRO shall not be responsible for any taxes that are imposed on CONTRACTOR. Furthermore, CONTRACTOR understands that it cannot claim exemption from taxes by virtue of any exemption that is provided to METRO.

8.2. Warranty

CONTRACTOR warrants that for a period of one year from date of delivery and/or installation, whichever is later, the goods provided, including software, shall be free of any defects that interfere with or prohibit the use of the goods for the purposes for which they were obtained.

During the warranty period, METRO may, at its option, request that CONTRACTOR repair or replace any defective goods, by written notice to CONTRACTOR. In that event, CONTRACTOR shall repair or replace the defective goods, as required by METRO, at CONTRACTOR's expense, within thirty (30) days of written notice.
Alternatively, METRO may return the defective goods, at CONTRACTOR's expense, for a full refund. Exercise of either option shall not relieve CONTRACTOR of any liability to METRO for damages sustained by virtue of CONTRACTOR's breach of warranty.

8.3. Software License

CONTRACTOR warrants and represents that it is the owner of or otherwise has the right to and does hereby grant METRO a license to use any software provided for the purposes for which the software was obtained or proprietary material set forth in METRO's solicitation and/or CONTRACTOR's response to the solicitation.

8.4. Confidentiality

Tennessee Code Annotated § 10-7-504(i) specifies that information which would allow a person to obtain unauthorized access to confidential information or to government property shall be maintained as confidential. "Government property" includes electronic information processing systems, telecommunication systems, or other communications systems of a governmental entity subject to this chapter. Such records include: (A) Plans, security codes, passwords, combinations, or computer programs used to protect electronic information and government property; (B) Information that would identify those areas of structural or operational vulnerability that would permit unlawful disruption to, or interference with, the services provided by a governmental entity; and (C) Information that could be used to disrupt, interfere with, or gain unauthorized access to electronic information or government property.

The foregoing listing is not intended to be comprehensive, and any information which METRO marks or otherwise designates as anything other than "Public Information" will be deemed and treated as sensitive information, which is defined as any information not specifically labeled as "Public Information". Information which qualifies as "sensitive information" may be presented in oral, written, graphic, and/or machine-readable formats. Regardless of presentation format, such information will be deemed and treated as sensitive information.

CONTRACTOR, and its Agents, for METRO, may have access to sensitive information. CONTRACTOR, and its Agents, are required to maintain such information in a manner appropriate to its level of sensitivity. All sensitive information must be secured at all times including, but not limited to, the secured destruction of any written or electronic information no longer needed. The unauthorized access, modification, deletion, or disclosure of any METRO information may compromise the integrity and security of METRO, violate individual rights of privacy, and/or constitute a criminal act.

Upon the request of METRO, CONTRACTOR shall return all information in whatever form in a format chosen by METRO. In the event of any disclosure or threatened disclosure of METRO information, METRO is further authorized and entitled to immediately seek and obtain injunctive or other similar relief against CONTRACTOR, including but not limited to emergency and ex parte relief where available.

8.5. Information Ownership

All METRO information is and shall be the sole property of METRO. CONTRACTOR hereby waives any and all statutory and common law liens it may now or hereafter have with respect to METRO information. Nothing in this Contract or any other agreement between METRO and CONTRACTOR shall operate as an obstacle to such METRO's right to retrieve any and all METRO information from CONTRACTOR or its agents or to retrieve such information or place such information with a third party for provision of services to METRO, including without limitation, any outstanding payments, overdue payments and/or disputes, pending legal action, or arbitration. Upon METRO's request,

CONTRACTOR shall supply METRO with an inventory of METRO information that CONTRACTOR stores and/or backs up.

Any information provided to the CONTRACTOR, including information provided by METRO customers or citizens, is only to be used to fulfill the contracted services. Any additional information that is inferred or determined based on primary information that is provided to the CONTRACTOR, i.e. "second-order data", is only to be used to fulfill the contracted services. This information is not to be used for marketing or commercial purposes and the CONTRACTOR asserts no rights to this information outside of fulfilling the contracted services. Storage of this information is not allowed outside United States' jurisdiction.

8.6. Information Security Breach Notification

In addition to the notification requirements in any Business Associate Agreement with METRO, when applicable, CONTRACTOR shall notify METRO of any data breach within 24 hours of CONTRACTOR's knowledge or reasonable belief (whichever is earlier) that such breach has occurred (Breach Notice) by contacting the METRO ITS Help Desk. The Breach Notice should describe the nature of the breach, the scope of the information compromised, the date the breach occurred, and the identities of the individuals affected or potentially affected by the breach as well as specific information about the data compromised so that METRO can properly notify those individuals whose information was compromised. CONTRACTOR shall periodically update the information contained in the Breach Notice to METRO and reasonably cooperate with METRO in connection with METRO's efforts to mitigate the damage or harm of such breach.

8.7. Virus Representation and Warranty

CONTRACTOR represents and warrants that Products and/or Services, or any media upon which the Products and/or Services are stored, to the CONTRACTOR’s knowledge, do not have, nor shall CONTRACTOR or its Agents otherwise introduce into METRO's systems, network, or infrastructure, any type of software routines or element which is designed to or capable of unauthorized access to or intrusion upon, disabling, deactivating, deleting, or otherwise damaging or interfering with any system, equipment, software, data, or the METRO network. In the event of a breach of this representation and warranty, CONTRACTOR shall compensate METRO for any and all harm, injury, damages, costs, and expenses incurred by METRO resulting from the breach.

For CONTRACTOR managed systems, CONTRACTOR shall install and maintain ICSA Labs certified or AV-Test approved Antivirus Software and, to the extent possible, use real time protection features. CONTRACTOR shall maintain the Anti-virus Software in accordance with the Antivirus Software provider's recommended practices. In addition, CONTRACTOR shall ensure that:

- Anti-virus Software checks for new Anti-virus signatures no less than once per day, and;
- Anti-virus signatures are current and no less recent than two versions/releases behind the most current version/release of the Anti-virus signatures for the Anti-virus Software.

8.8. Copyright, Trademark, Service Mark, or Patent Infringement

CONTRACTOR shall, at its own expense, be entitled to and shall have the duty to defend any suit that may be brought against METRO to the extent that it is based on a claim that the products or services furnished infringe a Copyright, Trademark, Service Mark, or Patent. CONTRACTOR shall further indemnify and hold harmless METRO against any award of damages and costs made against METRO by a final judgment of a court of last resort in any such suit. METRO shall provide CONTRACTOR immediate notice in writing of the existence of such claim and full right and opportunity to conduct the defense thereof, together with all available information and reasonable cooperation, assistance and authority to enable CONTRACTOR to do so. No costs or expenses shall be incurred for the account of CONTRACTOR without its written consent. METRO reserves the right to participate in the defense of any such action. CONTRACTOR shall have the right to enter into negotiations for and the right to effect settlement or compromise of any such action, but no such settlement or compromise shall be binding upon METRO unless approved by the METRO Department of Law Settlement Committee and, where required, the METRO Council.

If the products or services furnished under this Contract are likely to, or do become, the subject of such a claim of infringement, then without diminishing CONTRACTOR's obligation to satisfy the final award, CONTRACTOR may at its option and expense:

- Procure for METRO the right to continue using the products or services
- Replace or modify the alleged infringing products or services with other equally suitable products or services that are satisfactory to METRO, so that they become non-infringing
- Remove the products or discontinue the services and cancel any future charges pertaining thereto Provided; however, that CONTRACTOR will not exercise the Remove option above until CONTRACTOR and METRO have determined that the Procure and/or Replace options are impractical. CONTRACTOR shall have no liability to METRO; however, if any such infringement or claim thereof is based upon or arises out of:

- The use of the products or services in combination with apparatus or devices not supplied or else approved by CONTRACTOR;
- The use of the products or services in a manner for which the products or services were neither designated nor contemplated; or,
- The claimed infringement in which METRO has any direct or indirect interest by license or otherwise, separate from that granted herein.

8.9. Maintenance of Records

CONTRACTOR shall maintain documentation for all charges against METRO. The books, records, and documents of CONTRACTOR, insofar as they relate to work performed or money received under this Contract, shall be maintained for a period of three (3) full years from the date of final payment and will be subject to audit, at any reasonable time and upon reasonable notice by METRO or its duly appointed representatives. The records shall be maintained in accordance with generally accepted accounting principles. In the event of litigation, working papers and other documents shall be produced in accordance with applicable laws and/or rules of discovery. Breach of the provisions of this paragraph is a material breach of this Contract.

All documents and supporting materials related in any manner whatsoever to this Contract or any designated portion thereof, which are in the possession of CONTRACTOR or any subcontractor or subconsultant shall be made available to METRO for inspection and copying upon written request from METRO. Said documents shall also be made available for inspection and/or copying by any state, federal or other regulatory authority, upon request from METRO. Said records include, but are not limited to, all drawings, plans, specifications, submittals, correspondence, minutes, memoranda, tape recordings, videos, or other writings or things which document the procurement and/or performance of this Contract. Said records expressly include those documents reflecting the cost, including all subcontractors' records and payroll records of CONTRACTOR and subcontractors.

8.10. Monitoring

CONTRACTOR's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by METRO, the Department of Finance, the Division of Internal Audit, or their duly appointed representatives.

METRO shall have the option of reviewing and performing a security assessment of the information security management practices of CONTRACTOR. METRO shall have the right, at its expense, during normal business hours and with reasonable advance notice, to evaluate, test, and review at CONTRACTOR's premises the Products and/or Services to ensure compliance with the terms and conditions of this Contract. METRO shall have the right to conduct such audits by use of its own employees and internal audit staff, or by use of outside consultants and auditors.

8.11. METRO Property

Any METRO property, including but not limited to books, records, and equipment that is in CONTRACTOR's possession shall be maintained by CONTRACTOR in good condition and repair, and shall be returned to METRO by CONTRACTOR upon termination of this Contract. All goods, documents, records, and other work product and property produced during the performance of this Contract are deemed to be METRO property. METRO property

includes, but is not limited to, all documents which make up this Contract; all other documents furnished by METRO; all goods, records, reports, information , data, specifications, computer programs, technical reports, operating manuals and similar work or other documents, conceptual drawings, design documents, closeout documents, and other submittals by CONTRACTOR of any of its subcontractors; and, all other original works of authorship, whether created by METRO, CONTRACTOR or any of its subcontractors embodied in any tangible medium of expression, including, without limitation, pictorial, graphic, sculptural works, two (2) dimensional works, and three (3) dimensional works. Any of Contractor's or its subcontractors' works of authorship comprised within the Work Product (whether created alone or in concert with Metro or a third party) shall be deemed to be "works made for hire" and made in the course of services rendered and, whether pursuant to the provisions of Section 101 of the U.S. Copyright Act or other Applicable Law, such Work Product shall belong exclusively to Metro. Contractor and its subcontractors grant Metro a non-exclusive, perpetual, worldwide, fully paid up, royalty- free license, with rights to sublicense through multiple levels of sublicenses, to reproduce, make, have made, create derivative works of, distribute, publicly perform and publicly display by all means, now known or later developed, such rights.

Except as to Contracts involving sensitive information, CONTRACTOR may keep one (1) copy of the aforementioned documents upon completion of this Contract; provided, however, that in no event shall CONTRACTOR use, or permit to be used, any portion of the documents on other projects without METRO's prior written authorization. CONTRACTOR shall maintain sensitive information securely and if required by METRO, provide secured destruction of said information. Distribution and/or reproduction of METRO sensitive information outside of the intended and approved use are strictly prohibited unless permission in writing is first received from the METRO Chief Information Security Officer. The storage of METRO sensitive information to third-party hosted network storage areas, such as Microsoft Skydrive, Google Docs, Dropbox, or other cloud storage mechanisms, shall not be allowed without first receiving permission in writing from the METRO Chief Information Security Officer.

8.12. Modification of Contract

This Contract may be modified only by written amendment executed by all parties and their signatories hereto. All change orders, where required, shall be executed in conformance with section 4.24.020 of the Metropolitan Code of Laws. Should the Parties enter into Purchase Orders for parts and/or services that include accompanying service agreements, the Parties shall negotiate the terms of the those accompanying service agreements, which terms shall be approved by the Purchasing Agent, and incorporated herein.

8.13. Partnership/Joint Venture

This Contract shall not in any way be construed or intended to create a partnership or joint venture between the Parties or to create the relationship of principal and agent between or among any of the Parties. None of the Parties hereto shall hold itself out in a manner contrary to the terms of this paragraph. No Party shall become liable for any representation, act, or omission of any other Party contrary to the terms of this Contract.

8.14. Waiver

No waiver of any provision of this Contract shall affect the right of any Party to enforce such provision or to exercise any right or remedy available to it.

8.15. Employment

CONTRACTOR shall not subscribe to any personnel policy which permits or allows for the promotion, demotion, employment, dismissal or laying off of any individual due to race, creed, color, national origin, age, sex, or which is in violation of applicable laws concerning the employment of individuals with disabilities.

CONTRACTOR shall not knowingly employ, permit, dispatch, subcontract, or instruct any person who is an undocumented and/or unlawful worker to perform work in whole or part under the terms of this Contract.

Violation of either of these contract provisions may result in suspension or debarment if not resolved in a timely manner, not to exceed ninety (90) days, to the satisfaction of METRO.

8.16. Compliance with Laws

CONTRACTOR agrees to comply with all applicable federal, state and local laws and regulations.

8.17. Iran Divestment Act

In accordance with the Iran Divestment Act, Tennessee Code Annotated § 12-12-101 et seq., CONTRACTOR certifies that to the best of its knowledge and belief, neither CONTRACTOR nor any of its subcontractors are on the list created pursuant to Tennessee Code Annotated § 12-12-106. Misrepresentation may result in civil and criminal sanctions, including contract termination, debarment, or suspension from being a contractor or subcontractor under METRO contracts.

8.18. Israel Anti-Boycott Act

In accordance with Tennessee Code Annotated Title 12, Chapter 4, Part 1 CONTRACTOR certifies that CONTRACTOR is not currently engaged in, and will not for the duration of this Contract engage in, a boycott of Israel.

8.19. Taxes and Licensure

CONTRACTOR shall have all applicable licenses and be current on its payment of all applicable gross receipt taxes and personal property taxes.

8.20. Ethical Standards

It shall be a breach of the Ethics in Public Contracting standards in the Metropolitan Code of Laws for any person to offer, give or agree to give any employee or former employee, or for any employee or former employee to solicit, demand, accept or agree to accept from another person, a gratuity or an offer of employment in connection with any decision, approval, disapproval, recommendation, preparation of any part of a program requirement or a purchase request, influencing the content of any specification or procurement standard, rendering of advice, investigation, auditing or in any other advisory capacity in any proceeding or application, request for ruling, determination, claim or controversy or other particular matter, pertaining to any program requirement of a contract or subcontract or to any solicitation or proposal therefore. It shall be a breach of the Ethics in Public Contracting standards for any payment, gratuity or offer of employment to be made by or on behalf of a subcontractor under a contract to the prime contractor or higher tier subcontractor or a person associated therewith, as an inducement for the award of a subcontract or order. Breach of the provisions of this paragraph is, in addition to a breach of this contract, a breach of ethical and legal standards which may result in civil or criminal sanction and/or debarment or suspension from being a contractor or subcontractor under METRO contracts.

Pursuant to Metropolitan Code of Laws, Section 4.48.020, entities and persons doing business with, or proposing to do business with, the Metropolitan Government of Nashville & Davidson County must adhere to the ethical standards prescribed in Section 4.48 of the Code. By signing this contract, you agree that you have read the standards in Section 4.48 and understand that you are obligated to follow them. Violation of any of those standards is a breach of contract and a breach of legal standards that may result in sanctions, including those set out in Section 4.48

8.21. Indemnification and Hold Harmless

CONTRACTOR shall indemnify and hold harmless METRO, its officers, agents, and employees from:

A. Any claims, damages, costs, and attorney fees for injuries or damages arising, in part or in whole, from the negligent or intentional acts or omissions of CONTRACTOR, its officers, employees, and/or agents, including its sub or independent contractors, in connection with the performance of the contract.

B. Any claims, damages, penalties, costs, and attorney fees arising from any failure of CONTRACTOR, its officers, employees, and/or agents, including its sub or independent contractors, to observe applicable laws, including, but not limited to, labor laws and minimum wage laws.

C. In any and all claims against METRO, its officers, agents, or employees, by any employee of CONTRACTOR, any

subcontractor, anyone directly or indirectly employed by any of them, or anyone for whose acts any of them may be liable, the indemnification obligation shall not be limited in any way by any limitation on the amount or type of damages, compensation, or benefits payable by or for CONTRACTOR or any subcontractor under workers' compensation acts, disability acts, or other employee benefit acts.

D. METRO will not indemnify, defend, or hold harmless in any fashion CONTRACTOR from any claims arising from any failure, regardless of any language in any attachment or other document that CONTRACTOR may provide.

E. CONTRACTOR shall pay METRO any expenses incurred as a result of CONTRACTOR's failure to fulfill any obligation in a professional and timely manner under this Contract.

8.22. Attorney Fees

CONTRACTOR agrees that in the event either party takes legal action to enforce any provision of this Contract or to obtain a remedy for any breach of this Contract, and in the event METRO prevails in such action, CONTRACTOR shall pay all expenses of such action incurred at any and all stages of the litigation, including costs, and reasonable attorney fees for METRO.

8.23. Assignment--Consent Required

The provisions of this Contract shall inure to the benefit of and shall be binding upon the respective successors and assignees of the parties hereto. Except for the rights of money due to CONTRACTOR under this Contract, neither this Contract nor any of the rights and obligations of CONTRACTOR hereunder shall be assigned or transferred in whole or in part without the prior written consent of METRO. Any such assignment or transfer shall not release CONTRACTOR from its obligations hereunder.

NOTICE OF ASSIGNMENT OF ANY RIGHTS TO MONEY DUE TO CONTRACTOR UNDER THIS CONTRACT MUST BE SENT TO THE ATTENTION OF:

PRG@NASHVILLE.GOV (preferred method) OR
METRO PURCHASING AGENT
DEPARTMENT OF FINANCE
PROCUREMENT DIVISION
730 2ND AVENUE SOUTH
PO BOX 196300
NASHVILLE, TN 37219-6300

Funds Assignment Requests should contain complete contact information (contact person, organization name, address, telephone number, and email) for METRO to use to request any follow up information needed to complete or investigate the requested funds assignment. To the extent permitted by law, METRO has the discretion to approve or deny a Funds Assignment Request.

8.24. Entire Contract

This Contract sets forth the entire agreement between the parties with respect to the subject matter hereof and shall govern the respective duties and obligations of the parties.

8.25. Force Majeure

No party shall have any liability to the other hereunder by reason of any delay or failure to perform any obligation or covenant if the delay or failure to perform is occasioned by *force majeure*, meaning any act of God, storm, fire, casualty, unanticipated work stoppage, strike, lockout, labor dispute, civil disturbance, riot, war, national emergency, act of Government, act of public enemy, or other cause of similar or dissimilar nature beyond its control.

8.26. Governing Law

The validity, construction, and effect of this Contract and any and all extensions and/or modifications thereof shall be governed by the laws of the State of Tennessee. Tennessee law shall govern regardless of any language in any attachment or other document that CONTRACTOR may provide.

8.27. Venue

Any action between the Parties arising from this Contract shall be maintained in the courts of Davidson County, Tennessee.

8.28. Severability

Should any provision of this Contract be declared to be invalid by any court of competent jurisdiction, such provision shall be severed and shall not affect the validity of the remaining provisions of this Contract.

[BALANCE OF PAGE IS INTENTIONALLY LEFT BLANK]

Contract Number: 6508243

Notices and Designation of Agent for Service of Process

All notices to METRO shall be mailed or hand delivered to:

PURCHASING AGENT

PROCUREMENT DIVISION

DEPARTMENT OF FINANCE

PO BOX 196300

NASHVILLE, TN 37219-6300

Notices to CONTRACTOR shall be mailed or hand delivered to:

CONTRACTOR: Carahsoft Technology Corporation

Attention: Colby Bender

Address: 11493 Sunset Hills Road, Suite 100, Reston, VA 20190

Telephone: 703-673-3635

Fax: N/A

E-mail: contracts@carahsoft.com

CONTRACTOR designates the following as the CONTRACTOR's agent for service of process and will waive any objection to service of process if process is served upon this agent:

Designated Agent: BUSINESS FILINGS INCORPORATED

Attention: N/A

Address: 800 S GAY ST, STE 2021, KNOXVILLE, TN 37929-9710 USA

Email: N/A

[SPACE INTENTIONALLY LEFT BLANK]

Notices & Designations
Department & Project Manager

Contract Number	6508243

The primary DEPARTMENT/AGENCY responsible for the administration of this contract is:

DEPARTMENT	Information Technology Services
Attention	Dawn Clark
Address	700 President Ronald Reagan Way - Suite 301
Telephone	615-862-6033
Email	dawn.clark@nashville.gov

The primary DEPARTMENT/AGENCY responsible for the administration of this contract designates the following individual as the PROJECT MANAGER responsible for the duties outlined in APPENDIX – Z CONTRACT ADMINISTRATION:

Project Manager	Dawn Clark
Title	IS Assistant Director
Address	700 President Ronald Reagan Way - Suite 301
Telephone	615-862-6033
Email	dawn.clark@nashville.gov

Appendix Z – Contract Administration

Upon filing with the Metropolitan Clerk, the PROJECT MANAGER designated by the primary DEPARTMENT/AGENCY is responsible for contract administration. Duties related to contract administration include, but are not necessarily limited to, the following:

Vendor Performance Management Plan
For contracts in excess of $50,000.00, the project manager will develop a vendor performance management plan. This plan is managed by the primary department/agency and will be retained by the department/agency for their records. At contract close out, copies of all vendor performance management documents will be sent to PRG@nashville.gov.

For best practices related to vendor performance management, project managers will consult chapter eight of the PROCUREMENT MANUAL found on the division of purchases internal resources page: https://metronashville.sharepoint.com/sites/IMFinanceProcurement.

Amendment
For all contracts, the project manager will notify PRG@nashville.gov if changes to the term, value, scope, conditions, or any other material aspect of the contract are required. The email notification will include a complete CONTRACT AMENDMENT REQUEST FORM found on the division of purchases internal resources page: https://metronashville.sharepoint.com/sites/IMFinanceProcurement.

Escalation
For contracts that include an escalation/de-escalation clause, the project manager will notify PRG@nashville.gov when any request for escalation/de-escalation is received. The email notification will include any documentation required by the contract to support the request.

Contract Close Out – Purchasing
For all contracts, the project manager will notify PRG@nashville.gov when the work is complete and has been accepted by the department/agency. The email notification will include the contract number, contract title, date of completion, warranty start date and warranty end date (if applicable), and copies of all vendor performance management documents (if applicable).

Contract Close Out – BAO
For contracts with compliance monitored by the Business Assistance Office (BAO), the project manager will notify the designated contract compliance officer via email when the contract is complete and final payment has been issued. The email notification will include the contract number, contract title, and the date final payment was issued.

Best Practices
Project managers are strongly encouraged to consult chapter eight of the PROCUREMENT MANUAL for best practices related to contract administration. The manual is found on the division of purchases internal resources page:
https://metronashville.sharepoint.com/sites/IMFinanceProcurement

Contract Number 6508243

Effective Date

This contract shall not be binding upon the parties until it has been fully electronically approved by the CONTRACTOR, the authorized representatives of the Metropolitan Government, and filed in the office of the Metropolitan Clerk.

THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

APPROVED AS TO PROJECT SCOPE:

Dept. / Agency / Comm. Head or Board Chair. | Dept. Fin.

APPROVED AS TO COMPLIANCE WITH PROCUREMENT CODE:

Michelle A. Hernandez Lane | Purchasing

Purchasing Agent

APPROVED AS TO AVAILABILITY OF FUNDS:

Kevin Crumbo/mjw | EJ

Director of Finance | BA

APPROVED AS TO FORM AND LEGALITY:

Tara Ladd | BC

Metropolitan Attorney | Insurance

FILED BY THE METROPOLITAN CLERK:

Metropolitan Clerk | Date

CONTRACTOR:

Carahsoft Technology Corp.

Company Name

Colby Bender

Signature of Company's Contracting Officer

Colby Bender

Officer's Name

Contracts Team Lead

Officer's Title

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
1Kosmos	0.24%
3CLogic	0.40%
443 Technologies	0.25%
7SIGNAL Solutions, Inc	0.50%
ABBYY USA Software House, Inc.	0.24%
Abnormal Security	0.25%
Acalvio Technologies	0.50%
Accela, Inc.	0.24%
Accuvant Inc.	0.25%
AchieveIt Online, LLC	0.50%
Acis Tek Corporation	0.25%
Aclima	0.25%
Acquia	2.00%
Adaptus, LLC	0.50%
ADF Solutions	0.25%
Adlumin	0.25%
Adobe	2.00%
Advologix	0.50%
AECOM	0.25%
AeroCloud Systems	0.50%
Agate Software	0.50%
Agilet Solutions	0.25%
Aisera	0.25%
Akamai	2.00%
AkitaBox	1.20%
AlertEnterprise	0.25%
Alfresco	0.25%
ALTR Solutions Inc	0.50%
Amazon Web Services	2.00%
AMIICUSS LLC	0.25%
amp Tech	0.25%
AmpliFund	0.25%
Anaconda	0.25%
Anaplan	2.00%
Anjuna	0.25%
APIsec.ai	2.00%
AppBuddy	0.50%
Appian Corporation	0.25%
Appinium	0.50%
Applied Frameworks	0.25%
AppOmni	0.25%
Aquera	0.50%
Arbola, Inc.	10.00%
archTIS	0.24%
Arctic Wolf	2.00%
Ardoq, Inc	0.25%
Area 1 Security	0.50%
ARInspect	0.25%
Arista	1.00%
Armis, Inc.	0.25%
Armored Things	0.50%
ArmorText	0.50%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Arria NLG (USA) Inc	0.25%
ASG Technologies	0.25%
Asite	2.00%
AspireHR	0.25%
AssetOptics	2.00%
Assima	2.00%
Assured Data Protection, Inc.	0.25%
Astronomer	0.25%
Attestiv	0.50%
Attivo Networks, Inc.	1.00%
Authenticiti	0.50%
Automated Office Solutions	0.24%
Automize A/S	0.25%
Automox, Inc.	2.00%
AutoRABIT	2.00%
AutoReturn	0.25%
Avaap USA LLC	0.25%
Avela, Inc	0.25%
AvePoint Public Sector, Inc.	2.00%
Aviatrix	0.25%
Avisare	0.25%
Babel Street	0.25%
Backblaze	0.25%
Bamboo Health	0.25%
Bay-InfoTech	0.25%
BEINCOURT	0.25%
Benefitfocus.com, Inc.	0.25%
Bento Biology Platforms	0.25%
BetterUp	0.25%
Big Compass	0.25%
BigID	0.50%
Binti	0.50%
Blackthorn.io, Inc.	0.50%
Blancco Technology Group	0.67%
Blocksi, Inc	0.25%
Blue Fusion Technologies	0.25%
Bluescape Software	0.25%
BlueVector	1.00%
Blyncsy, Inc.	1.96%
Bonfire	0.50%
Bonterra Tech	0.24%
Boomi	1.00%
Box, Inc.	0.25%
Brainstorm	0.50%
Bravium Consulting Inc.	2.00%
Brazen Technologies, Inc.	0.25%
Bromium	0.25%
Buurst, Inc.	0.24%
Byos	0.25%
C2 Labs Inc.	0.50%
CA Technologies	2.00%
Callinize, INc. dba Tenfold	0.25%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
CalypsoAI Corp.	0.50%
Campus Kaizen	0.25%
Canto	2.00%
Carahsoft	1.00%
Cardinal Path LLC	1.00%
CareAR	1.00%
Casebook PBC	2.00%
Casepoint	0.25%
Catch Intelligence	2.00%
CBI Secure	0.24%
Cellebrite	2.00%
Celonis	2.00%
CelWell Services	2.00%
Center for Internet Security	0.25%
Centrics IT	0.25%
CEPTES Software	0.22%
Cerna Solutions	0.50%
Certificial	2.00%
Certus Group	0.25%
Chainalysis	2.00%
Change and Innovation Agency	0.50%
Check Point Software Technologies	0.25%
Checkpoint Services Inc.	0.25%
Chooch Intelligence Technologies Co.	0.25%
Chorus Intelligence	0.25%
Chronicle	0.25%
Citibot	0.50%
Citrix	2.00%
City Innovate	1.00%
Clarifai	0.50%
Clariti Cloud, Inc.	2.00%
Claroty	0.25%
Class Technologies, Inc	2.00%
Clear Skye	0.50%
Cloud Academy, Inc.	0.50%
Cloud SynApps Inc.	0.24%
Cloud Warriors	1.88%
CloudBees, Inc.	0.50%
Cloudbolt	2.00%
CloudCover	2.50%
Cloudera Government Solutions Inc.	0.50%
Cloudnomics	0.25%
cloudPWR	0.50%
CloudSaver	2.00%
CMA Technology Solutions	0.25%
Cobwebs	0.25%
CodeLock	0.25%
Codescience, Inc.	0.50%
Codoxo	0.25%
CogAbility, Inc.	0.25%
Cohesity, Inc.	0.25%
Collibra Inc	0.50%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
CommunityCX	0.25%
Commvault	2.00%
CompassCom	0.93%
CompuNet Inc.	0.25%
Conga	0.25%
Connecting Point	2.00%
Connecting Software	2.00%
Contraforce	0.47%
Conveyal LLC	0.25%
Copado	2.00%
CORAScloud	0.50%
Corellium, Inc.	0.25%
CoreView USA	2.00%
Cornea	0.25%
Cosi Consulting	3.00%
CounterCraft	0.25%
Crave.io	0.25%
Crayon Software Experts LLC	1.00%
Cribl	0.25%
CrisisGo	2.00%
CriticalStart	0.50%
Cronos Consulting Group	0.50%
CrowdAI	0.50%
CrowdStrike	1.00%
Culture Partners	0.25%
Customertimes Corp.	2.00%
Cvent Inc.	0.25%
CyanGate	2.00%
Cyara	0.50%
Cyber-Ark	0.25%
CyberReef	2.00%
CyberSixGill	0.50%
Cybrary	2.00%
Cycognito	2.00%
Cynerio	10.00%
D2L	0.25%
Daric	0.24%
Darzin Software	0.25%
Databricks Inc.	0.50%
Datadog	0.25%
DataShapes	0.25%
Decision Lens, Inc.	0.50%
Deep Instinct	0.49%
Defend3D	0.25%
Delinea Inc.	1.00%
Dell	2.00%
Deloitte	1.00%
Deloitte Transactions and Business	1.00%
Delphix	2.00%
DigEplan	0.50%
DigitalBlue Software	2.00%
DigitalXForce	2.00%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
DigitSec Inc.	0.25%
Diona	0.25%
Docebo	0.25%
Doctums	0.25%
DocuSign	2.00%
Druva	2.00%
DSA Technologies	0.25%
Dun & Bradstreet, Inc.	2.00%
eCare Vault	2.00%
eCivis, Inc	0.03%
Eclypsium, Inc.	0.25%
EcoInteractive	0.25%
Edbrix	0.50%
Edge Systems	0.25%
eHawk Solutions	0.25%
Elasticsearch Federal Inc	2.00%
Elasticsearch Inc.	2.00%
ElectrifAi	0.50%
Ellucian Company L.P.	2.00%
EMC	0.25%
Enhanced Voting	1.00%
Entara Corporation	0.25%
EPAY	0.13%
e-PlanSoft	0.25%
Equinix	0.25%
Ernst & Young	0.50%
Esper Regulatory Technologies, Inc.	0.25%
EVAN360	0.50%
Everbridge	0.22%
Everlaw	0.25%
EvidenceIQ	1.00%
EvolveWare Inc.	0.25%
Exabeam	1.67%
Exiger	0.24%
Exterro, Inc.	1.00%
ExtraHop	2.00%
F3 Technology Partners	0.25%
F5 Networks, Inc.	2.00%
FastDial	0.50%
Federated Wireless	0.25%
FedStore	0.25%
Fend Incorporated	0.25%
Ferretly	0.50%
FI Consulting	0.25%
Fidelis Security	0.25%
Field2Base, Inc	0.25%
FireEye	2.00%
FiscalNote, Inc.	10.00%
Five9	2.00%
Fivetran	2.00%
Flashpoint	2.00%
Flexera Software	2.00%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Flok Consulting, Inc.	0.23%
Flosum	0.50%
Flowtrac	0.25%
Fluid Mobility	2.00%
FM Systems	0.50%
ForceBrain.com, Inc.	0.50%
Forcelution Apps B.V.	0.25%
Forensic Logic	1.00%
Forescout Technologies	2.00%
FormAssembly	2.00%
Fortinet	2.00%
Fortra, LLC	0.00%
FulcrumApp	0.25%
Fusion Health	0.50%
Fusion Risk Management	0.50%
FutureFit AI	0.50%
Gallus Communications LLC dba	0.25%
Genesys	2.00%
GeoSolutions USA Corp	2.00%
GigaKOM	5.00%
Gigamon	2.00%
Gimmal	0.25%
GitLab	2.00%
GL Suite, Inc. (dba GL Solutions)	0.25%
Glance	0.50%
Global Business Consulting Services	3.85%
Gold Bridge Partners	0.25%
Golden Recursion	0.50%
Google	2.00%
GoSecure Inc	0.25%
Granicus	2.00%
Gravel Road Data Labs, LLC	1.99%
Gray Quarter, Inc.	0.50%
Great Northern Consulting Services	0.25%
Green Diamond	0.25%
GreenAppy, LLC	0.50%
GreyMatter.io	0.25%
GreyNoise	0.50%
Greystones Group	0.25%
Gridless Power Corporation	0.50%
Guardian Alliance Technologies, Inc.	1.00%
Guidehouse	2.00%
Gyst Technologies	0.25%
H2O.ai	0.50%
HackerOne	0.25%
Halcyon	0.25%
HashiCorp	0.25%
HealthTech Solutions LLC	0.25%
Heimdall Data	0.50%
Hello Lamp Post	0.25%
Hexalytics Inc	0.19%
HHS Tech Group	0.25%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Hike2 LLC	0.00%
HiPER Solutions, LLC	2.00%
Hootsuite Media Inc.	0.25%
Horizon3.ai	2.00%
HPE	2.00%
HYCU, Inc.	0.25%
Hyland LLC	0.25%
IBM	1.00%
iboss	0.47%
Icertis	2.00%
Ideal Integrations	2.00%
IDEMIA Identity & Security USA	0.25%
Identity Automation	1.99%
iLAB	0.25%
Illumio	0.25%
Image Access Corporation	2.00%
Imagine Solutions	0.25%
Imagine Solutions llc	0.25%
Imperva	2.00%
Incapsulate	0.50%
Incode Technologies	2.00%
Indigov	0.25%
Industrial Defender	0.00%
Infoblox	1.00%
Infocyte, Inc.	0.50%
Informatica, Inc.	2.00%
Informatix, Inc.	2.00%
Infosec (previously Infosec Institute)	0.25%
Inframappa	0.25%
Innive Inc	0.35%
InSource	0.50%
ins-pi GmbH	0.25%
Instabase	0.25%
Insystech Inc	0.50%
Intact Partners Inc	0.50%
Intelinair	0.25%
Intellective 1	0.50%
Interact	0.50%
Interactive Data, LLC	0.50%
Interos	2.00%
Invictus Apps	0.25%
Invita Healthcare Technologies	0.50%
IP Pathways, LLC	0.74%
Iron Mountain	0.21%
IronNet Cybersecurity	1.00%
Ispheres	0.25%
ITS Delivers	0.25%
Ivanti, Inc.	0.25%
John Snow Labs	2.00%
JSMpros Inc	0.25%
Juniper	0.25%
JusticeText	0.25%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Kapalya Inc.	2.00%
Kaseware, Inc.	0.25%
Keeper Security, Inc.	2.00%
Keralia	2.00%
Keyavi Data Corp	0.50%
Keyser Consulting Group, LLC	0.25%
Kinetica DB Inc.	0.25%
Kinney Group	2.00%
Kion	2.00%
KIRO Group	0.25%
Kiteworks	2.00%
Konverge Digital Solutions	0.25%
KPMG	1.00%
Kyndi	0.25%
Kyriba	0.50%
Lacuna Technologies Inc.	0.50%
LaunchPad	0.50%
Leadership Connect	0.50%
Leankor	0.50%
Leaptree Limited	0.50%
LeaseAccelerator	0.50%
LeGuard, Inc.	0.50%
LEIDIT LLC	0.25%
Level Access, Inc.	0.50%
LexisNexis Risk Holdings	1.00%
LinkedIn CAD	1.00%
LinkedIn Corporation	1.00%
Liqid, Inc.	0.25%
LiveAction	0.50%
Livestream Learning Studio	0.25%
LNB Solutions	0.25%
Locality Media dba First Due	2.00%
LogicManager	0.25%
LogicMonitor	0.25%
Looker Data Sciences, Inc.	0.25%
Lookout Inc.	1.00%
Lovelytics	0.25%
Luminare	0.25%
LUMU Technologies	0.25%
MAD Security	0.15%
MaeTech Inc.	0.05%
Magnet Forensics	0.15%
Mandiant	1.00%
MangoApps	0.15%
MapAnything	2.00%
Mark43, Inc.	0.06%
MarkLogic	0.15%
Material Security	0.50%
Matillion	0.15%
Maverick Quantum Inc.	0.49%
Mazars USA LLP	0.15%
Mazda Computing	0.15%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
McAfee	1.00%
McKinsey & Company	2.00%
Measure UAS, Inc.	0.50%
MedTrainer	0.15%
Menlo Security	0.15%
Merative	0.15%
Mercurio Analytics, Inc.	0.15%
Mercury Storage	0.15%
Merlin International	0.15%
Metrc	0.50%
Micro Focus	2.00%
Microsoft Corporation	2.00%
Microsoft CSP	2.00%
Millsapps, Ballinger & Associates	0.05%
Mimecast North America Inc	0.15%
Mission Essentials LLC	0.15%
MobileMind Technologies	0.50%
Moove.ai	0.15%
Mossé Security	0.15%
Moveworks Inc	0.15%
Moxfive	1.24%
MS2 (Midwestern Software Solutions)	0.07%
MST Solutions	0.49%
MTX Group Inc.	2.00%
MuleSoft	2.00%
MV VeriSol	0.50%
mxHero	2.00%
My Emma	0.05%
Nally Ventures	0.50%
NaphCare, Inc	0.50%
NCS Analytics	0.50%
NetApp	0.15%
Netcraftsmen	0.15%
NetDocuments	0.15%
NetFoundry	2.00%
NetImpact Strategies, Inc	0.15%
Netskope	0.50%
NetSmart Technologies, Inc.	0.15%
NetSPI	0.15%
Netwrix Corporation	5.00%
NetX	0.15%
New Relic, Inc.	2.00%
NexTalk, Inc.	0.50%
Nicus	2.00%
Nile Global Inc.	0.15%
Nintex	0.15%
NNData	0.08%
Noname Public Sector LLC	0.15%
Northpoint Solutions LLC	0.50%
Northwoods Consulting Partners, Inc.	0.50%
Novacoast	9.09%
nsKnox Technologies	0.15%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
NTT DATA	2.00%
NU Borders	0.15%
Nuance	2.00%
Nucleus Security, Inc.	2.00%
NuHarbor	0.15%
Nutanix	1.00%
Nuvolo Technologies	0.50%
NWO.ai INC	0.15%
Oak Innovation Limited	2.00%
Ocient	2.00%
Odaseva	2.00%
Okta, Inc.	0.15%
On Point Technology	2.00%
On2It	0.15%
Open Storage Solutions	0.15%
OpenCounter, Inc.	0.50%
OpenGov	0.91%
OPEXUS	0.15%
OPSWAT, Inc.	0.15%
Optezo, Inc.	0.02%
Orbital Insight, Inc.	0.15%
Orca Security	0.15%
Otava	2.00%
Outpost Security	0.15%
Outreach Solutions as a Service LLC	2.00%
OutSystems	0.15%
OwnBackup	2.00%
Oxford Consulting Group	0.15%
PacketViper	2.00%
Palo Alto Networks	2.00%
Panther International, LLC	2.00%
Paperless Innovations, Inc.	0.15%
Pathlock	0.15%
Paxera Health	0.50%
PaymentWorks	0.50%
PayScale, Inc.	0.15%
PC Matic, Inc.	0.15%
PCI Pal	0.15%
Peak Performance Solutions	2.00%
PencilData	0.50%
Percipient.AI	2.00%
Peregrine Technologies	0.50%
Permuta Technologies, Inc.	0.15%
Persado	0.50%
PhoneLiveStreaming	2.00%
Photon Medical Communications, Inc.	0.12%
Pick Cloud	0.15%
Ping Identity Corporation	1.00%
Planergy	0.15%
Planet Technologies	1.50%
PlatCore	0.50%
Playground	0.15%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Plotly	0.15%
Poly	0.15%
Pondera Solutions	10.00%
Pondurance, LLC	0.15%
Precisio Business Solutions, Corp.	0.12%
Preservica	1.50%
Procore Technologies Inc.	2.00%
Proficio	0.50%
Project Hosts, Inc.	0.15%
Promise Network, Inc.	0.15%
Proofpoint, Inc.	2.00%
prooV Inc.	0.12%
ProSymmetry	2.00%
Proven Optics LLC	0.50%
Provisions Group LLC	0.15%
PublicInput.com	0.15%
Pulselight	0.50%
Pyramid Analytics	2.00%
Qii.AI	0.50%
Qmulos, LLC	0.15%
QTS Realty Trust, Inc	0.14%
Qualtrics	2.00%
quantiFind	0.50%
Quantiphi Inc	1.00%
Questica	0.50%
Queue-it	0.05%
Quickbase	0.15%
Quicko Technosoft Labs Pvt. Ltd.	0.12%
Quova, Inc.	0.15%
QuSecure	0.15%
Quzara	3.00%
R4	0.14%
Rackspace	1.76%
Radiant Logic, Inc.	0.15%
Ram Mounts	0.15%
RangeForce	2.00%
Rapid7	2.00%
Ratio PBC, Inc.	0.15%
Ready.net	0.15%
ReadyWorks	0.15%
Recite Me	0.15%
Recorded Future	2.00%
Redapt Inc	0.15%
Reframe Solutions	0.15%
REI Systems	2.00%
Remix Technologies	0.15%
Rendered.AI	0.15%
ResourceX	0.15%
Rhino Health	0.15%
Rhondos	2.00%
RideAmigos	0.50%
Right-Hand Cybersecurity	0.15%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Ripcord Inc.	0.15%
Risklens	1.00%
RiskSense	2.00%
Riverbed Technology	1.00%
R-MOR LLC	0.15%
Rocket Software	2.00%
Rocket.Chat	0.15%
ROK Technologies	1.00%
Roundtrip	2.00%
RSA	2.00%
Rubrik	0.50%
Ruckus Wireless	0.05%
Run Consultants	0.50%
Run:AI	2.00%
runZero	0.15%
R-Zero Systems	0.15%
S Nimbus, LLC	0.15%
Saasyan	1.79%
sailpoint	0.50%
SAINAPSE Inc	0.15%
Salesforce.com	0.50%
Salty Cloud, PBC	0.15%
SAP	2.00%
SAP NS2	0.14%
Saviynt	5.00%
Scale AI	2.00%
SchoolBanks, Inc	0.50%
SDGblue, LLC	0.15%
S-Docs	0.12%
Secured Communications	0.15%
Secureworks, Inc.	1.00%
Securin	0.15%
Security Scorecard	1.00%
SecZetta	0.40%
Selfhelp Community Services	0.15%
Semarchy, Inc.	2.00%
Semperis	0.15%
Sentinel One	2.00%
ServiceNow	2.00%
sFiles	2.00%
ShadowDragon Federal	1.00%
Sherpa Government Solutions, LLC	0.05%
Shiftsmart	0.15%
Shmoop	0.50%
SightCall, Inc.	0.50%
Silverback Learning Solutions dba	0.01%
SimpliGov LLC	1.00%
Singlewire Software	0.15%
Sitetracker	0.50%
Sixteen Labs	0.15%
Skedulo	2.00%
Skuid, Inc.	0.02%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Skyline Technology Solutions	0.15%
SkyPlanner LLC	0.50%
Smartsheet	0.50%
Snowflake Inc.	2.00%
Socrata, Inc.	0.15%
Socure	0.15%
Sodales Solutions	0.15%
Softdocs SC, LLC	0.50%
Software Information Resource Corp	0.15%
Solace Health	0.15%
Sonitum Inc. dba SonicCloud	0.15%
Sophos Inc	0.15%
Spatialitics, LLC	0.13%
Spectralogic	2.00%
Sphere Technology Solutions	0.50%
Splunk	1.00%
SportGait	0.15%
SpringCM	5.00%
SpringML	0.50%
Sprinklr	0.50%
Stage2Data	0.15%
Stave	0.50%
Stony Point	0.15%
Stralto Inc.	0.15%
Submittable	0.15%
SuccessKPI Inc.	0.15%
Suggestion Ox	0.15%
Sun Management	0.15%
Swiftly, Inc.	0.50%
Sylabs	0.15%
Symantec	2.00%
Symmetry Systems	2.00%
Syncsort	0.15%
Synergy SKY	0.15%
Syntasa	2.00%
System Automation Corporation	0.50%
Tableau Software	2.00%
Talend Inc.	0.15%
Talkdesk	2.00%
TAMR	0.15%
Tanium Federal Corporation	0.15%
Tanium Inc.	0.15%
Team Cymru	0.50%
Team IA	2.00%
Tecnics Consulting Inc.	2.00%
Tek Advisory Group, LLC	0.50%
TeleMessage	2.00%
Telos Corporation	0.50%
Tenable Public Sector, LLC	2.00%
Tensor Networks	0.50%
Teradata	2.00%
Terrascope	0.15%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Tessian	0.15%
Theiagen Genomics	0.15%
Thentia	2.00%
ThoughtSpot, Inc.	0.15%
Tintri	1.00%
Titan Technologies	0.15%
TonicAI	0.15%
TrackIt Project Management Systems,	0.50%
Traction on Demand	1.00%
TRADS	1.00%
TranslateLive	0.50%
TransUnion	1.00%
Tricentis Americas, Inc.	2.00%
Tricentis USA Corp	2.00%
Trimble	0.05%
Trinity Cyber LLC	0.50%
Trinity Education Group, Inc.	0.50%
True Zero Technologies Inc.	0.05%
truED Consulting	0.15%
Trusona	0.15%
Trustwave	2.00%
Tufin	0.15%
Turbonomic	0.50%
TVU Networks	1.00%
Twenty Labs	0.15%
Twilio	2.00%
Tyler Technologies, Inc.	2.00%
Udacity, Inc.	0.50%
UiPath, Inc.	0.15%
Unit4	0.50%
Unite Us	0.15%
UniVoIP	0.15%
Unqork	0.20%
UserWay	2.00%
Valimail	0.50%
Varonis	0.15%
Vector Zero	0.15%
Vectra	1.00%
Veeam Software Corp.	0.15%
Venyu Solutions dba Eatel	0.14%
Veracode	5.00%
Verge Technology Solutions	0.15%
VERITAS	0.15%
Veritone, Inc.	0.14%
Verkada	0.94%
VersaFile	0.15%
Vertiba	0.50%
Vexcel Group	0.15%
Via Science, Inc	0.15%
Vibronyx	0.15%
VIQ Solutions	5.00%
Virsec	2.00%

Exhibit A - Pricing for Contract 6508243

Cloud Service Provider	Nashville METRO Discount
Virtru Corporation	0.15%
Virtustream	1.00%
Vision-e	0.05%
Visium Technologies	0.06%
Vivi	0.50%
VividCharts	0.50%
Vlocity	0.50%
VMware	2.00%
Voyager Analytics Inc	1.00%
Vyopta	0.15%
Wabbi	0.50%
WalkMe	1.99%
Wasabi Technologies, Inc.	0.05%
Webauthor.com, LLC	0.50%
WEKA IO	0.15%
WellSky	2.00%
Whispir	0.50%
WhiteHawk	2.00%
WireScreen	0.15%
WireSpring Technologies, Inc.	3.00%
WithSecure	0.05%
Wiz	0.02%
WizeHive, Inc.	0.15%
Wonderschool Inc.	0.50%
Workforce Software	0.15%
Workfront, Inc.	2.00%
Workiva	2.00%
Yansa Labs	0.50%
YellowSchedule	1.00%
Yext, Inc.	0.06%
Yubico, Inc.	0.15%
ZenCity	0.50%
ZenLedger	2.00%
Zentera	0.15%
Zimperium	2.00%
Zoom	2.00%
Zscaler US Government Solutions LLC	2.00%
Zscaler, Inc.	2.00%

SECTION A-1

General Terms and Conditions

1 **Safeguards.** In addition to the controls specified in the exhibits to this Agreement, Contractor agrees to implement administrative, physical, and technical safeguards to protect the availability, confidentiality and integrity of Metropolitan Government of Nashville and Davison County (Metro Government) Information, information technology assets and services. All such safeguards shall be in accordance with industry-wide best security practices and commensurate with the importance of the information being protected, but in no event less protective than those safeguards that Contractor uses to protect its own information or information of similar importance or is required by applicable federal or state law.

2 **Inventory.** Contractor agrees to maintain at all times during the Term of this Agreement a Product and Service Inventory. Contractor shall upon request of Metro Government, which shall be no more frequently than semi-annually, provide the current Product and Service Inventory to Metro Government within thirty (30) days of the request.

3 **Connection of Systems or Devices to the Metro Government Network.** Contractor shall not place any systems or devices on the Metro Government Network without the prior written permission of the Director of ITS, designee, or the designated Metro Government contact for this Agreement.

4 **Access Removal.** If granted access to Metro Government Network or systems, Contractor and its Agents shall only access those systems, applications or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass security controls. Notwithstanding anything to the contrary in the Purchasing Agreement or other agreement between Metro Government and Contractor, Metro Government at its sole discretion, may refuse granting access right to Metro Government Network or Sensitive Information to any Agent of Contractor, and may at any time remove access rights (whether physical premise access or system access) from Contractor or any Agents, without prior notice or liability to Contractor, if Metro Government reasonably suspects a security violation by Contractor or such Agent or otherwise deems such action appropriate to protect Metro Government Infrastructure, Metro Government Network or Metro Government Information.

5 **Subcontracting/Outsourcing.**

5.1 Prior Approval. Without Metro Government's prior written consent, Contractor may not subcontract with a third party to perform any of its obligations to Metro Government which involves access to Metro Government Information or connection to Metro Government Network. Nor shall Contractor outsource any Contractor infrastructure (physical or virtual) which Stores Sensitive Information without such consent. To obtain Metro Government's consent, Contractor shall contact the Metro Government ITS department. In addition, Metro Government may withdraw any prior consent if Metro Government reasonably suspect a violation by the subcontractor or outsource provider of this Agreement, or otherwise deems such withdraw necessary or appropriate to protect Metro Government Network, Metro Government Infrastructure or Metro Government Information.

5.2 Subcontractor Confidentiality. Contractor Agents are bound by the same confidentiality obligations set forth in this Agreement. Contractor or its Agent may not transfer, provide access to or otherwise make available Metro Government Information to any individual or entity outside of the United States (even within its own organization) without the prior written consent of Metro Government. To obtain such consent, Contractor shall send Metro Government a notice detailing the type of information to be disclosed, the purpose of the disclosure, the recipient's identification and location, and other information required by Metro Government.

5.3 Contractor Responsibility. Prior to subcontracting or outsourcing any Contractor's obligations to Metro Government, Contractor shall enter into a binding agreement with its subcontractor or outsource service provider ("Third Party Agreement") which (a) prohibits such third party to further subcontract any of its obligations, (b) contains provisions no less protective to Metro Government Network, Metro Government Infrastructure and/or Metro Government Information than those in this Agreement, and (c) expressly provides Metro Government the right to audit such subcontractor or outsource service provider to the same extent that Metro Government may audit Contractor under this Agreement. Contractor warrants that the Third Party Agreement will be enforceable by Metro Government in the U.S. against the subcontractor or outsource provider (e.g., as an intended third party beneficiary under the Third Party Agreement).

Without limiting any other rights of Metro Government in this Agreement, Contractor remains fully responsible and liable for the acts or omissions of its Agents. In the event of an unauthorized disclosure or use of Sensitive Information by its Agent, Contractor shall, at its own expense, provide assistance and cooperate fully with Metro Government to mitigate the damages to Metro Government and prevent further use or disclosure.

SECTION A-2

Definitions

Capitalized terms used in the Agreement shall have the meanings set forth in this Exhibit A-2 or in the *Metropolitan Government Information Security Glossary*, which can be found on the Metropolitan Government of Nashville website . Terms not defined in this Exhibit A-2 or otherwise in the Agreement shall have standard industry meanings.

1. "Affiliates" as applied to any particular entity, means those entities, businesses, and facilities that are controlled by, controlling, or under common control with a stated entity, as well as (with respect to Metro Government) any entity to which Metro Government and/or any of the foregoing provides information processing services.

2. "Agent" means any subcontractor, independent contractor, officer, director, employee, consultant or other representative of Contractor, whether under oral or written agreement, whether an individual or entity.

3. "Agreement" means this Information Security Agreement, including all applicable exhibits, addendums, and attachments.

4. "Information Breach" means any actual or suspected unauthorized disclosure or use of, or access to, Metro Government Information, or actual or suspected loss of Metro Government Information.

5. "Effective Date" means the date first set forth on page 1 of the Agreement.

6. "Metro Government Information" means an instance of an information type belonging to Metro Government. Any communication or representation of knowledge, such as facts, information, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual, owned by or entrusted to Metro Government.

7. "Metro Government Infrastructure" means any information technology system, virtual or physical, which is owned, controlled, leased, or rented by Metro Government, either residing on or outside of the Metro Government Network. Metro Government Infrastructure includes infrastructure obtained from an IAAS provider or systems that are provided and located on the Metro Government Network as part of a Service.

8. "Metro Government Network" means any Wide Area Network (WAN) or Local Area Network (LAN) owned, operated, managed or controlled by Metro Government.

9. "Term" means the period during which this Agreement is in effect.

SECTION AST

Agent Security and Training

1 **Background Check.** Upon written request from METRO, Contractor shall perform a background check which includes a criminal record check on all Agents, who may have access to Metro Government Information. Contractor shall not allow any Agents to access Metro Government Information or perform Services under a Purchasing Agreement if Contractor knows or reasonably should know that such Agent has been convicted of any felony or has been terminated from employment by any employer or contractor for theft, identity theft, misappropriation of property, or any other similar illegal acts.

2 **Information Security Officer.** If Agents will access or handle Metro Government Information, Contractor shall designate an Information Security Officer, who will be responsible for Contractor information security and compliance with the terms of this Agreement as it relates to Metro Government Information.

3 **Agent Access Control.** Contractor shall implement and maintain procedures to ensure that any Agent who accesses Metro Government Information has appropriate clearance, authorization, and supervision. These procedures must include:

3.1 Documented authorization and approval for access to applications or information stores which contain Metro Government Information; e.g., email from a supervisor approving individual access (note: approver should not also have technical rights to grant access to Sensitive Information); documented role-based access model; and any equivalent process which retains documentation of access approval.

3.2 Periodic (no less than annually) reviews of Agent user access rights in all applications or information stores which contain Sensitive Information. These reviews must ensure that access for all users is up-to-date, appropriate and approved.

3.3 Termination procedures which ensure that Agent's user accounts are promptly deactivated from applications or information stores which contain Sensitive Information when users are terminated or transferred. These procedures must ensure that accounts are deactivated or deleted no more than 14 business days after voluntary termination, and 24 hours after for cause terminations.

3.4 Procedures which ensure that Agent's user accounts in applications or information stores which contain Sensitive Information are disabled after a defined period of inactivity, no greater than every 180 days.

3.5 Procedures which ensure that all Agents use unique authentication credentials which are associated with the Agent's identity (for tracking and auditing purposes) when accessing systems which contain Sensitive Information.

3.6 Contractor will maintain record of all Agents who have been granted access to Metro Government Sensitive Information. Contractor agrees to maintain such records for the length of the agreement plus 3 years after end of agreement. Upon request, Contractor will supply Metro Government with the names and login IDs of all Agents who had or have access to Metro Government Information.

4 **Agent Training.**

4.1 Contractor shall ensure that any Agent who access applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of the information or information and the security of the application. Completion of this training must be documented and must occur before Agent may access any Sensitive Information. This training must include, at a minimum:

4.1.1 Appropriate identification and handling of Metro Government Information

4.1.1.1 Awareness of confidentiality requirements contained in this Agreement;

4.1.1.2 Procedures for encrypting Metro Government Information before emailing or transmitting over an Open Network, if the information classification of the information requires these controls;

4.1.1.3 Procedures for information storage on media or mobile devices (and encrypting when necessary).

4.1.2 Education about the procedures for recognizing and reporting potential Information Security Incidents;

4.1.3 Education about password maintenance and security (including instructions not to share passwords);

4.1.4 Education about identifying security events (e.g., phishing, social engineering, suspicious login attempts and failures);

4.1.5 Education about workstation and portable device protection; and

4.1.6 Awareness of sanctions for failing to comply with Contractor security policies and procedures regarding Sensitive Information.

4.1.7 Periodic reminders to Agents about the training topics set forth in this section.

4.2 Contractor shall ensure that any Agent who accesses applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of this information. Completion of this training must be documented and must occur before Agent may access any Metro Government Information. This training must include, at a minimum:

4.2.1 Instructions on how to identify Metro Government Information.

4.2.2 Instructions not to discuss or disclose any Sensitive Information to others, including friends or family.

4.2.3 Instructions not to take media or documents containing Sensitive Information home unless specifically authorized by Metro Government to do so.

4.2.4 Instructions not to publish, disclose, or send Metro Government Information using personal email, or to any Internet sites, or through Internet blogs such as Facebook or Twitter.

4.2.5 Instructions not to store Metro Government Information on any personal media such as cell phones, thumb drives, laptops, personal digital assistants (PDAs), unless specifically authorized by Metro Government to do so as part of the Agent's job.

4.2.6 Instructions on how to properly dispose of Metro Government Information, or media containing Metro Government Information, according to the terms in Exhibit DMH as well as applicable law or regulations.

5 Agent Sanctions. Contractor agrees to develop and enforce a documented sanctions policy for Agents who inappropriately and/or in violation of Contractor's policies and this Agreement, access, use or maintain applications or information stores which contain Sensitive Information. These sanctions must be applied consistently and commensurate to the severity of the violation, regardless of level within management, and including termination from employment or of contract with Contractor.

SECTION BU

Information Backup, Contingency Planning and Risk Management

1 General.

1.1 Contractor agrees to backup Metro Government Information which Contractor maintains or Stores. Backup and restoration procedures and related infrastructure, including frequency of backup, offsite storage, media lifespan and media reliability, must be commensurate with the criticality and availability requirement of the Metro Government Information being backed up.

1.2 Upon Metro Government's request, Contractor shall supply Metro Government with an inventory of Metro Government Information that Contractor Stores and/or backed up.

1.3 Contractor shall periodically, no less often than annually, test backup tapes or media by restoring Metro Government Information to a system similar to the original system where the Metro Government Information are stored.

1.4 Upon Metro Government's request, Contractor shall supply copies of Metro Government Information in a format requested by Metro Government.

1.5 Contractor shall backup business critical information at a frequency determined by Metro Government business owner.

2 Storage of Backup Media. Contractor shall store archival and backup media in a secured offsite location. Upon request, Contractor will promptly notify Metro Government of the physical address of the offsite location. The backups of the information should be stored in a manner commiserate with the security around the information. The backup tapes should be encrypted if the sensitivity of the information requires that level of security.

3 Disaster Recovery Plan. Contractor will maintain a Disaster Recovery Plan for all applications or information stores which contain business critical information. This plan will outline the procedures necessary to restore business critical information on the application or systems in a timely fashion in the case of an emergency or disaster.

4 Emergency Mode Operation Plan. Contractor shall maintain an emergency mode operating plan which ensures that systems or applications using or accessing business critical information are operational during an emergency or natural disaster, or are made operational after a disaster in a prompt manner, commensurate with the criticality of the information on the system.

5 Testing and Revision Procedure. Contractor agrees to test, at least annually, Contractor Disaster Recovery Plan and emergency mode operations plan and maintain a documented procedure for such testing. Contractor shall document the results and findings from such testing and revise the plan accordingly.

6 Risk Management Requirements. Contractor shall implement internal risk management practices to ensure the confidentiality, integrity and availability of Metro Government Information. These practices will be no less secure than the ones used by Contractor to protect Contractor's own Sensitive Information or information of comparable sensitivity.

SECTION CSP

Cloud Service Providers

1 Certifications and Compliance.

1.1. Contractor will, on at least an annual basis, hire a third party auditing firm to perform a Statement on Standards for Attestation Engagements (SSAE) No. 16 audit, or equivalent audit, on internal and external Contractor procedures and systems that access or contain Metro Data.

1.2. Contractor shall adhere to SOC 1/SSAE 16 audit compliance criteria and data security procedures (or any successor report of a similar nature that is generally accepted in the industry and utilized by Contractor) applicable to Contractor. Upon Metro's request, Contractor will provide Metro with a copy of the audit results set forth in Contractor's SOC 1/SSAE 16 audit report.

1.3. Metro shall have the right to terminate this Agreement (together with any related agreements, including licenses and/or Statement(s) of Work) and receive a full refund for all monies prepaid thereunder in the event that the Contractor fails to produce an acceptable SSAE-16/ SOC-1 Type II report.

1.4. The Contractor will ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act) 44 U.S.C. § 3541, et seq.), NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special Publications 800-53, 800-59, and 800-60. In addition, the Contractor must provide Metro with any documentation it requires for its reporting requirements within 10 days of a request.

1.5. Contractor agrees to comply with all applicable privacy laws.

2 **Data Security.** Metro data, including but not limited to data hosted, stored, or held by the Contractor in the Product(s) or in the platform operated by Contractor, or on any device owned or in the custody of Contractor, its employees, agents or Contractors, will be encrypted. Contractor will not transmit any unencrypted Metro Data over the internet or a wireless network, and will not store any Metro Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software approved by Metro.

3 **Use of Subcontractors.** The Contractor shall retain operational configuration and control of data repository systems used to process and store Metro data to include any or remote work. In the event that the Contractor has subcontract the operational configuration and control of any Metro data, Contractor is responsible for ensuring that any third parties that provide services to the Contractor meets security requirements that the Contractor has agreed upon in this contract.

4 **Location of Data.** The Contractor shall maintain all data within the United States, which means the 50 States, the District of Columbia, and outlying areas. Upon request, the Contractor shall provide Metro with a list of the physical locations that may contain Metro data within 20 days with updates on a quarterly basis.

5 **Personnel Access.** The Contactor will require all employees who will have access to Metro data, the architecture that supports Metro data, or any physical or logical devices/code to pass an appropriate background investigation.

6 Asset Availability.

6.1. The Contractor must inform Metro of any interruption in the availability of the cloud service as required by the agreed upon service level agreement. Whenever there is an interruption in service, the Contractor must inform Metro of the estimated time that the system or data will be unavailable. The Contractor must provide regular updates to Metro on the status of returning the service to an operating state according to any agreed upon SLAs and system availability requirements.

6.2. The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with Metro's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing timely notification to Metro and shall be responsible for working with Metro to identify appropriate remedies and if applicable, work with Metro to facilitate a smooth and seamless transition to an alternative solution and/or provider.

7 Misuse of Metro Data and Metadata.

7.1. The Contractor shall not access, use, or disclose Metro data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Metro data shall only be for purposes specified in this contract or task order. Contractor shall ensure

that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Metro data, sign a contract or task order specific nondisclosure agreement.

7.2. The Contractor shall use Metro-related data only to manage the operational environment that supports Metro data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer. A breach of the obligations or restrictions may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by the breach.

8 Data Breach and Incident Reporting.

8.1. The Contractor will submit reports of cyber incidents through approved reporting mechanisms. The Contractor's existing notification mechanisms that are already in place to communicate between the Contractor and its customers may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

8.2. The Contractor will use a template format when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

8.3. In addition to the above, if the incident concerns a breach of PII or a potential breach of PII, the Contractor will report to the contracting officer's designee within 24 hours of the discovery of any data breach. The Contractor shall provide Metro with all information and cooperation necessary to enable compliance by the Contractor and/or Metro with data breach reporting and mitigation actions required by applicable law, regulation, policy, and this contract.

9 **Facility Inspections.** The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by Metro, conduct a security audit based on Metro's criteria as needed, but no more than once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with Metro within 20 days of the Contractor's receipt of the audit results.

10 Law Enforcement.

10.1. The Contractor shall record all physical access to the cloud storage facilities and all logical access to Metro data. This may include the entrant's name, role, purpose, account identification, entry and exit time.

10.2. If Metro data is co-located with the non-Metro data, the Contractor shall isolate Metro data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Metro personnel identified by the Metro personnel, and without the Contractor's involvement.

11 **Maintenance.** The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement to prevent proactively the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, with special emphasis on assuring that the vendor's PVM systems and programs apply standardized configurations with automated continuous monitoring of the same to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained to assure all software products deployed in the Contractor's operating environment and serving Metro are compatible with existing systems and architecture of Metro.

12 **Notification.** The Contractor shall notify Metro within 60 minutes of any warrants, seizures, or subpoenas it receives that could result in the loss or unauthorized disclosure of any Metro data. The Contractor shall cooperate with Metro to take all measures to protect Metro data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.

13 **Supply Chain**. The Contractor is responsible for exercising due diligence to use genuine hardware and software products that are free of malware.

14 **Service Level Agreements.** The Contractor shall work with Metro to develop a service level agreement, including defining roles, responsibilities, terms, and clear measures for performance by Contractor.

SECTION IR

Incident Response

1 Incident Reporting. Contractor shall report any Information Security Incident of which it becomes aware, or failure of any technical or procedural controls, which has or had a potential to affect Metro Government Network, Metro Government Infrastructure or Metro Government Information to Metro Government and according to the following timeline and procedure:

1.1 Contractor shall promptly report to Metro Government any successful Information Security Incident (with or without actual harm to system or information) within 24 hours of becoming aware of the incident. At a minimum, such report shall contain: (a) date and time when the Information Security Incident occurred; (b) the date and time when such incident was discovered by Contractor; (b) identification of the systems, programs, networks and/or Metro Government Information affected by such incident; (c) preliminary impact analysis; (d) description and the scope of the incident; and (e) any mitigation steps taken by Contractor However, if Contractor is experiencing or has experienced a Information Breach or a successful Information Security Incident to systems that host or Store Sensitive Information or an Information Security Incident that is causing or has caused material disruption to the functionality or operation of Contractor systems or damage to Contractor hardware, software or information, including a successful attack by Malicious Software, Contractor shall report such security breach or incident to Metro Government both to the ITS Help Desk at (615) 862-HELP and to the Metro Government department within 24 hours from Contractor's reasonable awareness of such security breach or incident.

1.2 Contractor shall document any attempted but unsuccessful Information Security Incident of which it becomes aware and report to Metro Government upon its request. The frequency, content, and format of such report will be mutually agreed upon by the parties.

2 Incident Response.

2.1 Contractor shall have a documented procedure for promptly responding to an Information Security Incidents and Information Breach that complies with applicable law and shall follow such procedure in case of an incident. Contractor shall have clear roles defined and communicated within its organization for effective internal incidence response.

2.2 Contractor shall designate a contact person for Metro Government to contact in the event of an Information Security Incident. This contact person should possess the requisite authority and knowledge to: (i) act as a liaison to communicate between Contractor and Metro Government regarding the incident (including providing information requested by Metro Government); (ii) perform the reporting obligations of Contractor under this exhibit; and (iii) develop a mitigation strategy to remedy or mitigate any damage to Metro Government Network, Metro Government Infrastructure, Metro Government Information or the Product or Service provided to Metro Government that may result from the Information Security Incident.

SECTION PAT

Patch Creation and Certification

1 **Security Patch Required.** Unless otherwise expressly agreed by Metro Government and Contractor, for Products that are no longer under performance warranty, Contractor shall provide no less than standard maintenance and support service for the Products, which service includes providing Security Patches for the Products, for as long as Metro Government is using the Products.

2 **Timeframe for Release.** For Vulnerabilities contained within the Product that are discovered by Contractor itself or through Responsible Disclosure, Contractor shall promptly create and release a Security Patch. Contractor must release a Security Patch: (i) within 90 days for Critical Vulnerabilities, (ii) within 180 days for Important Vulnerabilities, and (iii) within one (1) year for all other Vulnerabilities after Contractor becomes aware of the Vulnerabilities. For Vulnerabilities contained within the Product that have become publicly known to exist and are exploitable, Contractor will release a Security Patch in a faster timeframe based on the risk created by the Vulnerability, which timeframe should be no longer than thirty (30) days. For the avoidance of doubt, Contractor is not responsible for creation of Security Patches for Vulnerabilities in the Product that is caused solely by the Off-the-Shelf Software installed by Metro Government.

3 **Timeframe for Compatibility Certification.** Contractor shall promptly Certify General Compatibility of a Security Patch for third party software which the Product is dependent upon when such patch is released. For a Security Patch for Microsoft Windows Operating Systems, Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days, and shall Certify General Compatibility of an Important Security Patch within thirty (30) days, from the release of the patch. For Security Patches for Off-the-Shelf Software (OTS), Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days and Certify General Compatibility of an Important Security Patch within thirty (30) days from its release. For Security Patch for all other third party software or system, Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days and an Important Security Patch within thirty (30) days from its release. . Contractor shall publish whether the Security Patches are generally compatible with each related Product.

4 **Notice of Un-patchable Vulnerability.** If Contractor cannot create a Security Patch for a Vulnerability, or Certify General Compatibility of a Security Patch for OTS software, within the timeframe specified herein, Contractor shall notify Metro Government of the un-patchable Vulnerability in writing. Such notice shall include sufficient technical information for Metro Government to evaluate the need for and the extent of immediate action to be taken to minimize the potential effect of the Vulnerability until a Security Patch or any other proposed fix or mitigation is received.

5 **Vulnerability Report.** Contractor shall maintain a Vulnerability Report for all Products and Services and shall make such report available to Metro Government upon request, provided that Metro Government shall use no less than reasonable care to protect such report from unauthorized disclosure. The Vulnerability Report should (a) identify and track all known Vulnerabilities in the Products or Services on a continuing and regular basis, (b) document all Vulnerabilities that are addressed in any change made to the Product or Service, including without limitation Security Patches, upgrades, service packs, updates, new versions, and new releases of the Product or Service, (c) reference the specific Vulnerability and the corresponding change made to the Product or Service to remedy the risk, (d) specify the critical level of the Vulnerability and the applicable Security Patch, and (e) other technical information sufficient for Metro Government to evaluate the need for and the extent of its own precautionary or protective action. Contractor shall not hide or provide un-documented Security Patches in any type of change to their Product or Service.

6 **SCCM Compatibility for Windows Based Products.** Contractor Patches for Products that operate on the Microsoft Windows Operating System must be deployable with Microsoft's System Center Configuration Manager.

SECTION PES

Physical and Environmental Security

Contractor shall implement security measures at any Contractor facilities where Sensitive Information is stored. Such security measures must include, at a minimum:

1 **Contingency Operations.** A documented Disaster Recovery Plan for accessing the facility and the Sensitive Information, and restoring Sensitive Information if needed, in the case of an emergency or crisis.

2 **Environmental Safeguards**. Reasonable environmental safeguards to protect systems storing Sensitive Information from smoke, heat, water, fire, humidity, or power surge damage.

3 **Access Control.** Appropriate controls which ensure that only authorized personnel are allowed physical access to the facility. Examples of appropriate controls include, but are not limited to: signage; personnel badges and controlled badge access; visitor sign in, escort, and sign out; security guards; and video surveillance for information centers which store Sensitive Information.

4 **Maintenance Records.** Contractor shall conduct regular maintenance on systems which contain Sensitive Information and to facility's physical and environmental controls (e.g., temperature, physical access). Contractor shall maintain documentation of any repairs or maintenance performed on the systems or facility and shall provide Metro Government a copy of such records upon its reasonable request.

5 **Physical Safeguards.** Contractor shall use best efforts to prevent theft or damage to Contractor systems or storage media containing Sensitive Information. Such efforts shall include, but are not limited to:

5.1 Protecting systems or devices that contain un-encrypted Sensitive Information with physical barriers such as locked cabinet, floor to ceiling room, or secured cage.

5.2 Not storing Un-encrypted Sensitive Information in "multi-party" shared physical environments with other entities.

5.3 Not transporting or shipping un-encrypted media which stores Sensitive Information unless the information is sanitized through full media overwrite (at least one complete pass), or media destruction through shredding, pulverizing, or drive-punching (e.g., breaking the hard drive platters).

5.4 In the event Products generate, store, transmit or process Sensitive Information and the Product does not support encryption, Contractor shall be solely responsible for the provision of physical security measures for the applicable Products (e.g., cable locks on laptops).

SECTION SOFT

Software / System Capability

1 Supported Product.

1.1 Unless otherwise expressly agreed by Metro Government in writing, Contractor shall provide Metro Government only supported versions of the Product, which will not become “end of life” for at least 24 months. When the Product or Service requires third party components, Contractor must provide a Product that is compatible with currently supported third party components. Unless otherwise expressly agreed by Metro Government, Contractor represents that all third party components in its Product are currently supported, are not considered "end of life" by the third party provider of such components, and will not become "end of life" in less than 24 months from the date of acquisition by Metro Government.

1.2 If Open Source Software is incorporated into the Product, Contractor shall only use widely supported and active Open Source Software in the Product, and shall disclose such software to Metro Government prior to its acquisition of the Product.

1.3 Information transfers within applications and involving services should be done using web services, APIs, etc. as opposed to flat file information transport.

2 Software Capabilities Requirements.

2.1 Contractor shall disclose to Metro Government all default accounts included in their Product or provide a means for Metro Government to determine all accounts included in the Product.

2.2 Contractor shall not include fixed account passwords in the Product that cannot be changed by Metro Government. Contractor shall allow for any account to be renamed or disabled by Metro Government.

2.3 Contractor's Product shall support a configurable Session Timeout for all users or administrative access to the Product.

2.4 Contractor shall ensure that the Product shall transmit and store Authentication Credentials using Strong Encryption.

2.5 Contractor Products shall mask or hide the password entered during Interactive User Login.

2.6 Contractor shall ensure that Products provided can be configured to require a Strong Password for user authentication.

2.7 Contractor’s Product shall allow user accounts to be disabled after a configurable amount of failed login attempts over a configurable amount of time.

2.8 Contractor’s Product shall have the capability to require users to change an initial or temporary password on first login.

2.9 Contractor’s Product shall have the capability to report to Metro Government, on request, all user accounts and their respective access rights within three (3) business days or less of the request.

2.10 Contractor’s Product shall have the capability to function within Metro Governments Information Technology Environment. Specifications of this environment are available upon request.

3 Backdoor Software. Contractor shall not provide Products with Backdoor Software, including, without limitation, undocumented or secret access functions (e.g., accounts, authorization levels, over-rides or any backdoor). Contractor shall supply all information needed for the Metro Government to manage all access (local or remote) capabilities within the Product including denying of Remote Access entirely from any party including Contractor. Contractor shall not include any feature within the Product that would allow anyone to circumvent configured authorization remotely.

Affidavits

Compliance with Laws: After first being duly sworn according to law, the undersigned (Affiant) states that he/she and the contracting organization is presently in compliance with, and will continue to maintain compliance with, all applicable federal, state, and local laws.

Taxes and Licensure: Affiant states that Contractor has all applicable licenses, including business licenses. Affiant also states that Contractor is current on its payment of all applicable gross receipt taxes and personal property taxes. M.C.L. 4.20.065

Nondiscrimination: Affiant affirms that by its employment policy, standards and practices, it does not subscribe to any personnel policy which permits or allows for the promotion, demotion, employment, dismissal or laying off of any individual due to race, creed, color, national origin, age or sex, and are not in violation of, and will not violate, any applicable laws concerning the employment of individuals with disabilities. M.C.L. 4.28.020

Employment Requirement: Affiant affirms that Contactor's employment practices are in compliance with applicable United States immigrations laws. M.C.L. 4.40.060.

Covenant of Nondiscrimination: Affiant affirms that in consideration of the privilege to submit offers in response to this solicitation, we hereby consent, covenant, and agree as follows:
To adopt the policies of the Metropolitan Government relating to equal opportunity in contracting on projects and contracts funded, in whole or in part, with funds of the Metropolitan Government;
- To attempt certain good faith efforts to solicit Minority-owned and Woman-owned business participation on projects and contracts in addition to regular and customary solicitation efforts;
- Not to otherwise engage in discriminatory conduct;
- To provide a discrimination-free working environment;
- That this Covenant of Nondiscrimination shall be continuing in nature and shall remain in full force and effect without interruption;
- That the Covenant of Nondiscrimination shall be incorporated by reference into any contract or portion thereof which the Supplier may hereafter obtain; and
- That the failure of the Supplier to satisfactorily discharge any of the promises of nondiscrimination as made and set forth herein shall constitute a material breach of contract. M.C.L. 4.46.070

Contingent Fees: It is a breach of ethical standards for a person to be retained, or to retain a person, to solicit or secure a Metro contract upon an agreement or understanding for a contingent commission, percentage, or brokerage fee, except for retention of bona fide employees or bona fide established commercial selling agencies for the purpose of securing business. After first being duly sworn according to law, the undersigned Affiant states that the Contractor has not retained anyone in violation of the foregoing. M.C.L. 4.48.080

Iran Divestment Act Affidavit: By submission of this offer and in response to the solicitation, Contractor(s) and each person signing on behalf of Contractor(s) affirm, under penalty of perjury, that to the best of their knowledge and belief, neither the Contractor(s), nor proposed subcontractors, subconsultants, partners and any joint venturers, are on the list created pursuant to the Tennessee Code Annotated § 12-12-106 (Iran Divestment Act). Referenced website:

https://www.tn.gov/content/dam/tn/generalservices/documents/cpo/library/2022/List_of_persons_pursuant_to_Tenn._Code_Ann._12-12-106_Iran_Divestment_Act_updated_with%20NY05.04.22.pdf

Sexual Harassment: Affiant affirms that should it be awarded a contract with the Metropolitan Government for a period of more than twelve (12) months and/or valued at over five hundred thousand ($500,000) dollars, affiant shall be required to provide sexual harassment awareness and prevention training to its employees if those employees:

1. Have direct interactions with employees of the Metropolitan Government through email, phone, or in-person contact on a regular basis;
2. Have contact with the public such that the public may believe the contractor is an employee of the Metropolitan Government, including but not limited to a contractor with a phone number or email address associated with Metropolitan government or contractors with uniforms or vehicles bearing insignia of the Metropolitan Government; or
3. Work on property owned by the metropolitan government.

Such training shall be provided no later than (90) days of the effective date of the contract or (90) days of the employee's start date of employment with affiant if said employment occurs after the effective date of the contract. M.C.L. 2.230.020.

Affiant affirms that Contractor is not currently, and will not for the duration of the awarded Contract, engage in a boycott of Israel for any awarded contract that meets the following criteria:

- Has total potential value of two hundred fifty thousand ($250,000) or more;
- Affiant has ten (10) or more employees.

Affiant affirms that offeror is and will remain in compliance with the provisions of Chapter 4.12 of the Metro Procurement Code and the contents of its offer as submitted. Affiant further affirms that offeror understands that failure to remain in such compliance shall constitute a material breach of its agreement with the Metropolitan Government.

And Further Affiant Sayeth Not:

Organization Name: _____

Organization Officer Signature: _____

Name of Organization Officer: _____

Title: _____

Acceptable Use and External-Facing Services Policy

1. Scope

A. This Acceptable Use and External Facing Services Policy ("Policy") applies to customers' use of all services offered by Salesforce, Inc. or its affiliates ("Salesforce"). Capitalized terms used below but not defined in this policy have the meaning set forth in the Main Services Agreement ("MSA").

2. Last Updated

A. January 3, 2023

3. Changes to Policy

A. Salesforce may change this Policy by posting an updated version of the Policy at www.salesforce.com and such updates will be effective upon posting.

4. Violations

A. A customer's violation of this Policy will be considered a material breach of the MSA and/or other agreement governing the customer's use of the services.

5. Prohibited Material

A. Customers may not, and may not allow any third party, including its users, to use services to display, store, process, or transmit, or permit use of services to display, store, process, or transmit:

I. Material that infringes or misappropriates a third party's intellectual property or proprietary rights;

II. Hate-related or violent material, and/or material advocating discrimination against individuals or groups;

III. Obscene, excessively profane material or otherwise objectionable material;

IV. Material advocating or advancing criminal hacking, cracking, or phishing;

V. Material related to illegal drugs or paraphernalia;

VI. Malicious material;

VII. Unlawful software;

VIII. Malicious code, such as viruses, worms, time bombs, Trojan horses, and other harmful or malicious files, scripts, agents, or programs; or

IX. Material that violates, encourages, or furthers conduct that would violate any applicable laws, including any criminal laws, or any third-party rights, including publicity or privacy rights.

6. Prohibited Actions

A. Customers may not use a service to, nor allow its users or any third party to use a service to:

I. Generate or facilitate unsolicited commercial email (spam). Such prohibited activity includes, but is not limited to:

a. Sending communications or email in violation of the CAN-SPAM Act or any other applicable anti- spam law or regulation;

b. Imitating or impersonating Salesforce, another person or his, her, or its email address, or creating false accounts for the purpose of sending spam;

c. Mining data or harvesting any web property (including any External-Facing Service) to find email addresses or other user account information;

d. Sending unauthorized mail via open, third-party servers;

e. Sending email to users who have requested to be removed from a mailing list;

f. Selling to, exchanging with, sharing with, or distributing to a third party personal information, including the email addresses of any person without such person's knowing and continued consent to such disclosure; or

g. Sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no preexisting relationship;

II. Send, upload, distribute, or disseminate, or offer to do the same, with respect to unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, excessively profane, hateful, violent, or otherwise objectionable material, or promote, support, or facilitate unlawful, hateful, discriminatory, or violent causes;

III. Intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature;

IV. Conduct or forward multi-level marketing, such as pyramid schemes and the like;

V. Generate or facilitate SMS, MMS, or other text messages or push notifications in violation of the Telephone Consumer Protection Act, the Do-Not-Call Implementation Act, or any other applicable law including anti- spam, telemarketing, or telephone consumer protection laws or regulations;

VI. Use the services in any manner that violates any applicable industry standards, third-party policies, or requirements that Salesforce may communicate to its users, including all of the applicable guidelines published by the CTIA, the Mobile Marketing Association, the Self-Regulatory Principles as directed by the Digital Advertising Alliance and the Network Advertising Initiative, or any other generally accepted industry associations, carrier guidelines, or other industry standards;

VII. Transmit material that may be harmful to minors;

VIII. Illegally transmit another's intellectual property or other proprietary information without such owner's or licensor's permission;

IX. Impersonate another person, entity, or Salesforce (via the use of an email address or otherwise) or otherwise misrepresent themselves or the source of any communication;

X. Violate the rights (such as rights of privacy or publicity) of others;

XI. Promote, facilitate, or encourage illegal activity;

XII. Intentionally or unintentionally interfere with the availability of the service for other users, including, but not limited to, engaging in usage practices prohibited by the Documentation;

XIII. Mislead people about voting processes or census processes;

XIV. Engage in activity in connection with illegal peer-to-peer file sharing;

XV. Engage in or promote gambling, or run a gambling operation;

XVI. "Mine" bitcoins and other cryptocurrencies;

XVII. Sell, distribute, or export illegal or prescription drugs or other controlled substances or paraphernalia;

XVIII. Operate an "open proxy" or any other form of Internet proxy service that is capable of forwarding requests to any end user or third-party-supplied Internet host;

XIX. Perform significant load or security testing without first obtaining Salesforce's written consent;

XX. Remove any copyright, trademark, or other proprietary rights notices contained in or on the service or reformat or frame any portion of the web pages that are part of the service's administration display;

XXI. Access a third-party web property for the purposes of web scraping, web crawling, web monitoring, or other similar activity through a web client that does not take commercially reasonable efforts to identify itself via a unique User Agent string describing the purpose of the web client and obey the robots exclusion standard (also known as the robots.txt standard), including the crawl-delay directive;

XXII. Use a service in any manner that would disparage Salesforce;

XXIII. Use the Einstein Bot, or similar features, to communicate with any third party without clearly communicating that the individual is speaking with a bot;

XXIV. Use any product that incorporates artificial intelligence, for example, Einstein Vision, Einstein Language, Einstein Discovery, Einstein Prediction Builder, or Customer Data Platform (CDP), for the purposes of predicting an individual's racial or ethnic origin, and past, current, or future political opinions, religious or philosophical beliefs, trade union membership, age, gender, sex life, sexual orientation, disability, health status, medical condition, financial status, criminal convictions, or likelihood to engage in criminal acts. The previous sentence does not limit or prohibit use cases or tools designed specifically to identify security breaches, unauthorized access, fraud, and other security vulnerabilities. Additionally, customer may not submit images of individuals for the purposes of creating or analyzing biometric identifiers, such as face prints or fingerprints or scans of eyes, hands, or facial geometry;

XXV. Use any product that incorporates artificial intelligence, for example, Sales Cloud Einstein, Pardot Einstein, Salesforce Inbox, Einstein Engagement Scoring, Einstein Vision, Einstein Language, Einstein Bots, Service Cloud Einstein, Einstein Discovery, Einstein Prediction Builder, or Customer Data Platform (CDP), as part of a decision-making process with legal or similarly significant effects, unless customer ensures that the final decision is made by a human being. In this case, customer must take account of other factors beyond the Services' recommendations in making the final decision; or

XXVI. Directly manage, as the primary operator, private, for-profit prison facilities or detention centers in the United States. For-profit prisons and detention centers refer to privately owned facilities in which persons are incarcerated or otherwise involuntarily confined for purposes of execution of a punitive sentence imposed by a court or detention pending a trial, hearing, or other judicial or administrative proceeding.

B. Worldwide, customers may not use a service to commercially advertise or sell of any of the following firearms and/or related accessories to private citizens. Firearms: automatic firearms; semi-automatic firearms that have the capacity to accept a detachable magazine and any of the following: thumbhole stock, folding or telescoping stock, grenade launcher or flare launcher, flash or sound suppressor, forward pistol grip, pistol grip (in the case of a rifle) or second pistol grip (in the case of a pistol), barrel shroud; semi-automatic firearms with a fixed magazine that can accept more than 10 rounds; ghost guns; 3D printed guns; firearms without serial numbers; .50 BMG rifles; firearms that use .50 BMG ammunition. Firearm Parts: magazines capable of accepting more than 10 rounds; flash or sound suppressors; multi-burst trigger devices; grenade or rocket launchers; 80% or unfinished lower receivers; blueprints for ghost guns; blueprints for 3D printed guns; barrel shrouds; thumbhole stocks; threaded barrels capable of accepting a flash suppressor or sound suppressor.

7. U.S. Digital Millennium Copyright Act or Similar Statutory Obligations

A. To the extent a customer uses the services for hosting, advertising, sending electronic messages, or for the creation and hosting of, or for posting material on, websites, each customer must:

I. Comply with any notices received under Title II of the Digital Millennium Copyright Act of 1998 (Section 512 of the U.S. Copyright Act) or similar statute in other countries (the "DMCA");

II. Set up a process to expeditiously respond to notices of alleged infringement that comply with the DMCA and to implement a DMCA-compliant repeat infringers policy;

III. Publicly display a description of its notice and takedown process under the DMCA on its instance of the services; and

IV. Comply with such processes, policy(ies), and description.

B. It is Salesforce's policy to respond expeditiously to valid notices of claimed copyright infringement compliant with the DMCA. In appropriate circumstances, Salesforce will terminate the accounts of customers who Salesforce suspects to be repeatedly or blatantly infringing copyrights.

C. If Salesforce receives a notice alleging that material on a customer's instance of a service infringes another party's intellectual property, Salesforce may disable that customer's instance of the service or remove the allegedly infringing material. If Salesforce receives more than one such notice for the same customer, Salesforce reserves the right to immediately terminate such customer's subscriptions to the services as deemed necessary by Salesforce to ensure continued protection under the safe harbor provisions under the DMCA or to prevent violations of other applicable laws or third parties' rights.

Acquia

SUBSCRIPTION AND SERVICES AGREEMENT

This subscription and services agreement (the "**Agreement**"), the relevant terms of the Documentation, and any executed Orders and/or SOWs between the parties, are incorporated herein and shall govern the provision of the Services. Customer and its Affiliates may place orders under this Agreement by submitting separate Order(s) and SOW(s). This Agreement shall commence on the Effective Date of Customer's first executed Order or SOW ("**Effective Date**") and will continue until otherwise terminated in accordance with Section 12 below.

1. DEFINITIONS.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes hereof, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Ancillary Programs" means certain enabling software or tools, which Acquia makes available to Customer for download as part of the Subscription Services for purposes of facilitating Customer access to, operation of, and/or use with the Subscription Services.

"**Authorized Contractors**" means independent contractors, licensors, or subcontractors.

"**Customer Applications**" means all software programs, including without limitation Drupal, Node.js, and Magento, that Customer uses on the cloud platform comprising part of the Subscription Services. Subscription Services do not fall within the meaning of Customer Applications.

"**Customer Data**" means all data, records, files, images, graphics, audio, video, photographs, reports, forms and other content and material, in any format, that are submitted, stored, posted, displayed, transmitted, or otherwise used by or for Customer to the Subscription Services.

"**Data Center Region**" refers to the geographic region in which the Customer Data is housed.

"Deliverable" means any work product, deliverables, programs, interfaces, modifications, configurations, reports, or documentation developed or delivered in the performance of Professional Services.

"**Documentation**" means Acquia's product guides and other end user documentation for the Subscription Services and Ancillary Programs available online and through the help feature of the Subscription Services, as may be updated by Acquia from time to time to reflect the then-current Subscription Services.

"**Order**" or "**Order Form**" means an ordering document or online order specifying the Services to be provided hereunder that is entered into between Acquia and Customer from time to time, including any addenda and supplements thereto. Customer Affiliates may purchase Services subject to this Agreement by executing Orders hereunder.

"Professional Services" means fee-based migration, implementation, training or consulting services that Acquia performs as described in an Order or SOW, but excluding Support Services.

"**Services**" means the Subscription Services and Professional Services that Customer may purchase under an Order or SOW.

"Statement of Work" or "SOW" means a statement of work entered into and executed by the parties describing Professional Services to be provided by Acquia to Customer.

"Subscription Services" means the cloud platform made available by Acquia to Customer, the software made available by Acquia to Customer online via the applicable customer logins and/or associated Support Services, as ordered by Customer under an Order, as applicable.

"Support Services" means the level of support services purchased by Customer pursuant to an Order.

"Subscription Term" means the term of Subscription Services purchased by Customer which shall commence on the start date specified in the applicable Order and continue for the subscription term specified therein and any renewals thereto.

"**Trial Services**" means any Acquia product, service or functionality that may be made available by Acquia to Customer to try at Customer's option, at no additional charge, and which is designated as "beta," "trial," "non-GA," "pilot," "developer preview," "non-production," "evaluation," or by a similar designation.

"Third Party Marketplace" means any non-Acquia products or services made available as an accommodation through Acquia's website, which are subject to change during the Subscription Term.

2. SUBSCRIPTION SERVICES

2.1. Provision of Subscription Services. Acquia will make the Subscription Services available to Customer pursuant to this Agreement, the Documentation, and the relevant Order Form during the Subscription Term, solely for Customer's internal business purposes. Acquia's Affiliates and its Authorized Contractors may perform certain aspects of the Services and access Customer Data and Customer Applications provided that Acquia remain fully liable for same and responsible for ensuring that any of Acquia's obligations under this Agreement performed by its Affiliates and its Authorized Contractors are carried out in accordance with this Agreement. Customer's Affiliates and its Authorized Contractors may access certain aspects of the Services hosted or provided through such Services provided that Customer remain fully liable for same and responsible for ensuring that any of Customer's obligations under this Agreement performed by its Affiliates and its Authorized Contractors are carried out in accordance with this Agreement. Customer's use of the Subscription Services includes the right to access all functionality available in the Subscription Services during the Subscription Term. So long as Acquia does not materially degrade the functionality, as described in the Documentation, of the Subscription Services during the applicable Subscription Term (i) Acquia may modify the systems and environment used to provide the Subscription Services to reflect changes in technology, industry practices and patterns of system use, and (ii) update the Documentation accordingly. Subsequent updates, upgrades, enhancements to the Subscription Services made generally available to all subscribing customers will be made available to Customer at no additional charge, but the purchase of Subscription Services is not contingent on the delivery of any future functionality or features. New features, functionality or enhancements to the Subscription Services may be marketed separately by Acquia and may require the payment of additional fees. Acquia will determine, in its sole discretion, whether access to such new features, functionality or enhancements will require an additional fee.

2.2 Trial Services. If Customer registers or accepts an invitation for Trial Services, including through Acquia's website, or executes an Order for the same, Acquia will make such Trial Services available to Customer on a trial basis, free of charge, until the earlier of (a) the end of the free trial period for which Customer registered to use the applicable Trial Services, or (b) the end date specified in the applicable Order. Trial Services are provided for evaluation purposes and not for production use. Customer shall have sole

responsibility and Acquia assumes no liability for any Customer Data that Customer may choose to upload on the Trial Services. Trial Services may contain bugs or errors, and may be subject to additional terms. TRIAL SERVICES ARE NOT CONSIDERED "SERVICES" HEREUNDER AND ARE PROVIDED "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTY AND ACQUIA SHALL HAVE NO INDEMNIFICATION OBLIGATIONS NOR LIABILITY OF ANY TYPE WITH RESPECT TO THE TRIAL SERVICES. Acquia may, in its sole discretion, discontinue Trial Services at any time.

2.3. Third Party Marketplace. As part of the Subscription Services, Acquia may provide access to the Third Party Marketplace solely as an accommodation to Customer. Customer may choose to use any, all or none of the offerings on such Third Party Marketplace at its sole discretion. Customer's use of any offering on the Third Party Marketplace is subject to the applicable provider's terms and conditions and any such terms and conditions associated with such use are solely between Customer and such third party provider. Acquia does not provide any Support Services for Third Party Marketplace products and services.

2.4 Ancillary Programs. As part of the Subscription Services, Acquia may provide Customer with access to download certain Ancillary Programs for use with the Subscription Services. Acquia grants Customer during the Subscription Term a non-exclusive, non-transferable non-assignable, limited licensed to use such Ancillary Programs in object code (machine readable) format only on each site hosted by Acquia under an Order for Subscription Service to facilitate Customer access to, operation of, and/or use of the Subscription Services subject to the terms of this Agreement. Ancillary Programs shall only be used to upload, download and synchronize files between Customer's computer or other Customer owned or controlled devices and the Subscription Services.

3. SECURITY AND DATA PRIVACY

3.1. Security and Internal Controls. In accordance with Acquia's Security Annex incorporated herein by reference, Acquia shall (i) maintain a security framework of policies, procedures, and controls that includes administrative, physical, and technical safeguards for protection of the security and integrity of the Subscription Services, and of the Customer Data contained within the Subscription Services, using the capabilities of currently available technologies and in accordance with prevailing industry practices and standards, (ii) access and use the Customer Data solely to perform its obligations in accordance with the terms of this Agreement, and (iii) perform periodic testing by independent third party audit organizations, which include with Service Organization Controls 1 (SOC 1), SOC 2 audits and ISO 27001 certification or surveillance audits performed annually. In no event during the Subscription Term shall Acquia materially diminish the protections provided by the controls set forth in Acquia's then-current Security Annex.

3.2. Data Privacy. In performing the Subscription Services, Acquia will comply with the Acquia Privacy Policy incorporated herein by reference. The Acquia Privacy Policy is subject to change at Acquia's discretion; however, Acquia policy changes will not result in a material reduction in the level of protection provided for Customer Data during the Subscription Term. Except with respect to Trial Services, the terms of the Acquia GDPR Data Processing Addendum ("DPA") are hereby incorporated by reference and shall apply to the extent Customer Data includes Personal Data, as defined in the DPA. To the extent Customer's use of the Subscription Services includes the processing of Customer Data by Acquia that are subject to the General Data Protection Regulation (EU) 2016/679 or the UK GDPR, as defined in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (jointly "GDPR"), such data processing by Acquia as data processor complies with the requirements of the aforementioned regulation and any Personal Data transfer out of the European Union, the European Economic Area, the United Kingdom, and Switzerland shall be governed by the Standard Contractual Clauses as attached to the DPA, unless the Customer has opted out of those clauses. For the purposes of the Standard Contractual Clauses, Customer and its applicable Affiliates are each the data exporter, and Customer's acceptance of this Agreement, and an applicable Affiliate's execution of an Order Form, shall be treated as its execution of the Standard Contractual Clauses and Appendices. Where Customer's use of the Subscription Services includes the processing of California Consumer's Personal Information by Acquia that are subject to the California Consumer Protection Act of 2018, and its implementing regulations, as amended or superseded from time to time ("CCPA"), such data processing by Acquia as a "service provider" complies with the requirements of the CCPA. Acquia shall process personal data and personal information on behalf of and in accordance with Customer's instructions consistent with this Agreement and as necessary to provide the Subscription Services and will reasonably cooperate with Customer in its efforts to respond to requests by data subjects and/or California Consumers to exercise their rights under the GDPR or CCPA and to otherwise comply with the GDPR or CCPA.

3.3. Data Center Region. Customer may select the Data Center Region from those available for the applicable Subscription Services. Acquia will not move the selected Data Center Region and the Customer Data contained within such Data Center Region, without Customer's written consent or unless required to comply with the law or requests of a governmental or regulatory body (including subpoenas or court orders). Customer consents to Acquia's storage of Customer Data in, and transfer of Customer Data into, the Data Center Region Customer selects.

3.4. Compliance with Law. Acquia will comply with all laws applicable to the provision of the Subscription Services, including applicable security breach notification laws, but not including any laws applicable to the Customer's industry that is not generally applicable to information technology services providers.

4. CUSTOMER OBLIGATIONS

4.1. Responsibilities. Customer shall (i) access and use the Services in accordance with this Agreement, applicable laws and government regulations and Acquia's Acceptable Use Policy incorporated herein by reference, (ii) use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify Acquia promptly of any such unauthorized access or use, and (iii) take commercially reasonable steps necessary to ensure the security and compliance of the Customer Applications.

4.2. Customer Data. Customer has and shall maintain all rights as are required to allow Acquia to provide the Subscription Services to Customer as set forth in this Agreement, including without limitation to send the Customer Data to Acquia pursuant to this Agreement and to allow Acquia to access, use, and store Customer Data to provide the Subscription Services pursuant to this Agreement. Customer is responsible for its legal and regulatory compliance in its use of any Subscription Services and shall make Acquia aware of any Customer Data processed, stored, or transmitted through the Subscription Services for which regulations other than those set forth in the Security Annex apply. If, in the course of providing Subscription Services, Acquia agrees in writing to process such Customer Data and Customer has subscribed to any applicable Subscription Services, Acquia shall process it only as permitted under this Agreement and in compliance with data protection legislation to which Acquia is subject as a service provider.

4.3 Restrictions. Customer shall not (i) license, sublicense, sell, resell, rent, lease, transfer, distribute or otherwise similarly exploit the Subscription Services or Ancillary Programs), (ii) use or permit others to use any security testing tools in order to probe, scan or attempt to penetrate or ascertain the security of the Subscription Services, (iii) copy, create a derivative work of reverse engineer, reverse assemble, disassemble, or decompile the Subscription Services, Ancillary Programs, or any part thereof or otherwise attempt to discover any source code or modify the Subscription Services or the Ancillary Programs), (iv) create a competitive offering based on the

Subscription Services, and (v) disclose any benchmark or performance tests of the Subscription Services.

5. PROFESSIONAL SERVICES

5.1. Standard Professional Services. A description of Acquia's standard Professional Services offerings, including training, and workshops, may be found in the Documentation. Standard Professional Services may be identified in an Order without the need for issuance of an SOW.

5.2. Other Professional Services. For any non-standard Professional Services, Acquia will provide Customer with Professional Services as set forth in the applicable SOW. Each SOW will include, at a minimum (i) a description of the Professional Services and any Deliverable to be delivered to Customer; (ii) the scope of Professional Services; (iii) the schedule for the provision of such Professional Services; and (iv) the applicable fees and payment terms for such Professional Services, if not specified elsewhere.

5.3. Change Orders. Changes to an SOW or Order Form will require, and shall become effective only when, fully documented in a written change order (each a "**Change Order**") signed by duly authorized representatives of the parties prior to implementation of the changes. Such changes may include, for example, changes to the scope of work and any corresponding changes to the estimated fees and schedule. Change Orders shall be deemed part of, and subject to, this Agreement.

5.4. Designated Contact and Cooperation. Each party will designate in each SOW an individual who will be the primary point of contact between the parties for all matters relating to the Professional Services to be performed thereunder. Customer will cooperate with Acquia, will provide Acquia with accurate and complete information, will provide Acquia with such assistance and access as Acquia may reasonably request, and will fulfill its responsibilities as set forth in this Agreement and the applicable SOW. If applicable, while on Customer premises for Professional Services, Acquia personnel shall comply with reasonable Customer rules and regulations regarding safety, conduct, and security made known to Acquia.

6. FEES AND PAYMENT

6.1. Fees. Customer shall pay all fees specified in each Order and SOW and any applicable additional fees if Customer exceeds the allotted capacity or other applicable limits specified in the Order. Except as otherwise specified herein or in an Order or SOW (i) fees are payable in United States dollars, (ii) fees are based on Services purchased, regardless of usage, (iii) payment obligations are non-cancelable and fees paid are non-refundable, (iv) all Services shall be deemed accepted upon delivery, and (v) the Subscription Services purchased cannot be decreased during the relevant Subscription Term. Customer shall reimburse Acquia for out-of-pocket expenses incurred by Acquia in connection with its performance of Services. Acquia will provide Customer with reasonably detailed invoices for such expenses. All amounts payable under this Agreement will be made without setoff or counterclaim, and without any deduction or withholding.

6.2. Invoicing and Payment. Unless otherwise specified in an Order, fees for Subscription Services specified in an Order will be invoiced annually in advance, fees for overages will be calculated and invoiced monthly in arrears, and, unless otherwise set forth in an SOW, all fees and expenses for standard Professional Services as described in Section 5.1 shall be invoiced upon completion, and all fees and expenses for non-standard Professional Services as described in 5.2 will be invoiced monthly in arrears on a time and materials basis. Except as otherwise stated in the applicable Order or SOW, Customer agrees to pay all invoiced amounts within thirty (30) days of invoice date. If Customer fails to pay any amounts due under this Agreement by the due date, in addition to any other rights or remedies it may have under this Agreement or by matter of law (i) Acquia reserves the right to suspend the Subscription Services upon thirty (30) days' notice, until such amounts are paid in full Acquia will not exercise its right to charge interest if the applicable charges are under reasonable and good faith dispute and Customer is cooperating diligently to resolve the issue.

6.3. Taxes. Fees for Services exclude all sales, value added and other taxes and duties imposed with respect to the sale, delivery, or use of any product or Services covered hereby. Unless Customer provides a valid, signed certificate or letter of exemption for each respective jurisdiction of its tax-exempt status, Customer is responsible for payment of all taxes, levies, duties, assessments, including but not limited to value-added, sales, use or withholding taxes, assessed or collected by any governmental body (collectively, "**Taxes**") arising from Acquia's provision of the Services hereunder, except any taxes assessed on Acquia's net income. If Acquia is required to directly pay or collect Taxes related to Customer's use or receipt of the Services hereunder, Customer agrees to promptly reimburse Acquia for any amounts paid by Acquia.

7. PROPRIETARY RIGHTS

7.1. Subscription Services. Except for the rights expressly granted under this Agreement, Acquia and its licensors retain all right, title and interest in and to the Subscription Services and Documentation, including all related intellectual property rights therein. Acquia reserves all rights in and to the Subscription Services and Documentation not expressly granted to Customer under this Agreement. Customer will not delete or in any manner alter the copyright, trademark, and other proprietary notices of Acquia.

7.2 Ancillary Programs, Third Party Software. The Subscription Services (including Ancillary Programs) may interoperate with certain software products, including open-source software, owned by third parties and licensed directly to the Customer by such third party ("**Third Party Software**"). Such Third Party Software is provided to the Customer without liability or obligation by Acquia and is governed by a license agreement directly between the Customer and the respective owner of the Third Party Software. Such license agreement may be found in the relevant section of the user interface subdirectory available through the Documentation.

7.3. Customer Data and Customer Applications. As between Customer and Acquia, Customer is and will remain the sole and exclusive owner of all right, title and interest to all Customer Data and Customer Applications, including any intellectual property rights therein. Customer hereby grants Acquia, its Affiliates and applicable Authorized Contractors all necessary rights to host, use, process, store, display and transmit Customer Data and Customer Applications solely as necessary for Acquia to provide the Services in accordance with this Agreement. By using Ancillary Programs Customer grants Acquia permission to access Customer's computer or other devices to the extent necessary in enabling Ancillary Programs. Customer represents that it has, and warrants that it shall maintain, all rights as required to allow Acquia to compile, use, store, and retain aggregated Customer Data, including without limitation in combination with other Acquia customers' data, for internal or marketing uses (provided that no such marketing use shall include any information that can identify Customer or its customers). Subject to the limited licenses granted herein, Acquia acquires no right, title or interest from Customer or Customer licensors hereunder in or to Customer Data and Customer Applications, including any intellectual property rights therein. Customer reserves all rights in and to the Customer Data that are not expressly granted to Acquia pursuant to this Agreement.

7.4. Deliverables. Excluding any property that constitutes Outside Property, any Deliverables shall be the sole property of Customer upon Customer's payment in full of all associated Professional Services fees. Acquia shall execute and, at Customer's written request, require its personnel to execute any document that may be necessary or desirable to establish or perfect Customer's rights to the ownership of such Deliverables. For purposes of this Agreement, "**Outside Property**" means any and all technology and information, methodologies, data, designs, ideas, concepts, know-how,

techniques, user-interfaces, templates, documentation, software, hardware, modules, development tools and other tangible or intangible technical material or information that Acquia possesses or owns prior to the commencement of Professional Services or which it develops independent of any activities governed by this Agreement, and any derivatives, modifications or enhancements made to any such property. Outside Property shall also include any enhancements, modifications or derivatives made by Acquia to the Outside Property while performing Professional Services hereunder, and any software, modules, routines or algorithms which are developed by Acquia during the term in providing the Professional Services to Customer, provided such software, modules, routines or algorithms have general application to work performed by Acquia for its other customers and do not include any content that is specific to Customer or which, directly or indirectly, incorporate or disclose Customer's Confidential Information.

7.5. Outside Property License. To the extent that Acquia incorporates any Outside Property into any Deliverables, then Acquia hereby grants Customer a limited, royalty-free, non-exclusive, non-transferable (subject to Section 14.11), without right to sublicense, license to use such Outside Property delivered to Customer solely as necessary for and in conjunction with Customer's use of the Deliverables.

8. CONFIDENTIALITY

8.1. Definition of Confidential Information. "**Confidential Information**" means all confidential or proprietary information of a party ("**Disclosing Party**") disclosed to the other party ("**Receiving Party**"), whether orally or in writing, that is designated as confidential or reasonably should be understood to be confidential given the nature of information and the circumstances of disclosure. Without limiting the coverage of these confidentiality obligations, the parties acknowledge and agree that Confidential Information of each party shall include related benchmark or similar test results, other technology and technical information, security information, security audit reports, and business and marketing plans, except that Acquia may reference and use Customer's name, logos and the nature of the Services provided hereunder in Acquia's business development and marketing efforts.

8.2. Exceptions. Confidential Information shall not include information that (i) is or becomes publicly available without a breach of any obligation owed to the Disclosing Party, (ii) is already known to the Receiving Party at the time of its disclosure by the Disclosing Party, without a breach of any obligation owed to the Disclosing Party, (iii) following its disclosure to the Receiving Party, is received by the Receiving Party from a third party without breach of any obligation owed to Disclosing Party, (iv) is independently developed by Receiving Party without reference to or use of the Disclosing Party's Confidential Information or (v) information that is disclosed pursuant to law

8.3. Protection of Confidential Information. The Receiving Party shall use the same degree of care used to protect the confidentiality of its own Confidential Information of like kind (but in no event less than reasonable care), and, except with Disclosing Party's written consent, shall (i) not use any Confidential Information of Disclosing Party for any purpose outside the scope of this Agreement and (ii) limit access to Confidential Information of Disclosing Party to those of its and its Authorized Contractors, Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have a duty or obligation of confidentiality no less stringent than that set forth herein.

8.4. Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent required by applicable law, regulation or legal process, provided that the Receiving Party (i) provides prompt written notice to the extent legally permitted, (ii) provides reasonable assistance, in the event the Disclosing Party wishes to oppose the disclosure, and (iii) limits disclosure to that required by law, regulation or legal process.

9. REPRESENTATIONS, WARRANTIES AND DISCLAIMERS

9.1. Acquia Representations & Warranties. Acquia represents and warrants that (i) Acquia has the legal authority to enter into this Agreement, (ii) the Subscription Services will materially conform with the relevant Documentation, (iii) the functionality and security of the Subscription Services will not be materially decreased during a Subscription Term, and (iv) Professional Services will be performed in a competent and workmanlike manner consistent with generally accepted industry standards.

9.2. Remedies. For any failure of any Subscription Services or Professional Services, as applicable, to conform to their respective warranties, to the extent permitted by state law, Acquia's liability and Customer's sole and exclusive remedy shall be for Acquia, in the case of a breach of the warranty set forth in Section 9.1 (ii), (iii), and/or (iv), to use commercially reasonable efforts to correct such failure; or, in the case of a breach of the warranty set forth in Section 9.1 (iv) to re-perform the affected Professional Services. If the foregoing remedies are not commercially practicable, Acquia may, in its sole discretion, terminate the applicable Order or SOW upon providing Customer with written notice thereof, and, as Customer's sole and exclusive remedy, refund to Customer
(a) in the case of breach of the warranty set forth in Section 9.1(ii) or (iii), any Subscription Services fees paid by Customer with respect to the unexpired portion of the current Subscription Term for the non-conforming Subscription Services; or (b) in the case of breach of the warranty set forth in Section 9.1(iv), any fees paid by Customer for the portion of Professional Services giving rise to the breach.

9.3. Customer Representations & Warranties. Customer represents and warrants that (i) it has the legal authority to enter into this Agreement, and (ii) it will use the Services in accordance with the terms and conditions set forth in this Agreement and in compliance with all applicable laws, rules and regulations.

9.4. Disclaimer. TO THE EXTENT PERMITTED BY STATE LAW, EXCEPT AS EXPRESSLY PROVIDED HEREIN, ACQUIA MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, ORAL OR WRITTEN, STATUTORY OR OTHERWISE, AND ACQUIA HEREBY DISCLAIMS ALL IMPLIED WARRANTIES AND CONDITIONS, INCLUDING, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY WITH RESPECT TO THE QUALITY, PERFORMANCE, ACCURACY OR FUNCTIONALITY OF THE SERVICES OR THAT THE SERVICES ARE OR WILL BE ERROR FREE OR WILL ACCOMPLISH ANY PARTICULAR RESULT.

10. MUTUAL INDEMNIFICATION

10.1. Indemnification by Acquia. Acquia shall indemnify, defend and hold Customer harmless from and against any judgments, settlements, costs and fees reasonably incurred (including reasonable attorney's fees) resulting from any claim, demand, suit, or proceeding made or brought against Customer by a third party alleging that the use of the Subscription Services hereunder infringes or misappropriates the valid intellectual property rights of a third party (a "**Claim Against Customer**"); provided that Customer (a) promptly gives Acquia written notice of the Claim Against Customer; (b) gives Acquia sole control of the defense and settlement of the Claim Against Customer (provided that Acquia may not settle any Claim Against Customer unless the settlement unconditionally releases Customer of all liability and provided that Customer cannot be bound by any settlement absent approval of the Metropolitan Council); and (c) provides to Acquia all reasonable assistance, at Acquia's expense. In the event of a Claim Against Customer, or if Acquia reasonably believes the Subscription Services may infringe or misappropriate, Acquia may in Acquia's sole discretion and at no cost to Customer (i) modify the Subscription Services so that they no longer infringe or misappropriate, without breaching Acquia's warranties hereunder, (ii) obtain a license for Customer's continued use of Subscription Services in accordance with this Agreement, or (iii) terminate Customer's subscriptions for such Subscription Services and refund to Customer any prepaid fees covering the remainder of the term of such subscriptions after the effective date of termination. Notwithstanding the foregoing, Acquia shall have no obligation to indemnify, defend, or hold Customer harmless

from any Claim Against Customer to the extent it arises from (i) Customer Data or Customer Applications, (ii) use by Customer after notice by Acquia to discontinue use of all or a portion of the Subscription Services, (iii) use of Services by Customer in combination with equipment or software not supplied by Acquia where the Service itself would not be infringing, (iv) or Customer's breach of this Agreement.

10.2. Indemnification by Customer. To the extent permitted by state law, Customer shall indemnify, defend and hold Acquia harmless from and against any judgments, settlements, costs and fees reasonably incurred (including reasonable attorney's fees) resulting from any claim, demand, suit or proceeding made or brought against Acquia by a third party alleging that Customer Data or Customer Application violates applicable law or a third party's rights (a "**Claim Against Acquia**"); provided that Acquia (a) promptly gives Customer written notice of the Claim Against Acquia; (b) gives Customer sole control of the defense and settlement of the Claim Against Acquia (provided that Customer may not settle any Claim Against Acquia unless the settlement unconditionally releases Acquia of all liability); and (c) provides to Customer all reasonable assistance, at Customer's expense.

10.3. Exclusive Remedy. This Section 10 states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of claim described in this Section.

11. LIMITATION OF LIABILITY

11.1. Limitation of Liability. To the extent permitted by state law, EXCEPT FOR (I) EACH PARTY'S OBLIGATIONS SET FORTH IN SECTION 10 (MUTUAL INDEMNIFICATION), (II) INFRINGEMENT OR MISAPPROPRIATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, INCLUDING TRADE SECRETS, (III) DAMAGES FOR BODILY INJURY, DEATH, DAMAGE TO REAL OR TANGIBLE PERSONAL PROPERTY; OR (IV) ANY OTHER LIABILITY THAT MAY NOT BE LIMITED UNDER APPLICABLE LAW (THE "EXCLUDED MATTERS"), IN NO EVENT SHALL EITHER PARTY'S TOTAL AGGREGATE LIABILITY RELATING TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) EXCEED THE AMOUNT PAID OR PAYABLE BY CUSTOMER FOR THOSE SERVICES GIVING RISE TO SUCH CLAIM UNDER THE APPLICABLE ORDER FORM AND/OR SOW IN THE 12 MONTHS PRECEDING THE APPLICABLE INCIDENT.

11.2. Exclusion of Consequential and Related Damages. To the extent permitted by state law, EXCEPT FOR THE EXCLUDED MATTERS, IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

12. TERM AND TERMINATION

12.1. Term of Agreement. This Agreement commences on the Effective Date and continues until otherwise terminated, by written agreement of the parties, in accordance with Section 12.3 or upon the expiration of the last Subscription Term or renewal thereof.

12.2. Termination. A party may terminate this Agreement (or, at such party's option, the individual Order Forms or SOWs affected by the applicable breach), for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such same 30 day period, or (ii) automatically if the other party becomes the subject of a petition in bankruptcy or other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Upon termination of an Order or SOW for cause by Customer and upon Customer's written request, Acquia shall refund, on a pro rata basis, any fees paid thereunder that cover the remainder of the applicable Subscription Term after the effective date of termination. Upon termination of an Order or SOW for cause by Acquia, all amounts owed by Customer thereunder shall become due and payable. In no event shall any termination relieve Customer of the obligation to pay all fees payable to Acquia for the period prior to the effective date of termination. Upon termination of an Order Form or this Agreement for any reason, Customer's right to access and use the Subscription Services (including any Ancillary Programs) terminates. Upon such termination, Customer must (a) immediately destroy all copies of the Ancillary Programs, and (b) immediately and, upon Acquia's request, provide Acquia with written certification of such destruction.

12.3. Data Portability and Deletion. Upon request made by Customer within 7 days of termination or expiration of the Subscription Services, Acquia will make Customer Data and Customer Applications available to Customer for export or download as provided in the Documentation. At the end of such 7-day period, Acquia will delete or otherwise render inaccessible any Customer Data and Customer Applications, unless legally prohibited. Acquia has no obligation to retain the Customer Data for Customer purposes after this 7-day post termination period.

12.4. Survival. Section 7 (Proprietary Rights), 8 (Confidentiality), 9.4 (Disclaimer), 10 (Mutual Indemnification), 11 (Limitation of Liability), 12.4 (Refund upon Termination), 13 (Notices, Governing Law and Jurisdiction) and 14 (General Provisions) and any other rights and obligations of the parties hereunder that by their nature are reasonably intended to survive termination or expiration, shall survive any termination or expiration of this Agreement.

13. NOTICES, GOVERNING LAW AND JURISDICTION

13.1. Manner of Giving Notice. Except as otherwise specified in this Agreement, all legal notices of default, breach or termination ("**Legal Notices**") hereunder shall be in writing and shall be deemed to have been given upon (i) personal delivery, (ii) the fifth business day after being sent by certified mail return receipt requested, or (iii) the first business day after sending by a generally recognized international guaranteed overnight delivery service. Each party shall send all Legal Notices to the other party at the address set forth in the applicable Order Form or SOW, as such party may update such information from time to time, with, in the case of notices sent by Customer, a copy sent to the Acquia Legal Department at the address first set forth above. Billing-related notices to Customer will be addressed to the relevant billing contact designated by Customer on the applicable Order.

13.2. Governing Law and Jurisdiction. If Customer is entering into this Agreement from the UK or a European Union member country, then this Agreement is governed by the laws of England and subject to the exclusive jurisdiction of the courts of England and Wales. If Customer is entering into this Agreement from Australia, then this Agreement is governed by the laws of New South Wales and subject to the exclusive jurisdiction of the courts of Sydney. Otherwise, this Agreement shall be governed and construed in accordance with the laws of the state of Tennessee, and subject to the exclusive jurisdiction of the federal or state courts in Tennessee, without giving effect to any conflict of Law rules or principles. Each party consents to the jurisdiction of such court in any such civil action or legal proceeding and waives any objection to the laying of venue of any such civil action or legal proceeding in such court. Notwithstanding the foregoing, the parties acknowledge that any unauthorized disclosure of Confidential Information or any actual or alleged infringement of such party's or third party's intellectual property rights might cause the other party to suffer irreparable harm for which damages would be an inadequate remedy and that, in such event, the aggrieved party may seek, in addition to any other available remedies, injunctive and other equitable, without bond and without the necessity of showing actual monetary damages. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act do not apply to the Agreement.

14. GENERAL PROVISIONS

14.1. Import and Export Compliance. Each party shall comply with all applicable import, re-import, export and re-export control laws, treaties, agreements, and regulations. Export controls may include, but are not limited to, those of the Export Administration Regulations of the U.S. Department of Commerce (EAR), the Department of State International Traffic in Arms Regulations (ITAR), and country-specific economic sanctions programs implemented by the Office of Foreign Assets Control (OFAC), which may restrict or require licenses for the export of Items from the United States and their re-export from other countries. Each party represents that it is not named on any U.S. government denied-party list. Customer shall not permit users to access or use Services in a U.S.-embargoed country or in violation of any U.S. export law or regulation.

14.2. Anti-Corruption. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of the other party's employees or agents in connection with this Agreement. If a party learns of any violation of the above restriction, such party will use reasonable efforts to promptly notify the other party.

14.3. Federal Government End Use Provisions *(only applicable for the U.S.)*. If the Services are being or have been acquired with U.S. Federal Government funds, or Customer is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure or transfer of the Services, or any related documentation of any kind, including technical data, manuals or Acquia Property is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995), as applicable. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire the software and Services with only those rights set forth in this Agreement and any amendment hereto.

14.4. Subscription Service Analyses. Acquia may (i) compile statistical and other information related to the performance, operation and use of the Subscription Services, and (ii) use, and share data from the Subscription Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as 'Subscription Service Analyses"). Subscription Service Analyses will not incorporate any information, including Customer Data, in a form that could serve to identify Customer or an individual. Acquia retains all intellectual property rights in Subscription Service Analyses.

14.5. Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

14.6. Non-Solicitation. Customer agrees that during the term of each Order Form and/or SOW and for twelve (12) months thereafter, it will not recruit or otherwise solicit for employment any person employed by Acquia who participated in the performance of Services under the applicable Order Form and/or SOW. Nothing in this clause shall be construed to prohibit individual Acquia employees from responding to public employment advertisements, postings or job fairs of Customer, provided such response is not prompted by Customer intentionally circumventing the restrictions of this Section.

14.7. No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement.

14.8. Public Relations. Upon approval by Customer,Acquia may identify Customer as an Acquia customer in advertising, media relations, trade shows, the website, and other similar promotional activities, using Customer's name and trademarks in accordance with Customer's trademark guidelines. Customer shall also assist Acquia in preparing a press release announcing Customer as a new Acquia Customer, with the view to publishing within 60 days following the Effective Date and in preparing a case study for external use that details Customer's use of the Services within 6 months following the Effective Date. Acquia shall not publish such press release or case study without Customer's prior, written approval as to its contents.

14.9. Waiver. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right.

14.10. Force Majeure. Neither party shall be liable under this Agreement for delays or failures to perform the Services or this Agreement due to causes beyond its reasonable control. Such delays include, but are not limited to, fire, natural catastrophe, government legislation, acts, orders, or regulation, strikes or labor difficulties, to the extent not occasioned by the fault or negligence of the delayed party. Any such excuse for delay shall last only as long as the event remains beyond the reasonable control of the delayed party. The delayed party shall use its best efforts to minimize the delays caused by any such event beyond its reasonable control. If the force majeure event continues for more than thirty (30) calendar days, then either party may terminate the Agreement upon written notice to the other party.

14.11. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

14.12. Assignment. Neither party may assign its rights and obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of the other party. Notwithstanding the foregoing, either party may assign this Agreement in its entirety (including all Order Forms and SOWs), without consent of the other party, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors, and permitted assigns.

14.13. Entire Agreement. The Goods and Services Contract, this Agreement and the relevant addendaconstitutes the entire agreement between the parties as it relates to the subject matter and supersedes all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning or relating to the same. Except as otherwise provided herein, no modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by both parties. To the extent of any conflict or inconsistency between the provisions of the Goods and Services Contract, this Agreement, the Documentation, any Order Form or SOW, the terms of such Goods and Services Contract shall take first priority with the Order Form or SOW taking second priority. Notwithstanding any language to the contrary therein, no terms or conditions stated in a PO, payment system, other order documentation or otherwise (excluding Order Forms and/or SOWs) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void.

ACQUIA DATA PROCESSING ADDENDUM[1]

(including EU SCCs, UK IDTA, and US State Privacy Laws requirements)

This Data Processing Addendum (the "**DPA**"), which forms part of the Subscription and Services Agreement (the "**Agreement**") between Acquia and the customer specified on page of this DPA ("**Customer**"), is entered into by Acquia and Customer effective as of the last signature date below.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Customer Affiliates, if and to the extent Acquia processes Personal Data for which such Customer Affiliates qualify as the Controller. In providing the Services to Customer pursuant to the Agreement, Acquia may Process Personal Data on behalf of Customer, and the parties agree to comply with the following provisions with respect to any Personal Data. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Acquia under this DPA and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Customer Affiliate(s).

Except as modified below, the terms of the Agreement shall remain in full force and effect. Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. In case of a conflict between the terms of the DPA and the Agreement, the terms of the DPA shall prevail. This DPA supersedes and replaces all prior agreements between Customer and Acquia regarding the subject matter of this DPA.

DEFINITIONS.
In this DPA, the following terms shall have the meanings set out below:

"**Acquia**" means Acquia Inc., a company incorporated in Delaware and its primary address as 53 State Street, Boston, MA 02109, USA.

"**Acquia Affiliates**" means all Acquia Affiliates listed at https://www.acquia.com/about-us/legal/subprocessors.

"**Acquia Group**" means Acquia and Acquia Affiliates engaged in the Processing of Personal Data.

"**Annex**" herein means an appendix to the EU SCCs; as opposed to "Exhibit" which means an appendix to the DPA.

"**Controller**" means 'controller' or 'data controller' as defined in the GDPR, US State Privacy Laws, or analogous in other applicable Data Protection Laws.

"**Customer Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Acquia, but has not signed its own Order with Acquia and is not a "Customer" as defined under the Agreement.

"**Customer Group**" means Customer and any of its Customer Affiliates.

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including – where applicable – , but not limited to,

- the **GDPR** (as further defined herein and which includes the applicable regulations for the European Union, the United Kingdom, and Switzerland),
- the **US State Privacy Laws** (as further defined herein and which include, but are not limited to, the applicable laws of California, Colorado, Connecticut, Utah, and Virginia)
- the **South Africa** Protection of Personal Information Act ("**POPIA**"),

---

[1] **How to execute this DPA:**

- This DPA has been pre-signed by Acquia (end of DPA main body on **page**).
- Complete any information required in
  - The signature boxes at the end of the DPA main body on **page** ,
  - The information for the EU SCC Annexes I and II (**Exhibit 2** to this DPA)
  - The information for the UK IDTA (**Exhibit 3** to this DPA)
- Send the completed and signed DPA via email to privacy@acquia.com

- the Privacy Act 1988 of **Australia** ("**AUSPA**"),
- the **Canadian** Personal Information Protection and Electronic Documents Act ("**PIPEDA**").

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**EEA**" means the European Economic Area.

"**Exhibit**" herein means an appendix to the DPA; as opposed to "Annex" which means an appendix to the EU SCCs.

"**GDPR**" means

- **[European Union]** the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (also the "**EU GDPR**"),
- **[United Kingdom]** the "**UK GDPR**" (as defined in the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019), and
- **[Switzerland]** the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1;), and from 01 January 2023 onwards, the revised Swiss Federal Act on Data Protection of 25 September 2020 (both, as applicable, "**Swiss GDPR**").

"**Personal Data**" means all data which may be defined as 'personal data', 'personal information', 'personally identifiable information' or an analogous term as defined in the GDPR, US State Privacy Laws, or other applicable Data Protection Laws that is subjected to the Services under Customer's Agreement.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means 'processor' or 'data processor' as defined in the GDPR, US State Privacy Laws, or analogous in other applicable Data Protection Laws, including 'service provider" as that term is defined by the CCPA.

"**Product Notice**" means the respective notice describing privacy-related description of the Services, as available on Acquia's website at https://docs.acquia.com/guide/ (marked as '**GDPR Product Notice**').

"**Services**" means the services provided by Acquia to Customer as agreed in the Agreement.

"**Standard Contractual Clauses**" means

(i) where the **EU GDPR or Swiss Federal Act on Data Protection** apply, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"), as attached hereto in **Exhibit 2** ; and

(ii) (ii) where the **UK GDPR** applies, the "Standard Data Protection Clauses issued by the Commissioner under S119A(1) Data Protection 2018 – International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force 21 March 2022" ("**UK IDTA**"), as attached hereto in **Exhibit 3**.

"**Sub-processor**" means any Processor engaged by Acquia or a member of the Acquia Group.

"**Supervisory Authority**" means an independent public authority, which is established by an EU Member State pursuant to the GDPR, US Stata Privacy Laws, or other applicable Data Protection Laws.

"**US State Privacy Laws**" means the applicable privacy laws enacted by a state of the United States of America, including, but not limited to,

- the California Consumer Privacy Act of 2018 (California Civil Code §§1798.100 to 1798.199) and its implementing regulations, as amended or supplemented from time to time (the "**CCPA**");
- the California Privacy Rights Act of 2020 (2020 Cal. Legis. Serv. Proposition 24 codified at California Civil Code §§ 1798.100 et seq.), and its implementing regulations, as amended or supplemented from time to time (the "**CPRA**") [2];
- the Colorado Privacy Act, C.R.S.A. § 6-1-1301 et seq. (SB 21-190), including any implementing regulations and amendments thereto (the "**CPA**") [1];
- Connecticut Data Privacy Act, S.B. 6 (Connecticut 2022), including any implementing regulations and amendments thereto (the "**CTDPA**")[1];
- the Utah Consumer Privacy Act, Utah Code § 13-61-101 et seq. (SB 0227), including any implementing regulations

---

2 Date of the respective US State Privacy Laws coming into effect: CPRA and VCDPA: 01 January 2023; CPA and CTDPA: 01 July 2023; UCPA: 31 December 2023

and amendments thereto (the "**UCPA**")[1];

- the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-571 et seq. (SB 1392), including any implementing regulations and amendments thereto (the "**VCDPA**")[1].

1. DATA PROCESSING.

1.1 **Scope and Roles**. This DPA applies when Personal Data is Processed by Acquia as part of Acquia's provision of Services as agreed in the Agreement and the applicable Order. In this context, Customer (or a relevant Customer Affiliate) is the Controller (or, as the case may be, a Processor processing Personal Data on behalf of a third-party Controller) and Acquia is the Processor (or sub-Processor) with respect to Personal Data.

1.2 **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

1.3 **Acquia's Processing of Personal Data**. Acquia shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions as set forth in Section 2.

1.4 **Details of the Processing**. The subject matter of Processing of Personal Data by Acquia is the performance of the Services pursuant to the Agreement. Acquia will Process Personal Data as necessary to perform the Services pursuant to the Agreement and for the term of the Agreement. The type of personal data and categories of data subjects, the nature and purpose of the processing are further specified in the respective Product Notice incorporated herein.

1.5 **Compliance with Laws**. Each party will comply with all applicable laws, rules and regulations, including the Data Protection Laws.

2. CUSTOMER INSTRUCTIONS.

2.1 Acquia will process Personal Data in accordance with Customer's instructions. The parties agree that this DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Acquia in relation to the Processing of Personal Data. Additional or modified instructions require a documentation similar to this DPA and any such instructions leading to additional efforts by Acquia beyond the scope of the Services agreed in the Agreement and the Order may result in additional service fees payable by Customer that need to be documented in writing. Customer shall ensure that its instructions comply with Data Protection Laws and that the Processing of Personal Data in accordance with Customer's instructions will not cause Acquia to be in breach of Data Protection Laws or Standard Contractual Clauses.

2.2 Acquia shall notify the Customer if in Acquia's opinion any instruction Acquia receives pursuant to this Section 2 breaches (or causes either party to breach) any Data Protection Laws.

2.3 If Customer (or the relevant Customer Affiliate) is a Processor, Customer warrants to Acquia that Customer's instructions and actions, including electing Acquia as a (sub-)Processor, including any potential cross-border transfers, have been authorized by the relevant third-party Controller.

3. ACQUIA PERSONNEL.

3.1 **Limitation of Access**. Acquia shall ensure that Acquia's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

3.2 **Confidentiality**. Acquia shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training in their responsibilities, and have executed written confidentiality agreements. Acquia shall ensure that such confidentiality agreements survive the termination of the employment or engagement of its personnel.

3.3 **Reliability**. Acquia shall take commercially reasonable steps to ensure the reliability of any Acquia personnel engaged in the Processing of Personal Data.

3.4 **Data Protection Officer**. Acquia shall have appointed, or shall appoint, a data protection officer if Data Protection Laws require such appointment. Any such appointed person may be reached at privacy@acquia.com.

4. TECHNICAL AND ORGANIZATIONAL MEASURES, CERTIFICATIONS, AUDITS.

Acquia has implemented and will maintain the technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, alteration or damage, unauthorized

disclosure of, or access to, Personal Data), confidentiality and integrity of Customer Data as described in the Acquia Security Annex (available online at https://www.acquia.com/sites/default/files/legal/acquia-security-annex.pdf (the version applicable as of signature of this DPA is attached hereto as Exhibit 1)) also incorporated herein. Acquia regularly monitors compliance with these measures. Acquia has obtained third-party certifications and audits set forth in the Acquia Security Annex. In addition, the Acquia Security Annex specifies how Acquia allows for, and contributes to, audits.

If the EU SCCs or UK IDTA apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the EU SCCs. Nothing in this section of the DPA varies or modifies any Standard Contractual Clauses or Data Protection Laws or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Laws.

5. SUB-PROCESSORS.

5.1 **Sub-processors**. Customer acknowledges and agrees that (a) Acquia's Affiliates may be retained as Sub-processors; and (b) Acquia and its Affiliates respectively may engage third-party Sub-processors in the performance of the Services. Acquia or its Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Customer hereby consents to Acquia's use of Sub-processors as described in this Section.

5.2 **List of Current Sub-processors and Information about New Sub-processors**. Acquia shall make available to Customer a current list of Sub-processors for the Services at https://www.acquia.com/about-us/legal/subprocessors. Customer may subscribe to receive notifications of new sub-processors on the aforementioned website.

5.3 **Objection Right for new Sub-processors**. Customer may object to Acquia's use of a new Sub-processor by notifying Acquia promptly in writing within 10 business days after Acquia's update in accordance with the mechanism set out in Section 5.2 above. In the event Customer objects to a new Sub-processor: (i) Customer may immediately terminate the Agreement on giving written notice to Acquia; or (ii) where that objection is not unreasonable, Acquia will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid processing of Personal Data by the objected-to new Sub processor without unreasonably burdening Customer. If Acquia is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, without prejudice to Section 5.3 (i), Customer may terminate the applicable Order(s) in respect only to those Services which cannot be provided by Acquia without the use of the objected-to new Sub-processor, on the condition that Customer provides such termination notice within 90 days of being informed of the engagement of the Sub-processor as described in Section 5.2 above. If Customer terminates the Agreement under this Section 5.3, Acquia will then refund Customer any prepaid fees covering the remainder of the term of such terminated Order(s) following the effective date of termination with respect of such terminated Services. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Sub-processor.

5.4 **Acquia's Liability for Sub-processors**. Acquia shall be liable for the acts and omissions of its Sub-processors to the same extent Acquia would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise agreed.

6. RIGHTS OF DATA SUBJECTS.

6.1 Acquia shall, to the extent legally permitted, promptly notify Customer if Acquia receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("**right to be forgotten**"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"). Considering the nature of the Processing, Acquia shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Acquia shall upon Customer's request assist Customer in responding to such Data Subject Request, to the extent Acquia is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws.

6.2 To the extent legally permitted, Customer shall be responsible for any costs arising from Acquia's provision of such assistance as described in Section 6.1. Acquia shall bear the sole cost of the provision of such assistance if Acquia or its Sub-processors are required under Data Protection Laws to perform the activities or provide the information requested by the Customer.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION.

Acquia maintains a security incident management policy and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Acquia or its Sub-processors of which Acquia becomes aware (a "Personal Data Incident"), as required to assist

the Customer in ensuring compliance with its obligations to notify the Supervisory Authority in the event of Personal Data breach. Acquia shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Acquia deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Acquia's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's users.

8. Data Protection Impact Assessment and Assistance.

Upon Customer's request, Acquia shall provide Customer with reasonable cooperation and assistance needed: (i) to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services; and (ii) in connection with the Customer's obligations under Articles 32 to 34 (inclusive) of the GDPR. Acquia shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section.

9. Return or Deletion of Personal Data.

Acquia shall (at the Customer's sole option) return Personal Data to Customer and/or delete Personal Data after the end of the provision of Services relating to Processing in accordance with the timeframe specified in the Agreement, unless applicable law requires storage of Personal Data.

10. Transfers of Personal Data, Additional Safeguards, Government Data Production Request.

10.1 **Geographic Region.** Customer may select the geographic region in which Personal Data is housed from those available for the applicable Services. Once Customer has made its choice, Acquia will not move the Personal Data without Customer's prior written consent or unless required to comply with applicable law.

10.2 **Standard Contractual Clauses.**

10.2.1 **Current Standard Contractual Clauses.**

10.2.1.1 **Personal Data from the EU, EEA, Switzerland**: Where Acquia processes Personal Data that originates from the European Union, the EEA, and/or Switzerland, including for the purposes of providing Customer with 24/7 Customer support, such Personal Data shall be subjected to the EU SCCs as follows:

10.2.1.1.1 **Module Two** of the EU SCCs shall apply where Customer or a relevant Customer Affiliate is a Controller and **Module Three** shall apply where Customer or a relevant Customer Affiliate is a Processor;

10.2.1.1.2 Regarding **Clause 7** of the EU SCCs ("Docking Clause"), the optional docking clause shall apply;

10.2.1.1.3 Regarding **Clause 9** of the EU SCCs ("Use of sub-processors", Option 2 of Clause 9 (a) ("General Written Authorisation") shall apply with at least 30-day prior notice;

10.2.1.1.4 Regarding **Clause 11** of the EU SCCs ("Redress"), the optional language in Clause 11 (a) shall not apply;

10.2.1.1.5 Regarding **Clause 17** of the EU SCCs ("Governing Law"), Option 2 shall apply with the proviso that if the data exporter's EU Member State does not allow for third-party beneficiary rights, then the law of the Federal Republic of Germany shall apply;

10.2.1.1.6 Regarding **Clause 18 (b)** of the EU SCCs ("Choice of forum and jurisdiction"), the Parties agree that the choice of venue in the Agreement shall apply to this DPA as well unless the venue is not in an EU Member State, in which case the courts disputes under this DPA shall be resolved by the courts of Munich, Germany.

10.2.1.1.7 **Annex I** and **Annex II** of the EU SCCs shall be deemed completed with the information as set out in Exhibit 2 to this DPA.

10.2.1.2 **Personal Data from the UK:** Where Acquia processes Personal Data that originates from the United Kingdom, including for the purposes of providing Customer with 24/7 Customer support, such Personal Data shall be subjected to the UK IDTA as attached hereto as **Exhibit 3**, unless the Customer has opted out of those clauses.

10.2.1.3 **Personal Data from Switzerland:** Where Acquia processes Personal Data that originates from Switzerland, including for the purposes of providing Customer with 24/7 Customer support, such Personal Data shall be subjected to the EU SCCs, unless the Customer has opted out of those clauses with the proviso that the place of habitual residence in clause 18 (c) of the EU SCCs shall also include Switzerland.

10.2.2 **Follow-up Standard Contractual Clauses.** If Acquia transfers Personal Data to a Sub-processor located outside the EEA (including the United Kingdom if it has not been granted an adequacy decision by the European Commission) or otherwise makes a transfer (including onward transfer) of Personal Data, that, in the absence of either party and/or Sub-Processor (as applicable) being bound by the Standard Contractual Clauses or any successor clauses issued by a competent body from time to time, would cause either party and/or a Sub-processor to breach any Data Protection Laws, then Acquia shall

ensure it has in place Standard Contractual Clauses with the relevant Sub-processors, and the Parties shall reasonably amend any data privacy agreement between the Parties (so that they apply at least for the term of the Agreement).

11. DATA PRODUCTION REQUEST AND ADDITIONAL SAFEGUARDS.

11.1 If Acquia receives a mandatory request, order, demand, notice or direction from any government agency or other third party ("**Requestor**") to disclose any Personal Data whether or not in writing and whether or not referencing any Data Protection Laws or identifying any specific Data Subjects ("**Data Production Request**"), in addition to Clause 5(d)(i) of the EU SCCs, Acquia shall deal with the Data Production Request in accordance with the following terms:

11.2 Acquia shall use every reasonable effort to redirect the Requestor to make the Data Production Request directly to the Customer.

11.3 Acquia shall not disclose any Personal Data to any person in response to a Data Production Request unless either it is under a compelling statutory obligation to make such disclosure, or (having regard to the circumstances and the rights and freedoms of any affected Data Subjects) there is an imminent risk of serious harm that merits disclosure in any event (for example, to protect individuals' vital interests).

11.4 Where, in accordance with this Section 10, disclosure of the Personal Data is required in response to a Data Production Request, Acquia shall notify the Customer in writing in advance (setting out all relevant details) and shall thereafter provide all reasonable cooperation and assistance to the Customer and, if requested by the Customer, assist it with any application, injunction, order or request to prevent (or where that is not possible, to delay) the disclosure of any Personal Data.

11.5 Except where Acquia is prohibited under the law applicable to the Requestor from prior notification, Acquia shall use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the Data Protection Laws.

11.6 To the extent permitted under the Data Production Request, Acquia shall notify and consult with the relevant Supervisory Authority in respect of the Data Production Request, and at all times thereafter cooperate with the Supervisory Authority and the Customer to deal with and address the Data Production Request. Acquia shall, if permitted under the law applicable to the Requestor, suspend (or where not possible, apply to suspend) the Data Production Request, so that it can notify and consult with the Customer and the relevant Supervisory Authority.

12. CCPA/CPRA PROVISIONS

12.1 **Applicability of the CCPA/CPRA.** To the extent Acquia Processes Personal Data governed by CCPA and/or CPRA on behalf of the Customer or a relevant Customer Affiliate, this Section 12 shall apply additionally; in case of discrepancies between this Section 12 and any other clause of this DPA, its Exhibits, or the Agreement, this Section 12 shall prevail.

12.2 **Definitions.** For this Section 12 of this DPA, the following terms shall have the meanings set out below:

"Business Purpose" has the meaning provided in § 1798.140(d) of the California Civil Code, as amended or supplemented from time to time.

"Consumer Rights Request" means a verified communication from a consumer requesting to access their rights under the CCPA.

"Personal Information" has the meaning provided in § 1798.140(o)(1) of the California Civil Code, as amended or supplemented from time to time.

12.3 **Relationship of Parties.** The Parties agree that in this context,

Customer or the relevant Customer Affiliate is the 'business', and

Acquia is solely the 'service provider' with respect to Personal Information,

as such terms are defined in the CCPA/CPRA.

12.4 **Business Purpose and Data Processing.** Customer/Customer Affiliate may disclose Personal Information to Acquia when necessary to perform a Business Purpose. Customer represents and warrants to Acquia that such disclosures of Personal Information shall be consistent with the requirements set forth in the CCPA/CPRA. Acquia shall Process Personal Information on behalf of the Customer/Customer Affiliate in accordance with and for the Business Purpose.

12.5 **Do Not Sell.** Acquia shall not sell Personal Information, nor shall it retain use, or disclose Personal Information, except as necessary to perform the Business Purpose, or as otherwise authorized by the CCPA/CPRA.

12.6 **Consumer Rights Requests**. Acquia shall notify Customer promptly if it receives a Consumer Rights Request concerning

the processing of Personal Information and, in any event, in a reasonable amount of time for Customer to meet its obligations to respond to such Consumer Rights Request under the CCPA. Acquia shall not respond to any Consumer Rights Request concerning Personal Information unless expressly instructed to do so by Customer, or otherwise required by law. To the extent Customer, in its use of the Services, does not have the ability to address a Consumer Rights Request, Acquia shall upon Customer's request assist Customer in responding to such Consumer Rights Request, to the extent Acquia is legally permitted to do so and the response to such Consumer Rights Request is required under the CCPA. To the extent legally permitted, Customer shall be responsible for any costs arising from Acquia's provision of such assistance.

13. LIABILITY.
The total and aggregate liability of each party under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement.

14. TERM AND TERMINATION OF THE DPA.
This DPA will become legally binding once Acquia has received a countersigned DPA from Customer, in accordance with the instructions set forth below, and the DPA shall continue in force until the termination of the Agreement.

The parties hereto have executed this DPA as of the day and year last set forth below.

CUSTOMER: (data exporter)	_____	**ACQUIA INC.** (data importer)	
Business Address:	_____	Business Address: Street, Boston, MA 02109, USA	53 State
Signature:	_____	Signature:	_____
Print Name:	_____	Print Name:	_____
Title:	_____	Title:	_____
E-mail:	_____	E-mail:	privacy@acquia.com
Date of signature:	_____	Date of signature:	_____

Exhibit 1
to the ACQUIA GDPR DATA PROCESSING ADDENDUM
Security Annex

Defined terms not otherwise defined herein shall have the means ascribed to them in the Agreement or DPA. In case of a conflict between this Security Annex and the Agreement or DPA, the Agreement or the DPA shall prevail.

1. Security Policy. Acquia maintains a company-wide information security management system and control program that includes written security policies, standards and procedures based upon ISO/IEC 27001:2013 (collectively, the "Acquia Information Security Policy"). The Acquia Information Security Policy requires:

a. the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of Customer Data to the extent that such Customer Data is provided to Acquia and maintained or processed by Acquia during its provision of Services by utilizing practices such as:

   i. Secure software development practices;

   ii. Secure operating procedures and vulnerability management;

   iii. Ongoing employee training;

   iv. Controlling physical and electronic access to Customer Data, and

   v. Means for detecting and preventing intrusions and security system failures on critical systems.

b. that Acquia follow the principle of least privilege access, allowing only active Acquia employees and contractors access to records containing Customer Data and limits access to those persons who are reasonably required to know such information in order to accomplish a valid business purpose or to comply with record retention regulations;

c. that Customer Data that is identified as such to Acquia by the customer at intake, is secured appropriately commensurate to the nature of Customer Data, including any individual personal data provided to Acquia by Customer as set forth in this Exhibit, using commercially available and industry accepted controls and precautionary measures;

d. that commercially reasonable standards are followed with respect to strong change-control procedures and technical controls that enforce segregation of duties, minimum necessary dataset, and access controls;

e. monitoring of operations and maintaining procedures to ensure that security policies are operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Customer Data, and continuously improving information safeguards as necessary to mitigate risks;

f. a security patch and vulnerability management process based on accepted industry standard practices and protocols, including, monitoring threats, and responding to vulnerabilities reported by third parties; and

g. A security incident response and disaster recovery planning, including documentation of responsive actions taken in connection with any security incident related to Customer Data.

2. Security Practices and Processes

a. Customers are responsible for its legal and regulatory compliance in its use of any Subscription Services and shall make Acquia aware of any Customer Data processed, stored or transmitted through the Subscription Services for which regulations other than those set forth in the Security Annex apply. If, in the course of providing Subscription Services, Acquia agrees in writing to process such Customer Data and Customer has subscribed to any applicable Subscription Services, Acquia shall process it only as permitted under this Agreement and in compliance with data protection legislation to which Acquia is subject as a service provider. In the event that Acquia agrees to receive Customer Data from Customer, Acquia will manage and/or process such Customer Data pursuant to the security requirements, obligations, specifications and event reporting procedures as set forth in this Annex and the Agreement, and any amendments.

b. Acquia will comply with: (i) secure software development practices consistent with industry accepted standards and practices, and (ii) industry best practices on privacy and security.

c. Acquia restricts access to Customer Data and systems by users, applications and other systems. These controls include (i) controls to systems and data, limited to properly authenticated and authorized individuals based on principles of least

privilege and need-to-know; and (ii) physical access controls, as described below. Acquia will limit access to Customer Data to the minimum necessary dataset required to accomplish the intended business purpose or use. Acquia facilities and/or any Authroized Contractor facilities that process Customer Data will be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., electronic locks, access badges, and video surveillance) that provide a physically secure environment.

d. Acquia logs access to controlled systems and records, including successful and failed system access attempts, and restricts, and restricts the connection times of users. Acquia will use unique logins on all network equipment, whenever commercially reasonable.

e. Acquia maintains processes to identify and deploy security patches in a timely manner. Unless otherwise expressly agreed in writing, "timely" means that Acquia will introduce a fix or patch as soon as commercially reasonable after Acquia becomes aware of the security problem or availability of a fix or patch.

3. **Patch and Vulnerability Management.**

a. Acquia follows commercially reasonable best practices for patch management, criticality ranking and patching time frame requirements for all Acquia-operated systems, switches, routers, appliances, servers, and workstation PC's, as applicable.

b. Where feasible, Acquia ensures that trusted, commercially available anti-virus software is installed, enabled, and kept current on Acquia servers and systems used in accessing, processing, transmitting, or storing Customer Data.

c. Acquia maintains trusted, current, commercially available anti-malware protection capabilities on Acquia devices, particularly those used for accessing, processing, transmitting, or storing Customer Data.

d. Acquia maintains a vulnerability management solution for devices connected to Acquia's LAN. Such solution is designed to regularly assess Acquia's network for known vulnerabilities.

4. **Security Monitoring**

a. Acquia has a designated security team which monitors Acquia's control environment which is designed to prevent unauthorized access to or modification of Acquia's Customer Data. Acquia regularly monitors controls of critical systems, network and procedures to validate proper implementation and effectiveness in addressing the threats, vulnerabilities and risks identified. This monitoring is variable by the criticality, exposure, and the system's assets and may include: (i) internal risk assessments; (ii) validation of Multi-Factor Authentication for select environments; (iii) third party compliance, including hosting services and third-party components; and (iv) assessing changes affecting systems processing authentications, authorizations, and auditing.

b. Acquia performs periodic vulnerability assessments on Acquia applications and systems. Penetration tests are performed either by Acquia or by an established, reputable independent third party.

5. **Security of Data Processing.** Acquia has implemented and will maintain technical and organizational measures inclusive of administrative, technical and physical safeguards to ensure a level of security appropriate to the risk of the data processing for the Acquia Services as described in this Acquia Security Annex (the "Security Measures"). These Security Measures may be changed by Acquia from time to time during the Term of the Agreement in order to take into account advancements in available security technologies. However, Acquia will not materially decrease the overall security of the Services during the Term of the Agreement.

The Security Measures may include, but will not be limited to, the following measures for ensuring the ongoing confidentiality, integrity, and availability of Customer Data in order to prevent unauthorized access, use, modification or disclosure of Customer Data:

a. Background Checks

Performance of background checks on all personnel, as well as execution of non-disclosure commitments prior to employment and acknowledgment of professional behavior in the workplace documents, which includes anti-harassment and business ethics;

b. Training

Security and privacy awareness training, inclusive of acknowledgment and agreement to abide by organizational security policies, for all personnel upon hire and annually thereafter;

c. Customer Data

Pseudonymisation or encryption of Customer Data in transit and at rest utilizing industry-standard mechanisms for certain Acquia Services;

A process for regularly testing, assessing and evaluating the effectiveness of administrative, technical and physical safeguards for ensuring the security of the processing, transmission or storage of Customer Data through external and internal audits as further described below;

Preventing access, use, modification or disclosure of Customer Data except by authorized Acquia personnel (1) to provide the Subscription Services and prevent or address service or technical problems, (2) as compelled by law, or (3) as Customer expressly permits in writing.

d. Availability

The ability to restore the availability and access to Customer Data in a timely manner in the event of an incident impacting the availability of Customer Data by maintaining a backup solution for disaster recovery purposes;

e. Logging and Monitoring

Logging and monitoring of security logs via a Security Incident Event Management ("SIEM") system and alerting to a dedicated Incident Response team upon the detection of suspicious system and/or user behaviors;

f. Vulnerability Triaging

Processes and tooling for regularly identifying, assessing and triaging vulnerabilities based on industry-standard guidelines;

g. Policies

Maintenance of a comprehensive set of security and privacy policies, procedures and plans that are reviewed on at least an annual basis and provide guidance to the organization regarding security and privacy practices; and,

h. Subprocessors

Processes for evaluating prospective and existing Subprocessors to ensure that they have the ability and commit to appropriate administrative, technical and physical measures to ensure the ongoing confidentiality, integrity and availability of Customer Data.

By implementing the Security Measures detailed above Acquia, takes into account the risks that are related to data processing, in particular the ones resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

6. **Secure Data Transmissions.** Any Customer Customer Data that Acquia transmits over a public communications network will be protected during transmission by using, or making available, industry accepted standards such as TLS, SSH and VPNs.

7. **Data and Media Disposal.** Acquia maintains procedures that align with industry standards, such as NIST SP 800-88, regarding the disposal of both tangible property and electronic files containing Customer Data, taking into account available technology so that Customer Data cannot be reconstructed and read.

8. **Backup and Retention.** Acquia will backup systems used to provide services to Customer to ensure adequate recovery capabilities in accordance with the schedule set forth in the Documentation for the applicable Services. Back-ups will be appropriately protected to ensure only authorized individuals are able to access the Customer Data, including but not limited to encryption of data stored off-site in electronic media and appropriate classification and protection of hard copy records, as applicable. If not separately backed up, Acquia will secure any files containing Customer Data against unauthorized access in accordance with the terms of the Agreement.

9. **Customer Data.** Acquia will comply with applicable laws and regulations to the provision of the Services concerning the confidentiality, security, and processing of any Customer Data that it receives from Customer. In the event Acquia processes types of Customer Data that are subject to additional regulatory requirements due to the nature of the data or its place of origin (as defined in section 2a above) Acquia will reasonably cooperate with Customer to arrange compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g., EU SCCs, UK IDTA, Business Associate Agreement governing Protected Health Information), implementation of additional security controls required by relevant law, completion of regulatory filings applicable to Acquia, and participation in relevant regulatory audits as applicable from

section 13 below.

10. Security Incident Management and Remediation. For purposes of this Annex, a "**Security Incident**" means (i) the loss of, (ii) unauthorized acquisition, use or disclosure of, or (iii) unauthorized access to, Customer Data resulting from a security breach of the Acquia platform. Acquia maintains a response function capable of identifying and assessing the seriousness and extent of a Security Incident, mitigating the effect of a Security Incident, conducting root cause analysis, implementing and documenting remedial action plans, and preventing the recurrence of Security Incidents. Acquia has an established set of procedures to ensure personnel and contractors promptly report actual and/or suspected breaches of security. Acquia keeps an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents, as well as performing required recovery actions to remedy the impact.

a. Security Incidents on Acquia's platform are logged and reviewed, secured, and retained as required by applicable laws and regulations.

b. In the case of a Security Incident that relates to Customer Data, Acquia shall (a) promptly assess and contain such Security Incident, (b) notify Customer, without undue delay, upon becoming aware of such Incident, and in no case later than forty-eight (48) hours after Acquia has become aware of such Security Incident, via a Support ticket to each of the individuals identified by Customer for distribution of such Support Tickets (or such other addresses as may be provided by Customer from time to time) and provide regular status updates to Customer regarding the investigation at a frequency reasonably requested by Customer depending upon the severity of such Incident, (c) as applicable, provide reasonable cooperation and assistance to Customer needed to fulfill Customer's obligations related to Customer's use of the Services, as applicable, and (d) immediately take all steps reasonably necessary and within Acquia's reasonable control, including without limitation, those reasonably requested by Customer, to limit, stop, prevent and remediate such Incident. Following this initial notification, Acquia will promptly investigate the Security Incident and take all reasonable and necessary steps to prevent any further compromise of the Customer Data. If a security deficiency is identified within any Acquia information system during this investigation, Acquia will provide a report to Customer containing a description of the nature of the Security Incident, an identification of any Customer Data that was disclosed, destroyed, altered or compromised, and any investigative, corrective, or remedial actions taken or planned by Acquia to mitigate the risk of further Security Incidents. Acquia will maintain log files sufficient to enable Customer to determine what Customer Data was accessed and when, regardless of whether such data is physically or electronically maintained.

11. Business Continuity and Disaster Recovery. Acquia maintains business continuity and disaster recovery planning processes to establish and maintain plans and procedures for the continuity, recovery and operation of information systems, processes and facilities that could impact the availability of Customer Data (**"BC/DR Plans"**). These BC/DR Plans include processes for responding to emergencies (e.g., natural disasters such as fire, earthquakes, or hurricanes, or other disasters such as sabotage, virus, and terrorism), and includes:

(i) descriptions of roles and responsibilities: identifying key individuals and the recovery team responsible for implementing recovery actions; (ii) data backup plans, providing for periodic backups of data from database systems that can be used to reconstruct data; (iii) contingency plans and disaster recovery guides that will be followed by members of the recovery team before, during and after an unplanned disruptive event in order to minimize downtime and data loss; and (iv) procedures for annual testing and evaluating the BC/DR Plans including documenting the tests in writing.

12. Security Evaluations.

a. Acquia performs periodic risk assessments that evaluate and assess the security of the system's physical configuration and environment, software, information handling processes, and user practices including appropriate logs and reports on security activity.

b. In addition, security policies are regularly reviewed and evaluated to ensure operational effectiveness, compliance with applicable laws and regulations, and to address new threats and risks.

c. Security Policies are also reviewed when there is a material change in Acquia's business practices or the external threat environment that may reasonably implicate the security or integrity of records containing Customer Data. Acquia uses a documented change control process for software, systems, applications, and databases that ensures access changes are controlled, approved, and recorded.

Acquia will promptly notify Customer of any planned system configuration changes or other changes that would adversely affect the confidentiality, integrity, or availability of Customer's Customer Data.

13. Acquia Certifications and Standards by Product Offering

Acquia engages reputable third-party, independent, audit firms to conduct the below audit engagements:

Acquia Offering	Completed Certifications and Attestations
Acquia Cloud Enterprise	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2013 • HIPAA[1] • PCI-DSS[2] • FedRAMP[3]
Acquia Cloud Site Factory	• SOC 1 Type 2 (SSAE18 & ISAE 3402) • SOC 2 Type 2 (Security, Availability and Confidentiality) • ISO 27001:2013 • HIPAA[1] • PCI-DSS[2] • FedRAMP[3]

1 HIPAA compliant indicates that the service can be used in a way that enables Customers to help meet its legal obligations for HIPAA compliance. Ultimately, Customers are responsible for ensuring compliance with legal obligations, that the Acquia service meets their compliance requirements, and that they secure the service appropriately. Customers can reference Acquia's SOC 2 report, which contains a matrix mapping HIPAA controls to Acquia's SOC 2 controls.

2 PCI-DSS compliance requires the purchase of Acquia's PCI Cloud configuration within Acquia Cloud Enterprise and Acquia Cloud Site Factory.

3 Federal Risk and Authorization Management Program ("FedRAMP") is available for select Customers (i.e., Federal Agency cloud deployments). Acquia's FedRAMP implementation is more fully described in its FedRAMP package, available via the OMB MAX repository system.

Acquia will provide copies of available audit reports for the applicable Services to Customers upon written request and under NDA. Such audit reports, and the information they contain, are Acquia Confidential Information and must be handled by Customer accordingly. Such reports may be used solely by Customer to evaluate the design and operating effectiveness of defined controls applicable to the Services and are provided without any warranty. Acquia can also provide summary level penetration test documentation available to Customers upon request sanitized of any sensitive information.

14. Training and Secure Development Practices. The Acquia Information Security Policy is communicated to all Acquia personnel, employees, and contractors. Acquia provides periodic and mandatory security awareness training to employees and contractors (collectively "Personnel"). Acquia imposes disciplinary measures for violations of the Acquia Information Security Policy:

Agreements with relevant subprocessors include requirements that these subprocessors address security risks, controls, and procedures for information systems and contain terms, conditions, and restrictions at least as protective and as restrictive as those set forth herein. Acquia shall supply each of its personnel and contractors with appropriate, ongoing training regarding information security procedures, risks, and threats and Acquia shall be responsible for the performance of any subcontractor. Acquia agrees that any Services performed for Customer involving use of Customer Data shall be performed only at the Data Center Region and by personnel permitted under the Agreement.

15. Acquia Shared Responsibility Model.

Acquia Responsibilities

Acquia is responsible for the confidentiality, integrity and availability (the "security") of the Services and internal Acquia information

technology systems. In addition to those measures detailed in "Security of Data Processing" above, Security Measures include, but are not limited to, server-level patching, vulnerability management, penetration testing, security event logging & monitoring, incident management, operational monitoring, 24/7 support, and ensuring customer site availability in accordance with the applicable SLA.

Acquia uses subprocessors for the Services and to support Acquia as a Processor of Customer data, all as more fully set forth on the website located at: https://www.acquia.com/about-us/legal/subprocessors. As these subprocessors are authorized subprocessors as defined in the Agreement, Acquia shall remain fully liable for their acts and omissions relating to the performance of the respective Services and shall be responsible for ensuring that obligations under this Security Annex and the Agreement are carried out in accordance with both.

Customer Responsibilities

The Customer is responsible for the security of their Customer Application(s), as applicable. For example, patching the open-source software Drupal, that are used in conjunction with the Services. This includes, but is not limited to, ensuring a secure configuration and coding of the applications, related application security monitoring activities, Customer user access management, password configurations, implementing multi-factor authentication, periodic penetration testing, appropriate Application-level DoS or DDoS protections, and/or vulnerability scanning of their applications, amongst others.

In addition, Customers are also responsible for the secure management of their users and provision of users for the purpose of granting access to Acquia's Services and abiding by the Subscription and Services Agreement, the Data Processing Agreement and Acquia's Acceptable Use Policy in using Acquia's Services.

16. **Access and Review.** Acquia will make summary level information regarding its security policies and procedures as well current, published, third-party audit audit reporting related to Customer's Customer Data available for Customer's review at Acquia upon reasonable prior written notice by Customer and subject to Acquia's confidentiality and security conditions, and subject to a written and mutually agreed audit plan. Acquia reserves the right to require its prior approval to any third-party review of the DR Plan, and reasonably condition and restrict such third-party access. As illustrated in, "Acquia Certifications and Standards by Product Offering" Customers may also review available audit reporting as outlined in Section 13.

17. **Customer Audits.** Acquia offers its Services in the cloud using AWS and a one-to-many business model that relies on standardization of best practices and industry standards for the benefit of its Customers. As a result, onsite audits by Customers pose security and privacy risks to Acquia, other Acquia Customers and Acquia Subprocessors. Moreover, AWS does not allow for physical audits of the AWS data centers but instead provides third party audits and certifications. It is for these reasons, among others, that Acquia's security program consists of the audits, certifications and available documentation detailed in "Third Party Audits, Certifications" above as part of balancing transparency regarding the security and privacy safeguards that Acquia has implemented, while also satisfying security and privacy requirements as part of security and privacy obligations to Acquia Customers, and its Subprocessors, including AWS.

Therefore, Customer agrees to exercise its right to conduct an audit or inspection of Acquia's processing of personal data within Customer Data by instructing Acquia to carry out audits as described above in the section "Third Party Audits, Certification" using its current processes and timing. If Customer wishes to change this instruction regarding the audit or inspection, then Customer shall send such request by written notice to Acquia and the parties agree to jointly discuss how to implement the changed instruction.

Exhibit 2
EU SCCs (Standard Contractual Clauses 2021) Annexes I and II

ANNEX I

LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: Customer per page above and any Customer Affiliates as further described in the DPA and Agreement

Address: per page above or as further described in the DPA and Agreement

Contact person's name, position and contact details: _____

Activities relevant to the data transferred under these Clauses: Use of the Services as procured by the Data exporter(s) from the Data importer(s) as further defined in the DPA and the Agreement.

Signature and date: per execution on page above

Role (controller/processor): Controller (or Processor on behalf of a third-party Controller)

2. _____

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. **Name**: Acquia Inc.

Address: 53 State Street, Boston, MA 02109, USA

Contact person's name, position and contact details: Stephan Dobrowolski, Assoc. General Counsel, privacy@acquia.com

Activities relevant to the data transferred under these Clauses: Provision of the Services as procured by the Data exporter(s) from the Data importer(s) as further defined in the DPA and the Agreement.

Signature and date: Per execution on page

Role (controller/processor): Processor.

2. The Acquia Affiliates as set out at: https://www.acquia.com/about-us/legal/subprocessors

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

Categories of personal data transferred

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

Sensitive data transferred (if applicable) and **applied restrictions or safeguards** that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security

measures.

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

The **frequency of the transfer** (e.g., whether the data is transferred on a one-off or continuous basis).

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

Nature of the processing

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

Purpose(s) of the data transfer and further processing

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

The **period for which the personal data will be retained**, or, if that is not possible, the criteria used to determine that period

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ .

For **transfers to (sub-) processors**, also specify subject matter, nature and duration of the processing

As specified in the relevant Product Notice per each Service available at https://docs.acquia.com/guide/ in connection with the relevant information regarding sub-processors set out at https://www.acquia.com/about-us/legal/subprocessors

COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the EU GDPR applies directly:	the competent supervisory authority determined in accordance with Clause 13 of the EU SCCs, and
Where the Swiss GDPR applies:	Federal Data Protection and Information Commissioner of Switzerland

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

- see the relevant Product Notice available online at https://docs.acquia.com/guide/ (marked as "**GDPR Product Notice**"), and
- see the Acquia Security Annex available online at https://www.acquia.com/sites/default/files/legal/acquia-security-annex.pdf (the version applicable as of signature of this DPA is attached hereto as **Exhibit 1**)

For transfers to (sub-) processors, alsodescribe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Acquia requires its sub-processors to adhere to technical and organizational measures which are at least as equivalent as those referenced in the Acquia Security Annex (see **Exhibit 1** to the DPA).

Exhibit 3
Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

PART 1: TABLES

TABLE 1: PARTIES

Start date	from the date of last signature on page of this DPA	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: per page above Trading name (if different): per page above Main address (if a company registered address): per page above Official registration number (if any) (company number or similar identifier): per page above	Full legal name: Acquia Inc. Trading name (if different): n/a Main address (if a company registered address): 53 State Street, Boston, MA 02109, USA Official registration number (if any) (company number or similar identifier): US Federal Tax ID (FEIN): 26-0493001
Key Contact	Full Name (optional): _____ Job Title: _____ Contact details including email: _____	Full Name (optional): n/a Job Title: Acquia Privacy Team Contact details including email: privacy@acquia.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: per page above Reference (if any): Exhibit 2 of the DPA to which this Exhibit 3 is attached Other identifier (if any): n/a Or

☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	n/a	n/a	n/a	n/a	n/a	n/a
2	yes	yes	no option	General Authorisation	30 days	see the relevant Product Notice available online at https://docs.acquia.com/guide/ (marked as "GDPR Product Notice")
3	yes	yes	no option	General Authorisation	30 days	see the relevant Product Notice available online at https://docs.acquia.com/guide/ (marked as "GDPR Product Notice")
4	n/a	n/a	n/a	n/a	n/a	n/a

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:	Exhibit 2 Annex I to the DPA
Annex 1B: Description of Transfer:	Exhibit 2 Annex I to the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	Exhibit 2 Annex II to the DPA
Annex III: List of Sub processors (Modules 2 and 3 only):	https://www.acquia.com/about-us/legal/subprocessors

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses[3]

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

[3] Alternative Part 2 Mandatory Clauses chosen.

ACQUIA ACCEPTABLE USE POLICY

This Acceptable Use Policy (this "Policy") describes prohibited uses of all services offered by Acquia Inc. and its affiliates (the "Services") and the website located at http://www.acquia.com and all associated sites (the "Acquia Site"). The examples described in this Policy are not exhaustive. We may modify this Policy at any time by posting a revised version on the Acquia Site. By using the Services or accessing the Acquia Site, you agree to the latest version of this Policy. If you violate the Policy or authorize or help others to do so, we may suspend or terminate your use of the Services.

You are solely responsible for any material that you or your end users maintain, transmit, download, view, post, distribute, or otherwise access or make available using the Services. By using the Services, you represent that you own the content that you make available through Acquia's Services and all proprietary or intellectual property rights therein, or have the express written authorization from the owner to copy, use and display such content.

Prohibited Use of Services

A. No Illegal, Harmful, or Offensive Use or Content

You may not use, encourage, promote, facilitate or instruct others to use, the Services or Acquia Site for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive.

Prohibited activities or content include but are not limited to:

- **Illegal, Harmful or Fraudulent Activities**. Any activities that are illegal, that violate the rights of others, or that may be harmful to others, our operations or reputation, including disseminating, promoting or facilitating child pornography, offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming.
- **Infringing Content**. Content that infringes or misappropriates the intellectual property or proprietary rights of others.
- **Offensive Content**. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography.
- **Harmful Content.** Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, malware, Trojan horses, worms, time bombs, or cancelbots.

B. No Security Violations

You may not use the Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include but are not limited to:

- **Unauthorized Access.** Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- **Interception**. Monitoring of data or traffic on a System without permission.
- **Falsification of Origin**. Forging TCPIP packet headers, email headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

C. No Network Abuse

You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include but are not limited to:

- **Unauthorized Access.** Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- **Interception.** Monitoring of data or traffic on a System without permission.
- **Falsification of Origin.** Forging TCPIP packet headers, email headers, or any part of a message describing its origin or route. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.

D. No Spam

You will not distribute, publish, send, or facilitate the sending of unsolicited mass email or other messages, promotions, advertising, or solicitations, like "spam. You will not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. You will not collect replies to messages sent from another Internet service provider if those messages violate this Policy or the acceptable use policy of that provider. All recipients in a Acquia customer or user's contact list must have given provable consent, online or otherwise, to receive email communication and for the specific content being sent to them. You must abide by the following rules:

- Email lists that were obtained by any means without consent are not allowed
- All email and recipient lists must adhere to the CAN-SPAM laws, as well as to any local spam laws for your location or the location of your recipient lists
- Email must abide by the rules outlined in this Policy

- No 3rd party unsubscribe methods are allowed

Our Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Services or Acquia Site. We may:

- investigate violations of this Policy or misuse of the Services or Acquia Site; or
- remove, disable access to, or modify any content or resource that violates this Policy or any other agreement we have with you for use of the Services or the Acquia Site.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

Feedback Loops and Abuse Reporting

Acquia is registered with Internet Service Provider ("ISP") feedback loops and monitors abuse reports. These feedback loops notify Acquia when your or your user's contact marks a message as "spam". You and your users are subject to warnings, suspension or termination if Acquia receives a report containing a high number of spam reported against your or your user's account.

Bounce Rates

An account's bounce rate is subject to be monitored by Acquia. An account's bounce rate should consistently remain under 8% as many ISPs will begin blocking IPs for higher bounce rates. Accounts with high bounce rates are subject to warnings, suspension or termination. To avoid such consequences, ensure your list of contacts are reviewed and maintained regularly.

Plugins and Integrations

You and your users utilizing Acquia's available integrations and plugins must adhere to Acquia's policies, as well as those of the 3rd party system being integrated. If you are found to be violating Acquia's or an integrated 3rd party system's policy, your account will be subject to suspension or deletion.

Reporting of Violations of this Policy

If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this Policy, please contact our Legal Department: legal@acquia.com.

PRIVACY POLICY

Introduction

Acquia Inc., including its wholly owned affiliates, ("Acquia", "us," "we," or "our,") is committed to protecting the privacy of your information. This Privacy Policy ("Policy") governs Acquia's use of personally identifiable information, also "personal data," about users of our products, services and/or software that are available for purchase and use through our sales teams, accessible by download on our websites (our "Services"), and also users of our website http://acquia.com as well as the other websites that Acquia operates and that link to this Policy (collectively referred to as "Site(s)"). It also describes the choices available to you regarding our use of your personally identifiable information and how you can access and update this information.

Acquia complies with the relevant regulation applying to personal data, including but not limited the General Data Protection Regulation issued by the European Union.

Our Sites may contain links to other websites, applications, and services maintained by third parties. The information practices of other services are governed by their privacy statements, which you should review to better understand their privacy practices.

EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

Acquia complies with the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the United States Department of Commerce regarding the collection, use, and retention of personally identifiable information transferred from the European Union, and the United Kingdom and/or Switzerland to the United States. Consistent with our commitment to protect personally identifiable information about individuals in the European Union, Acquia has certified to the Department of Commerce that it adheres to the Privacy Shield Principles of Notice, Choice, and Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability (the "Privacy Shield Principles" or the "Principles"). Acquia's EU-U.S. and Swiss-U.S. Privacy Shield Certification also extends to personally identifiable information that we receive directly through the Sites. More information on the EU-U.S. and Swiss-U.S. Privacy Shield and Acquia's scope of participation in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks are available at http://www.privacyshield.gov/welcome.

If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

California Residents

If you are a California consumer, for more information about your privacy rights, please see our California Consumer Privacy Statement.

Brazil Residents

If you are a Brazil consumer, for more information about your privacy rights under Lei Geral de Proteção de Dados Pessoais ("LGPD"), please contact us at Legal@acquia.com.

Privacy Policy Updates

Due to the Internet's rapidly evolving nature, Acquia may need to update this Privacy Policy from time to time. If so, Acquia will post our updated Privacy Policy on our Site located at http://acquia.com/about-us/legal/privacy-policy and post notice of the change so it is visible when users log-on for the first time after the change is posted so that you are always aware of what personally identifiable information we may collect and how we may use this information. If we make material changes to this policy, we will notify you here, by email, or by means of a notice on our home page. Acquia encourages you to review this Privacy Policy regularly for any changes. Your continued use of this Site and/or continued provision of personally identifiable information to us will be subject to the terms of the then-current Privacy Policy.

Data Integrity and Purpose Limitation

Acquia is a provider of cloud platform related services, including Platform as a Service ("PaaS") and Software as a Service ("SaaS") products, technical support services and professional consulting services for Drupal websites which processes personally identifiable information upon the instruction of its customers in accordance with the terms of the applicable agreement between Acquia and customer.

Information Collection and Use

You can generally visit our Site without revealing any personally identifiable information about yourself. However, in certain sections of the Site or interactions with us, we may invite you to participate in one or some of the following. We collect such information in the following situations:

- Surveys (If you voluntarily submit certain information to our services, such as filling out a survey about your user experience, we collect the information you have provided as part of that request)
- Contact Us features with questions or comments or request information, participate in chat or message boards (If you express an interest in obtaining additional information about our services, request customer support, use our "Contact Us" or similar features, register to use our services, sign up for an event, questionnaires, webinar, contests, or download certain content, we may require that you provide to us your contact information)
- If you interact with our websites or emails, we may automatically collect information about your device and your usage of our websites or emails, (such as Internet Protocol (IP) addresses or other identifiers, which may qualify as Personal Data) (see "Device and Usage Data Processing section, below) using cookies, Web Beacons, or similar technologies.
- If you make purchases via our Sites or register for an event or webinar, we may require that you provide your financial and billing information, such as billing name and address, credit card number or bank account information.
- If you communicate with us via a phone call from us, we may record that call.
- We require you to complete a registration form and/or create a profile to access certain restricted areas of the Site, to use certain services and when you download any software.
- If you visit our offices, you may be required to register as a visitor and to provide your name, email address, phone number, company name, and time and date of arrival. Additionally, due to the COVID-19 pandemic, you may be required to provide information regarding your health

status, including your temperature, COVID-19 related symptoms, exposure to COVID-19, positive individuals, and recent travel history.

Due to the nature of some of these activities, we may collect personally identifiable information such as your name, e-mail address, address, phone number, password, screen name, credit card information and other contact information that you voluntarily transmit with your on-line and in-person communications to us and personally identifiable information that you elect to include in your chart and message board postings.

If you use a forum on this Site, you should be aware that any personally identifiable information you submit there can be read, collected, or used by other users of these forums, and could be used to send you unsolicited messages. We are not responsible for the personally identifiable information you choose to submit in these forums. We receive permission to post testimonials that include personally identifiable information prior to posting.

If you provide us or our service providers with any Personal Data relating to other individuals, you represent that you have the authority to do so, and where required, have obtained the necessary consent, and acknowledge that it may be used in accordance with this Privacy Policy. If you believe that your Personal Data has been provided to us improperly, or want to exercise your rights relating to your Personal Data, please contact us by emailing privacy@acquia.com.

Orders

If you purchase a product or service from us, we request certain personally identifiable information from you on our order form. You must provide contact information (such as name, email, and shipping address) and financial information (such as credit card number, expiration date).

We use this information for billing purposes and to fill your orders. If we have trouble processing an order, we will use this information to contact you.

In addition, we may collect information about the performance, security, software configuration and availability of customer web sites in an automated fashion as part of the Acquia subscription services.

We use your personally identifiable information to register you to use our services or download or access software or other content, contact you to deliver certain goods, services or information that you have requested, provide you with notices regarding goods or services you have purchased, provide you with notices regarding goods or services that you may want to purchase in the future (including communications from third party service providers and/or Acquia technology partners concerning additional products/applications which compliment Acquia's services, or else are customizable with Acquia's services in order to maximize your digital experience while leveraging Acquia services), verify your authority to enter our Site and improve the content and general administration of the Site and our services.

Certain modules within the Drupal software connect your installation of Drupal to our subscription services, these modules will report to us, and we will collect, your IP address, operating system type and version, web server type and version, php version, database type and version, version of the services, modifications to your Drupal code, information regarding the availability of your website (e.g. if your website is live or down), website user statistics such as the number of nodes, number of users and

number of comments. The foregoing information will be linked to your personally identifiable information and user accounts and we may use the foregoing information to better provide technical support to you and our customers and to improve our services.

If you install and use the Acquia Search module and connect your Drupal site to the subscription services, in addition to the information we may collect, analyze and store when you use our services as stated above, the Acquia Search module may collect, analyze and store the content of your site in an index. This index will be stored and updated on our servers to enable Acquia Search to work with your site. A copy of this index may be retained for up to 14 days as a backup in the event there is a problem with the index. Additionally, information about the size of your index, the search queries performed on your index, performance of Acquia Search for your queries, and other operational information is stored indefinitely in order to enable Acquia to monitor performance over time, manage the Search Service, and to provide you with information about the Search activity on your site.

If you choose to contact us by e-mail, we will not disclose your contact information contained in the e-mail, but we may use your contact information to send you a response to your message. Notwithstanding the foregoing, we may publicly disclose the content and/or subject matter of your message, therefore, you should not send us any ideas, suggestions or content that you consider proprietary or confidential. All e-mail content (except your contact information) will be treated on a non-proprietary and non-confidential basis and may be used by us for any purpose.

Details of data processing

Acquia processes your personal data as a customer and other customer's personal data (in the following just "customer") in order to provide the contractually agreed Services.

Subject matter: The subject matter of the data processing is the performance of the Services agreed between Acquia and customer by Acquia involving personal data provided by customer.

Duration: As between customer and Acquia, the duration of the data processing is determined by customer and its contractual commitments with regard to the use of Acquia's Services.

Purpose: The purpose of the data processing by Acquia is the provision of the Services initiated by the customer from time to time.

Nature of the processing: Cloud computing as platform and software as a service and such other Services as described in the Documentation and initiated by the customer from time to time.

Type of personal data:

The type and extent of personal data that is subjected to Acquia's data processing is determined and controlled by our customer as data controller in its sole discretion - this may include, but is not limited to the following:

- First and last name
- Title, work department, and manager/supervisor name
- Position and employment history
- Employer

- Contact information (company, personal and work email, phone, home address, physical business address, emergency contact details)
- Photographs
- Biographical and directory information, including linked social media profile or posts
- Company user names or IDs and login credentials
- Identifiers related to work or personal devices used to access data exporter's IT systems
- Log information generated through the use of data exporter's IT systems
- Actions performed by the employee while accessing or using the Services
- Full time or part time status
- Business travel arrangements
- Training undertaken and training needs
- Localization data

Categories of data subjects: Customer's representatives and end-users including employees, contractors, collaborators and advisors of our customer (who are natural persons).

Communications from the Site

Special Offers and Updates

We will occasionally send you information on products, services, special deals, promotions. Out of respect for your privacy, we present the option not to receive these types of communications. Please see "Choice and Opt-out."

Newsletters

If you wish to subscribe to our newsletter(s), we will use your name and email address to send the newsletter to you. Out of respect for your privacy, we provide you a way to unsubscribe. Please see the "Choice and Opt-out" section.

Service-related Announcements

We will send you strictly service-related announcements on rare occasions when it is necessary to do so. For instance, if our service is temporarily suspended for maintenance, we might send you an email.

Generally, you may not opt-out of these communications, which are not promotional in nature. If you do not wish to receive them, you have the option to deactivate your account.

Customer Service

Based upon the personally identifiable information you provide us, we will send you a welcoming email to verify your username and password. We will also communicate with you in response to your inquiries, to provide the services you request, and to manage your account. We will communicate with you by email or telephone, in accordance with your wishes.

Choice/Opt-out

We or one of our authorized partners may place or read cookies on your device when you visit our websites for the purpose of serving you targeted advertising (also referred to as "online behavioral advertising" or "interest-based advertising"). To learn more about targeted advertising and advertising networks please visit the opt-out pages of the Network Advertising Initiative, here, and the Digital Advertising Alliance, here. We provide you the opportunity to 'opt-out' of having your personally identifiable information used for certain purposes, when we ask for your information.

To request updates or changes to your information or your preferences regarding receiving future promotional messages from us, you may contact our Privacy Officer using the information in the Contact Us section of this Privacy Policy or follow the opt-out instructions that are contained in the bottom of the email communication you received.

You will be notified prior to when your personally identifiable information is collected by any third party that is not our agent/service provider, so you can make an informed choice as to whether or not to share your information with that party.

Please note that if you opt out of receiving our promotional or marketing emails, you may still receive certain service-related communications from us, such as administrative and services announcements and messages about your account. Occasionally these materials are sent from a different email domain: marketing@theacquiateam.com.

Employment Opportunities

We provide you with a means for submitting your resume or other personally identifiable information through the Site for consideration for employment opportunities at Acquia. Personally identifiable information received through resume submissions will be kept confidential. We may contact you for additional information to supplement your resume, and we may use your personally identifiable information within Acquia, or keep it on file for future use, as we make our hiring decisions.

Children's Privacy

Acquia recognizes the privacy interests of children and we encourage parents and guardians to take an active role in their children's online activities and interests. This Site is not intended for children under the age of 13. Acquia does not target its services or this Site to children under 13. Acquia does not knowingly collect personally identifiable information from children under the age of 13. If you are a parent or guardian and believe your child has provided us with personal information without your consent, please contact us by emailing privacy@acquia.com.

Cookies and GIFs

We use small text files called cookies to improve overall Site experience. A cookie allows us to gather information about the use of our sites and how people interact with our emails. Cookies generally do not permit us to personally identify you (except as provided below). We may also use clear GIFs (a.k.a. "Web beacons") in HTML-based emails sent to our users to track which emails are opened by recipients.

Additionally, when using the Site, we and any of our third party service providers may use cookies and other tracking mechanisms to track your user activity on the Site and identify the organization or entity from which you are using the Site. If you register with the Site, we, and our third party service providers, will be able to associate all of your user activity with your personally identifiable registration information. We will use such user activity information to improve the Site, to provide context for our sales and support staff when interacting with you and customers, to initiate automated email marketing campaigns triggered by your activity on the Site and for other internal business analysis.

Aggregate Information

The Site may track information that will be maintained, used and disclosed in aggregate form only and which will not contain your personally identifiable information, for example, without limitation, the total number of visitors to our Site, the number of visitors to each page of our Site, browser type, External Web Sites (defined below) linked to and IP addresses. We may analyze this data for trends and statistics in the aggregate, and we may use such aggregate information to administer the Site, track users' movement, and gather broad demographic information for aggregate use.

Disclosure

We will not sell your personally identifiable information to any company or organization, except we may transfer your personally identifiable information to a successor entity upon a merger, consolidation or other corporate reorganization in which Acquia participates or to a purchaser or acquirer of all or substantially all of Acquia's assets to which this Site relates. We may provide your personally identifiable information and the data generated by cookies and the aggregate information to parent, subsidiary or affiliate entities within Acquia's corporate family, partner entities that are not within Acquia's corporate family and vendors and service agencies that we may engage to assist us in providing our services to you. For example, we may provide your personally identifiable information to a credit card processing company to process your payment. Such third party service providers may be obligated to protect your personally identifiable information consistent with the terms of this Privacy Policy and not for their promotional purposes and/or required to enter into written confidentiality and data processing agreements including the commitment to be compliant with the Standard Contractual Clauses issued by the European Commission. We will also disclose your personally identifiable information (a) if we are required to do so by law, regulation or other government authority, in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, or otherwise in cooperation with an ongoing investigation of a governmental authority (b) to enforce the Acquia Terms of Use agreement or to protect our rights or (c) to protect the safety of users of our Site and our services.

The Site may provide links to other Web sites or resources over which Acquia does not have control ("External Web Sites"). Such links do not constitute an endorsement by Acquia of those External Web Sites. You acknowledge that Acquia is providing these links to you only as a convenience, and further agree that Acquia is not responsible for the content of such External Web Sites. Your use of External Web Sites is subject to the terms of use and privacy policies located on the linked External Web Sites.

Security

We employ procedural and technological measures that are reasonably designed to help protect your personally identifiable information including sensitive data from loss, unauthorized access, disclosure, alteration or destruction. Acquia may use encryption, secure socket layer, firewall, password protection and other physical security measures to help prevent unauthorized access to your personally identifiable information including sensitive data. Acquia may also place internal restrictions on who in the company may access data to help prevent unauthorized access to your personally identifiable information. These precautions take into account the risks involved in the processing, the nature of personally identifiable information, and best practices in the industry for security and data protection.

Please find additional information about Acquia's security measures on our website https://www.acquia.com/solutions/security and for our Services specifically in our Acquia Security Annex available at https://www.acquia.com/sites/default/files/legal/acquia-security-annex.pdf

Accountability for Onward Transfer

Acquia is accountable for personally identifiable information that we receive and subsequently transfer to third parties. If third parties that process personally identifiable information on our behalf do so in a manner that does not comply with the Privacy Shield Principles, we are accountable, unless we prove that we are not responsible for the event giving rise to the damage.

Contact information and Customer personally identifiable information is accessible only by those Acquia employees and consultants who have a reasonable need to access such information in order for us to fulfill contractual, legal and professional obligations. All of our employees and consultants have entered into confidentiality agreements, and/or have been subjected to thorough criminal background checks requiring that they maintain the confidentiality of Customer personally identifiable information.

In the event Acquia discloses personally identifiable information covered by this Policy to a non-agent third party, it will do so consistent with any notice provided to Data Subjects and any choice they have exercised regarding such disclosure. Acquia will only disclose personally identifiable information to third-party agents that have given us contractual assurances that they will provide at least the same level of privacy protection as is required by this Privacy Policy and the Principles and that they will process personally identifiable information for limited and specific purposes consistent with any consent provided by the individual. If Acquia has knowledge that a third party to which it has disclosed personally identifiable information covered by this Privacy Policy is processing such personally identifiable information in a way that is contrary to this Privacy Policy and/or the Principles, Acquia will take reasonable steps to prevent or stop such processing. In such case, the third-party is liable for damages unless it is proven that Acquia is responsible for the event giving rise to the violation.

Acquia may use from time to time a limited number of third-party service providers, contractors, and other businesses to assist us in providing our solutions to our customers or in meeting internal business operation needs. These third-parties may access process or store personally identifiable information in the course of performing their duties to Acquia. Acquia maintains contracts with these providers restricting their access, use and disclosure of personally identifiable information in compliance with our obligations under the Principles.

Your rights relating to your personal data

Depending on the applicable local data protection laws, you have certain rights relating to your Personal Data including, but not limited to:

- Access to your data
- Rectification
- Erasure ("right to be forgotten")
- Restriction of Processing
- Object, opt-out, withdrawing your consent
- Transfer of your data

Acquia provides you with the ability to exert any such right by contacting us through this web form (https://acquia-privacy.my.onetrust.com/webform/29a25674-36fd-4a6f-8e09-7e5a4f94cf4a/8511aea7-dd1f-4353-9429-a0dbe52f01cc).

Enforcement and Liability

Acquia is subject to the jurisdiction and enforcement and investigatory authority of the United States Federal Trade Commission.

Acquia also commits to periodically reviewing and verifying the accuracy of this Policy and the company's compliance with the Principles, and remedying issues identified. All employees of Acquia that have access to personally identifiable information covered by this Policy in the U.S. are responsible for conducting themselves in accordance with this Policy. Failure of an Acquia employee to comply with this Policy may result in disciplinary action up to and including termination.

Acquia assures compliance with this EU-U.S. and Swiss-U.S. Privacy Shield Policy and the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks by utilizing the self-assessment approach as specified by the U.S. Department of Commerce. The assessment is conducted on an annual basis to ensure that all of Acquia's relevant privacy practices are being followed in conformance with this EU-U.S. and Swiss-U.S. Privacy Shield Policy and the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. Any employee that Acquia determines is in violation of these policies will be subject to discipline, up to and including termination of employment and/or criminal prosecution.

Dispute Resolution

Acquia assures compliance with this EU-U.S. and Swiss-U.S. Privacy Shield Policy by fully investigating and attempting to resolve any complaint or dispute regarding the use and disclosure of personally identifiable information in violation of this Privacy Policy.

Any questions or concerns regarding the use or disclosure of personally identifiable information should first be directed to the owner of the website in question (our customer); or if the question or concern is from our customer, then to Acquia at the address given below.

Acquia will respond to any inquiries or complaints within forty-five (45) days. In the event that Acquia fails to respond or its response is insufficient or does not address the concern, Acquia has registered with JAMS to provide independent third party dispute resolution at no cost to the complaining party. To

contact JAMS and/or learn more about the company's dispute resolution services, including instructions for submitting a complaint, please visit: https://www.jamsadr.com/eu-us-privacy-shield.

If your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

Acquia will cooperate with the United States Federal Trade Commissions and any data protection authorities of the EU Member States and/or United Kingdom ("DPAs") in the investigation and resolution of complaints that cannot be resolved between Acquia and the complainant that are brought to a relevant DPA.

Contact Us

If you have any questions or complaints regarding this Privacy Policy please contact us by mail: Acquia Inc. 53 State Street Boston, MA 02109 USA Attention: General Counsel

Or e-mail to privacy@acquia.com

Updated February 11, 2022

Cellebrite EULA

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING, ACCESSING OR USING CELLEBRITE-SUPPLIED SOFTWARE (AS PART OF A PRODUCT OR STANDALONE) CONSTITUTES EXPRESS ACCEPTANCE OF THIS AGREEMENT. CELLEBRITE IS WILLING TO LICENSE SOFTWARE TO YOU ONLY IF YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS AGREEMENT (THE "EULA"), ANY ADDITIONAL TERMS IN AN AGREEMENT SIGNED BY BUYER (AS DEFINED BELOW) AND CELLEBRITE, AND ANY "CLICK-ACCEPT" AGREEMENT, AS APPLICABLE. TO THE EXTENT OF ANY CONFLICT AMONG THIS EULA, ANY ADDITIONAL TERMS IN AN AGREEMENT SIGNED BY BUYER AND CELLEBRITE, ANY "CLICK-ACCEPT" AGREEMENT, ANY TERMS ON A PURCHASE ORDER AND CELLEBRITE'S TERMS AND CONDITIONS OF SALE, THE ORDER OF PRECEDENCE SHALL BE (A) AN AGREEMENT SIGNED BY BUYER AND CELLEBRITE; (B) THIS EULA; (C) THE "CLICK-ACCEPT" AGREEMENT; (D) CELLEBRITE'S TERMS AND CONDITIONS OF SALE; AND (E) BUYER'S PURCHASE ORDER, TO THE EXTENT SUCH TERMS ARE PERMISSIBLE UNDER CELLEBRITE'S TERMS AND CONDITIONS OF SALE OR AN AGREEMENT SIGNED BY BUYER AND CELLEBRITE (COLLECTIVELY, (A)-(E), AFTER APPLYING THE ORDER OF PRECEDENCE, THE "AGREEMENT").#

BY DOWNLOADING, INSTALLING, ACCESSING, OR USING THE SOFTWARE, USING THE PRODUCT OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED IN THE AGREEMENT, YOU INDIVIDUALLY AND ON BEHALF OF THE BUSINESS OR OTHER ORGANIZATION THAT YOU REPRESENT (THE "BUYER") EXPRESSLY CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED IN THE AGREEMENT, THEN (A) DO NOT DOWNLOAD, INSTALL, ACCESS, OR USE ANY SOFTWARE (OR, AS APPLICABLE, ANY PRODUCT IN WHICH ANY SOFTWARE IS EMBEDDED), AND (B) WITHIN THIRTY (30) DAYS AFTER RECEIPT OF ANY SOFTWARE (OR, IF AN AGREEMENT BETWEEN BUYER AND CELLEBRITE PROVIDES A SHORTER TIME PERIOD FOR ACCEPTANCE, SUCH SHORTER TIME PERIOD FOR ACCEPTANCE), EITHER RETURN SUCH SOFTWARE TO CELLEBRITE OR TO THE APPLICABLE AUTHORIZED RESELLER FOR FULL REFUND OF THE SOFTWARE LICENSE FEE, OR, IF SUCH SOFTWARE IS EMBEDDED IN A PRODUCT FOR WHICH NO SEPARATE SOFTWARE LICENSE FEE WAS CHARGED, RETURN SUCH PRODUCT AND EMBEDDED SOFTWARE, UNUSED, TO CELLEBRITE OR TO THE APPLICABLE AUTHORIZED RESELLER FOR A FULL REFUND OF THE LICENSE FEE PAID FOR THE APPLICABLE SOFTWARE EMBEDDED IN SUCH PRODUCT. YOUR RIGHT TO RETURN AND REFUND ONLY APPLIES IF YOU ARE THE ORIGINAL END USER PURCHASER OF SUCH PRODUCT AND/OR LICENSEE OF SUCH SOFTWARE.#

This EULA governs Buyer's access to and use of any Software and/or any Product (as defined below) first placed in use by Buyer on or after the release date of this EULA (the "Release Date").#

1. **DEFINITIONS –** In this Agreement, the following capitalized terms shall have the meaning set forth below:#
   "Affiliate" of a party means such party's parent corporation, an entity under the control of such party's parent corporation at any tier or an entity controlled by such party at any tier. For these purposes, "control" shall mean the power to direct or cause the direction of the management and policies of the entity, whether through the ownership of more than 50% of the outstanding voting interests in such entity or otherwise.#

Cellebrite EULA

"Agreement" means this EULA, combined with the Cellebrite General Terms and Conditions (the "GTC") which is incorporated by reference herein, and any additional terms agreed upon in writing and signed by Buyer and Cellebrite.#

"Authorization Product" means a product sold by Cellebrite or an authorized reseller of Cellebrite with embedded License Authorization Software, including but not limited to a USB dongle with embedded License Authorization Software.#

"Authorized Users" means the number of Users that Buyer is licensed to have access to the applicable Software, which may include Concurrent Users and/or Named Users, all as set forth in the Agreement. If the number of Authorized Users is not otherwise set forth in the Agreement, the number of Authorized Users shall be deemed to be equal to the number of Products (other than Authorization Products) purchased by Buyer.#

"Beta Software" means a pre-commercial, evaluation, pilot, "alpha", or "beta" version of the Software.#

"Cellebrite" means Cellebrite DI Ltd. or its Affiliate that has an agreement with Buyer and/or issues invoices to Buyer with respect to any Software and/or Product, as applicable.#

"Cellebrite Mobile Elite aaS" means the Cellebrite Mobile Elite as a Service solution to be provided to You by Cellebrite pursuant to any applicable order form and/or quote issued to you by Cellebrite and/or purchase order and/or agreement.#

"Cellebrite PaaS" means the Cellebrite Premium as a Service solution to be provided to You by Cellebrite pursuant to any applicable order form and/or quote issued to you by Cellebrite and/or purchase order and/or agreement.#

"Concurrent Users" means the number of Authorized Users (whether Named Users or not) of Buyer concurrently and/or simultaneously accessing, using or otherwise enjoying the benefit (except reviewing results of analyses generated by Software) of Software, either directly or indirectly from a remote location. If a single User connects to Software using multiple concurrent log-ins or connections, each such active logical connection or log-in is counted toward the number of Concurrent Users.#

"Documentation" means any documentation related to any Software provided by Cellebrite.#

"Embedded Software" means a copy of Software delivered embedded in or loaded onto a Product when such Product is sold by Cellebrite. Any Updates or Upgrades to Embedded Software are also deemed "Embedded Software", notwithstanding being separately delivered from the applicable Product.#

"Law" shall mean any law, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction or requirement of or by any governmental authority, as may be amended, changed or updated from time to time.#

"License Authorization Software" means Software that is provided together with hardware on which it is embedded that is used to validate the authorized use of standalone Software.#

"License Term" means the term of a paid subscription to an instance of Software or a unit of Product.#

"Named Users" means a User authorized by Buyer to access or use the Software through the assignment of a single user ID, regardless of whether such User is using Software at any given time. A non-human device capable of accessing or access Software is counted as a Named User.#

Cellebrite EULA

"Product" means a product (hardware and Software) manufactured by Cellebrite. The term "Product" includes without limitation the UFED Pro series, UFED field series and Analytics series of products. "Product" includes Authorization Products.#

"Remote Access Protocol" means any remote access application, including without limitation Remote Desktop Protocol (RDP) and Windows Remote Management (WinRM), used to connect a single remote computer (*e.g.*, a laptop) to a single host computer (*e.g.*, a desktop) with an Authorization Product directly connected to such host computer for each Authorization Product then licensed by Buyer, as long as such Authorized User, single remote computer and single host computer with an Authorization Product are all located in the Territory.#

"Software" means an instance of a program, module, feature, function, service, application, operation or capability of any Cellebrite-supplied software. The term "Software" includes without limitation any Embedded Software, Upgrade, Update, standalone software or any License Authorization Software.#

"Territory" means the country (not including external territories) in which Product was purchased or Software was licensed from Cellebrite or an authorized reseller of Cellebrite.#

"Third Party" means an individual or entity other than Buyer, Cellebrite and Cellebrite's Affiliates.#

"Third Party Software" means certain software provided by a Third Party embedded in any Product, either as a standalone feature or as part of any Software, and which may be subject to additional end user license restriction and agreements.#

"Update" means an update to any Software that is provided by Cellebrite and that may incorporate (i) corrections of any substantial defects; (ii) fixes of any minor bugs; (iii) at the sole discretion of Cellebrite, allowing additional compatibility of the Software with mobile devices provided by Third Parties; and/or (iv) at the sole discretion of Cellebrite, minor enhancements to the Software; provided, however, that Updates shall not include Upgrades. Updates are generally identified by Cellebrite by a change to the version number to the right of the first decimal point (*e.g.*, version 4.1 to 4.2).#

"Upgrade" means a new release of any Software that incorporates substantial changes or additions that (i) provide additional value and utility; (ii) may be priced and offered separately as optional additions to any Software; and/or (iii) are not generally made available to Cellebrite's customers without a separate charge. Upgrades are generally identified by Cellebrite by a change to the version number to the left of the first decimal point (*e.g.*, version 4.2 to 5.0).#

"User" means an individual able to gain access to any Software functionality.#

"You" means any individual seeking the benefit of or evaluating this EULA.#

2. LICENSE GRANT#

#

A. Software. Subject to the terms and conditions of this EULA, during the License Term, Cellebrite grants Buyer, and Buyer accepts, upon delivery of any Software, a non-exclusive, non-transferable, royalty free, and non-sublicensable license to the Software to (i) allow Authorized Users to use such Software, in executable form only, and any accompanying Documentation, only for Buyer's internal use in connection with the Products, in the Territory (or any other location specifically authorized by Cellebrite in writing) and only as authorized in the Agreement, and subject to the terms hereof; ii) make a reasonable number of copies of Software, (except with respect to Embedded Software), for use only as licensed in this EULA, though in no case more than the number of Authorized Users; and (iii) make one (1) copy of Software, (except with respect to Embedded Software), for backup, archival or disaster recovery purposes.#

Cellebrite EULA

#

i. Embedded Software Limitations. Buyer may only use Embedded Software for execution on the unit of Product originally delivered to Buyer with such Embedded Software installed or any replacement unit provided under a warranty from Cellebrite. Any Update or Upgrade of such Embedded Software that Cellebrite has licensed to Buyer may be loaded and executed only on the unit of Product on which any originally licensed Software is authorized to execute.#

#

ii. License Exclusion. Notwithstanding anything to the contrary, except as may otherwise be required by applicable Law, no license is granted for installation or use of any Software on any Product resold by anyone who is not an authorized reseller of Cellebrite for such Product.#

#

iii. Single Product; Single Authorization Product. Buyer's license to any Embedded Software is limited to a license to use such Embedded Software on one (1) Product for each Product purchased from Cellebrite or Cellebrite's authorized reseller. Buyer's license to any License Authorization Software is limited to a license to use such License Authorization Software on one (1) Authorization Product for each license to such standalone Software the authorized use of which is validated by such License Authorization Software and where such license is purchased from Cellebrite or Cellebrite's authorized reseller.#

#

iv. Authorization Products. Without limiting Section 2.D, Buyer shall not, and shall not permit any User to, use any Authorization Product on a computer other than the computer to which such Authorization Product is directly connected (*i.e.* not through a network), except that an Authorized User may use Remote Access Protocol with Cellebrite's UFED Physical Analyzer. Buyer shall ensure that multiple users cannot use Remote Access Protocol to access UFED Physical Analyzer simultaneously. For the avoidance of doubt, subject to the terms and conditions of this EULA, sharing a USB dongle among Concurrent Users is permitted.#

#

v. Remote Access Protocol. Buyer expressly acknowledges, agrees and warrants that except as required for use by Concurrent Users as allowed by the Agreement and as provided herein each computer running an Authorization Product will be configured or at least limited to serve only one remote connection at a time. In other words, only one Authorized User can use a Remote Access Protocol at the same time. For example, if a host computer is installed with multiple instances of Cellebrite's UFED Physical Analyzer, Buyer will ensure that it is not possible for multiple remote users to connect to the host computer and/or ensure that the foregoing does not occur. Regarding any other Cellebrite products or software other than Cellebrite's UFED Physical Analyzer, Buyer may not use a Remote Access Protocol unless expressly agreed to in writing by Cellebrite. Regarding Endpoint Inspector and/or Endpoint Mobile, it is hereby clarified and agreed that: (i) Buyer may use Remote Access Protocol and allow Authorized and Concurrent Users to use outside of Territory, as detailed in the Agreement; and (ii) Cellebrite may, at its sole discretion, inform any Endpoint Inspector and/or Endpoint Mobile's custodian about the nature of the use of the Endpoint Inspector and/or Endpoint Mobile application that will be installed and/or operated on or in relation to the custodian's device.#

#

vi. Named Users. If the Agreement specifies that any Software may be used by Named Users, Buyer shall (i) assign a unique login credential for access and use of the Software to each Named User, (ii) ensure that the Software is used only by the applicable Named Users, (iii)

Cellebrite EULA

ensure that Users do not share login credentials, and (iv) maintain the security and confidentiality of its Named User login credentials.#

#

vii. Concurrent Users. If the Agreement specifies that any Software may be used by Concurrent Users, Buyer may install one instance of such Software on one (1) designated host server for concurrent and simultaneous use and/or access by the applicable number of Concurrent Users. The number of Concurrent Users accessing such Software at any time may not exceed the number of Concurrent Users specified in the Agreement. Buyer must keep a record of all Authorized Users who are Concurrent Users.#

#

viii. Former BlackBag Software Users. Each copy of the Inspector, Digital Collector, Mobilyze, or SoftBlock Software may only be used, executed, or displayed by one (1) Authorized User and on one Licensed System at any given instance. The term "**Licensed System**" means a computer to which an activation key provided by BlackBag has been connected or accessed, as authorized by BlackBag in the applicable License Confirmation.#

ix. Cellebrite PaaS and Mobile Elite aaS Access and Use. Subject to Your compliance with the terms and conditions contained in this EULA and/or in any applicable order form and/or quote issued to You by Cellebrite and/or purchase order and/or agreement, Cellebrite hereby grants to You, during the relevant Cellebrite PaaS or Mobile Elite aaS (either services, for the purpose of this Section, the "**Service**") License Term, a limited, non-exclusive, non-transferable (a) right to access and use the Service in accordance with any relevant printed, paper, electronic or online user instructions and help files made available by Cellebrite for use with the Service, as may be updated from time to time by Cellebrite, and (b) license to download any relevant software if software is offered by Cellebrite for the purpose of using the Service, in each case solely for Your internal business purposes and not for the benefit of any other person or entity. By accessing and/or using the Service, You expressly acknowledge and agree that certain operational required information shall be shared with Cellebrite for the purpose of providing the service. Such information may include the number of unlocking actions purchased by You and/or left for Your use, types of software downloaded by You for the purpose of using the Service, etc. The Service may be affected by factors beyond Cellebrite's control and may not be continuous and uninterrupted. You acknowledge that the service may be subject to limitations and/or delays inherent in the use of the internet and electronic communications, and Cellebrite is not responsible or liable for any delays, delivery failures or other damage resulting from those technical difficulties beyond its control.

x. Premium and Mobile Elite Placement and Use. Any Premium and Mobile Elite Product, including Products connected by the Buyer to the Premium and/or Mobile Elite Product, may only be placed and used inside a room, lab, office. Premium Mobile may be placed and used anywhere in the Territory where security measures are consistent with sensitive activities. Cellebrite recommends to the Buyer having its Authorized Users certified for using and operation Premium and/or Mobile Elite, as applicable, and offers the top valued certifications in the field.

#

B. Software Provisions.#

#

i. Any use or operation of the Product, including the Software, with any product and/or mobile device developed, manufactured, produced, programmed, assembled and/or otherwise

Cellebrite EULA

maintained by any person or entity shall be permitted only after the User has obtained any consents or approvals required (to the extent required) pursuant to applicable Law.#

#

ii. TO THE EXTENT PERMITTED BY STATE LAW, UNDER NO CIRCUMSTANCES SHALL CELLEBRITE, ITS OFFICERS, EMPLOYEES OR REPRESENTATIVES BE LIABLE TO BUYER, USER OR ANY THIRD PARTY UNDER ANY CAUSE OF ACTION (WHETHER IN CONTRACT, TORT OR OTHERWISE) FOR ANY INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY OR OTHER INDIRECT DAMAGES UNDER ANY LEGAL THEORY ARISING OUT OF OR RELATING TO THE USE OF ANY OF THE CELLEBRITE SOFTWARE IN CONNECTION WITH ANY PRODUCT AND/OR MOBILE DEVICE DEVELOPED, MANUFACTURED, PRODUCED, PROGRAMMED, ASSEMBLED AND/OR OTHERWISE MAINTAINED BY ANY PERSON OR ENTITY, WITHOUT OBTAINING EACH APPLICABLE CONSENT AND APPROVAL.#

#

iii. No Obligation. Nothing in this EULA requires Cellebrite to provide Updates or Upgrades to Buyer or Buyer to accept such Updates or Upgrades.#

#

iv. Trial and Beta Software Licenses. Subject to the terms and conditions of this Agreement, Cellebrite may grant Buyer with, and Buyer accepts, a nonexclusive, time-limited and nontransferable license, effective upon delivery, to use a copy of Software or a Beta Version of the Software, in executable form only, and any accompanying Documentation, only for Buyer's internal use to test, trial or evaluate such Software and/or provide feedback to Cellebrite with respect thereto, in the Territory, and not for any business or productive purposes, for a period as specified by Cellebrite at its sole discretion, and subject to the restrictions in Section 2.#

#

Buyer assumes all risks and all costs associated with its use of the Trial and/or Beta Software, any obligations on behalf of Cellebrite to indemnify, defend, or hold harmless under this Agreement are not applicable to Buyer's use of any Trial and/or Beta Software. To the extent permitted by state law, Buyer's sole and exclusive remedy with respect to such Trial and/or Beta Software is termination of the license thereto. There is no guarantee that features or functions of the Trial and/or Beta Software will be available, or if available will be the same, as in the general release version of the Software. Cellebrite will be under no obligation to provide Buyer any maintenance or support services with respect to the Trial and/or Beta Software.#

#

IT IS CLARIFIED THAT THE LICENSE UNDER THIS SUB-SECTION IV IS PROVIDED "AS IS", WITHOUT ANY WARRANTY WHATSOEVER. TO THE EXTENT PERMITTED BY STATE LAW, CELLEBRITE DISCLAIMS ALL IMPLIED WARRANTIES, CONDITIONS AND REPRESENTATIONS IN RELATION TO THE TRAIL AND/OR BETA SOFTWARE, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, DURABILITY OR NON-INFRINGEMENT. TO THE EXTENT PERMITTED BY STATE LAW, IN NO EVENT WILL MAGNET FORENSICS BE LIABLE TO YOU OR TO ANY OTHER PARTY FOR ANY LOSS, DAMAGE, COST, INJURY OR EXPENSE, INCLUDING LOSS OF TIME, MONEY OR GOODWILL, OR FOR DAMAGES OF ANY KIND, WHETHER

Cellebrite EULA

DIRECT, SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL IN RELATION TO THE TRAIL AND/OR BETA SOFTWARE.#

#

v. Buyer represents, warrants and covenants to Cellebrite that (a) only Users of Buyer who have obtained any necessary consents and approvals pursuant to applicable Law shall be permitted to use any of the Products and/or Software; (b) Users of Buyer shall only use any of the Products and/or Software in compliance with the terms of service, terms of use or other agreement with a Third Party; and (c) Buyer and its Users shall only use any of the UFED family of Products in compliance with all applicable Laws.#

#

C. License Prohibitions. Notwithstanding anything to the contrary, Buyer shall not, and shall not permit, authorize or engage any Third Party to:#

i. modify, reverse compile, reverse assemble, reverse engineer or otherwise translate all or any portion of any Software, or create derivative works thereof;#

ii. assign, pledge, rent, lease, sublicense, share, distribute, sell or otherwise transfer the Software, any copy thereof, or any rights granted hereunder, to any third party, including without limitation selling any Product in a secondhand market;;#

iii. use any Software to provide service to any Third Party including by use on a time sharing, service bureau, application service provider (ASP), software as a service (SAAS), cloud services, rental or other similar basis;#

iv. make copies of or reproduce of any Software and/or Documentation, except as provided for in the license grant above;#

v. remove, alter, deface, cover, obfuscate or destroy any proprietary markings, copyrights notices, proprietary legends, labels or marks placed upon or contained within any Products and/or Software (including, without limitation, any copyright or other attribution statements such as for open source software);#

vi. use any Embedded Software other than with Products provided by Cellebrite or an authorized reseller of Cellebrite or for more than the number of Products purchased from Cellebrite or an authorized reseller of Cellebrite;#

vii. disclose any results of testing or benchmarking of any Software to any Third Party;#

viii. use any Update or Upgrade beyond those to which Buyer is entitled or with any Software to which Buyer does not have a valid, current license;#

ix. deactivate, modify or impair the functioning of any disabling code in any Software;#

x. circumvent or disable Cellebrite's copyright protection mechanisms or license management mechanisms;#

xi. use the Product, any Software or any Third Party Software, alone or in combination with other activities, products or services, in any activity or manner that violates or supports, assists, facilitates, enables, constitutes or is otherwise deemed to be in violation of:#

(1) any order, regulation or Law (including but not limited to any Law with respect to human rights or the rights of individuals) or to support any illegal activity;#

(2) any human rights standards of any person, group, or community, and best practice including internationally recognized human rights instruments, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights,

and the International Labor Organization Declaration on Fundamental Principles and Rights at Work;#

(3) any rights of any Third Party.#

xii. use any Product for any training purposes, other than for training Buyer's employees, where Buyer charges fees or receives other consideration for such training, except as authorized by Cellebrite in writing;#

xiii. combine or operate any Products or Software with other products or software, without prior written authorization of Cellebrite or its Affiliates, including without limitation any installation of any software on any Product; or,#

xiv. attempt any of the foregoing.#

#

The licenses set out hereunder are at all times subject to these prohibitions and any contravention thereof shall constitute a material breach of this Agreement. Cellebrite expressly reserves the right to seek all available legal and equitable remedies to prevent any of the foregoing and to recover any lost profits, damages or costs resulting from any of the foregoing.#

#

For the purpose of this Section, it is hereby clarified that "Third Party" shall include: Buyer's affiliates, employees, contractors, licensors, suppliers or customers. If the event that the Buyer is a governmental body the followings shall also be included: any federal, state, local, judicial or other governing body having jurisdiction over any of the foregoing.#

#

D. Legal Exception. Buyer agrees that, to the extent that any applicable Law (including without limitation national laws implementing 2009/24/EC on the Legal Protection of Computer Programs) grants Buyer the right to reverse engineer any Software to make it interoperable without Cellebrite's consent, before Buyer exercises any such rights, Buyer shall notify Cellebrite of such desire and, no later than sixty (60) days following receipt of such request, Cellebrite may decide either to: (a) perform the work to achieve such interoperability and charge its then-standard rates for such work to Buyer; or (b) permit Buyer to reverse engineer parts of such Software only to the extent necessary to achieve such interoperability. Only if and after Cellebrite, at its sole discretion, partly or completely denies Buyer's request, shall Buyer exercise its statutory rights.#

#

E. Network Usage. Buyer understands and agrees that Cellebrite may use Buyer's internal network and Internet connection for the limited purpose of transmitting license-related data at the time of installation, registration, use or update of Software to a Cellebrite-operated license server. At such time, Cellebrite may validate the license-related data in order to protect Cellebrite against unlicensed or illegal use of any Software. At its option, Cellebrite may only permit activation of Software upon exchange of license related data between Buyer's computer and the Cellebrite license server.#

#

F. Third Party Software. Buyer acknowledges and agrees that the access and use of any Software (or certain features thereof) may involve access and/or use of Third Party Software. In addition to the Agreement, Buyer shall comply with the terms and conditions applicable to any such Third Party Software, including without limitation the following terms and conditions:#

#

i. Bing Maps - included herein as part of this document#

#

ii. OpenStreetMap – included herein as part of this document

Cellebrite EULA

iii. Chainalysis – terms to be negotiated at the Purchase Order Level, if purchased by Buyer

G. No Implied Licenses. Except for the express licenses set forth herein, Cellebrite does not grant any license to Buyer, whether by implication or otherwise.

H. Open Source Software.

i. Software may use and/or be provided with third party open source software, libraries or other components ("Open Source Component"), including those detailed in the open source notices files separately conveyed to You. To the extent so stipulated by the license that governs each Open Source Component ("Open Source License"), each such Open Source Component is licensed directly to Buyer from its respective licensors and not sublicensed to Buyer by Cellebrite, and such Open Source Component is subject to its respective Open Source License, and not to this Agreement. If, and to the extent, an Open Source Component requires that this Agreement effectively impose, or incorporate by reference, certain disclaimers, permissions, provisions, prohibitions or restrictions, then such disclaimers, permissions, provisions, prohibitions or restrictions shall be deemed to be imposed, or incorporated by reference into this Agreement, as required, and shall supersede any conflicting provision of this Agreement, solely with respect to the corresponding Open Source Component which is governed by such Open Source License.

ii. If Buyer or another party on its behalf, modifies, replaces or substitutes any Open Source Component used in or provided with this Software, Buyer hereby fully, forever, irrevocably and unconditionally releases and discharges Cellebrite, its Affiliates and its and their employees, officers, directors, resellers, distributors and representatives (collectively, "Released Parties") from any and all claims, charges, complaints, demands, actions, causes of action, suits, rights, debts, covenants, liabilities, warranties, performance and maintenance and support obligations (collectively, "Released Claims"), of every kind and nature, with respect to such Software, including without limitation any such Released Claims that arise as a matter of applicable Law.

iii. If an Open Source License requires that the source code of its corresponding Open Source Component be made available to Buyer, and such source code was not delivered to Buyer with the Software, then Cellebrite hereby extends a written offer, valid for the period prescribed in such Open Source License, to obtain a copy of the source code of the corresponding Open Source Component, from Cellebrite. To accept this offer, Buyer shall contact Cellebrite at support@cellebrite.com.

I. Personal Data. The parties acknowledge and agree that: (a) Within the scope of this Agreement, the Product is an on-premise solution used and operated solely by Buyer without the involvement of Cellebrite; (b) Cellebrite is not engaged in any processing of 'personal data' (as this term is used in Laws governing data privacy and data protection) that flows through the Product; and therefore (c) with respect to Cellebrite activities in the scope of this Agreement, Cellebrite is neither a 'data controller' nor 'data processor' (as these terms are used in Laws governing data privacy and data protection).

3. OWNERSHIP

A. Title to Software. Notwithstanding anything to the contrary, Software furnished hereunder is provided to Licensee subject to and in accordance with the terms and conditions of the EULA. All

title and interest of the Software and and/or any related Documentation and any derivative works thereof shall remain solely and exclusively with Cellebrite or its licensors, as applicable. Nothing in this Agreement constitutes a sale, transfer or conveyance of any right, title or interest in any Software and/or Documentation or any derivative works thereof. Therefore, any reference to a sale of Software shall be understood as a license to Software under the terms and conditions of the Agreement. In the event of any conflict between the GTC and the EULA, the EULA shall take precedence over the GTC in all matters related to the Software.#

#

B. Intellectual Property. All intellectual property rights relating to the Software and/or the Products, including without limitation, all patents, trademarks, algorithms, binary codes, business methods, computer programs, copyrights, databases, know-how, logos, concepts, techniques, processes, methods, models, commercial secrets and any other intellectual property rights, including any new developments or derivative works of such intellectual property, whether registered or not, are and shall remain the sole and exclusive property of Cellebrite or its licensors, as applicable. All right, title and interest in and to any inventions, discoveries, improvements, methods, ideas, computer and other software or other works of authorship or other forms of intellectual property which are made, created, developed, written, conceived of or first reduced to practice solely, jointly with Licensee or on behalf of Licensee shall be and remain with Cellebrite or its licensors, as applicable. Any suggestions, improvements or other feedback provided by Licensee to Cellebrite regarding any Products, Software or services shall be the exclusive property of Cellebrite. Licensee hereby freely assigns any intellectual property rights to Cellebrite in accordance with this Section, including any moral rights, and appoints Cellebrite as its attorney-in-fact to pursue any such intellectual property rights worldwide. #

#

4. **CONFIDENTIALITY –** The parties may each disclose to the other proprietary information related to the subject of the Agreement ("Confidential Information"). Software, Documentation, Trade Secrets, and any technical information related thereto are Confidential Information of Cellebrite without any marking requirement, but any other information disclosed in writing must be marked "confidential" or "proprietary" to be deemed the Confidential Information of a party. Information disclosed orally may be deemed Confidential Information if the disclosing party says it is proprietary and summarizes it in a writing to the other party within twenty (20) days of the oral disclosure.#

Pursuant to 18 U.S.C. §1833(b) , Buyer shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of Cellebrite's Trade Secrets (as defined below) only if such disclosure is made: (i) in confidence to a Federal, State, or local government official or to an attorney, solely for the purpose of reporting or investigating a suspected violation of law; or (ii) in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. In court proceedings claiming retaliation by Cellebrite for Buyer's reporting a suspected violation of law, Buyer may only disclose Cellebrite Trade Secrets to Buyer's legal counsel and may only use the Trade Secret information, if Buyer (i) files documents containing Trade Secrets under seal; and (ii) Buyer does not otherwise disclose Cellebrite Trade Secrets, except pursuant to a court order.#

The term "Trade Secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (a) Cellebrite has taken reasonable measures to keep such information secret; and (b) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.#

Cellebrite EULA

The receiving party shall: (a) hold Confidential Information in confidence using the same degree of care as it normally exercises to protect its own proprietary information but at least reasonable care, (b) restrict disclosure and use of Confidential Information to only employees (including any agents, contractors or consultants) with a need to know who are advised of their obligations with respect to Confidential Information, (c) not copy, duplicate, reverse engineer or decompile Confidential Information, (d) use Confidential Information only in furtherance of performance under the Agreement, and (e) upon expiration or termination of the Agreement, at the disclosing party's option, destroy or return all Confidential Information to the disclosing party.#

The receiving party shall have no obligation regarding Confidential Information that: (a) was previously known to it free of any confidentiality obligation, (b) was independently developed by it, (c) is or becomes publicly available other than by unauthorized disclosure, (d) is disclosed to third parties by the disclosing party without restriction, (e) is received from a third party without violation of any confidentiality obligation or (f) that is disclosed pursuant to law.#

If a party is faced with legal action or a requirement under applicable Law to disclose or make available Confidential Information received hereunder, such party shall promptly notify the disclosing party and, upon request of the latter, cooperate in contesting such action or requirement, Neither party shall be liable for damages for any disclosure or unauthorized access pursuant to legal action or applicable Law or for inadvertent disclosure, access, or use if the customary degree of care as it uses with respect to its own proprietary information has been exercised and if, upon discovery of such inadvertent disclosure, access, or use the receiving party has endeavored to prevent any further (inadvertent or otherwise) disclosure or use.#

5. EXCLUSIVE REMEDIES AND LIMITATION OF LIABILITY.#

#

A. Definitions. For purposes of the exclusive remedies and limitations of liability set forth in this Section 5, Cellebrite shall be deemed to include its Affiliates and its and their directors, officers, employees, agents, representatives, shareholders, subcontractors and suppliers; and "damages" shall be deemed to refer collectively to all injury, damage, loss or expense incurred.#

#

B. Exclusive Remedies. To the extent permitted by state law, Cellebrite's entire liability and Buyer's exclusive remedies against Cellebrite for any damages caused by any Product or Software defect or failure, or arising from the performance or non-performance of any obligation under the Agreement, regardless of the form of action, whether in contract, tort including negligence, strict liability or otherwise shall be:#

#

i. For bodily injury or death to any person proximately caused by Cellebrite, Buyer's direct damages; and#

ii. For all other claims, Cellebrite's liability shall be limited to direct damages that are proven, in an amount not to exceed the total amount paid by Buyer to Cellebrite during the twelve (12) month period that immediately preceded the event that gave rise to the applicable claim.#

#

C. Limitation of Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY, TO THE EXTENT PERMITTED BY STATE LAW, CELLEBRITE SHALL NOT BE LIABLE FOR INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL OR OTHER INDIRECT DAMAGES, INCLUDING BUT NOT LIMITED TO LOST PROFITS, SAVINGS OR REVENUES OF ANY KIND, WHETHER OR NOT CELLEBRITE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS PROVISION SHALL APPLY EVEN IN THE EVENT OF THE FAILURE OF AN EXCLUSIVE REMEDY.#

Cellebrite EULA

#

D. No Liability to any Third Party. TO THE MAXIMUM EXTENT PERMITTED BY STATE LAW , CELLEBRITE DISCLAIMS ANY AND ALL LIABILITIES OR OBLIGATIONS WHATSOEVER RELATED TO ANY PRODUCT OR SOFTWARE OR LICENSING OF ANY SOFTWARE TO, OR USE BY, ANYONE OTHER THAN BUYER.#

#

E. Third Party Software Liability. Notwithstanding anything to the contrary, Cellebrite shall not be liable to Buyer or any User for any damages due to use of any Third Party Software. The limitations and exclusions from liability under the terms and conditions applicable to any Third Party Software (which are applicable to the arrangement between Buyer and the applicable provider of such Third Party Software) shall govern and apply with respect to the use of each such Third Party Software. Additionally, Cellebrite does not provide any warranty with respect to any Third Party Software. The warranty provided by the terms and conditions applicable to any Third Party Software (which are applicable to the arrangement between Buyer and the applicable provider of such Third Party Software) shall apply to Third Party Software.#

#

6. **BUYER INDEMNITY** – To the maximum extent permitted by state Law, Buyer shall, at its expense: (i) indemnify and hold Cellebrite and its Affiliates and its and their directors, officers, employees, agents, representatives, shareholders, subcontractors and suppliers harmless from and against any damages, claim, liabilities and expenses (including without limitation legal expenses) (whether brought by a Third Party or an employee, consultant or agent of Buyer's) arising out of any (a) misuse or use of any Product or Software furnished under the Agreement in a manner other than as authorized under this EULA, including without limitation using the Product or Software in a manner that violates applicable Law including without limitation a person's Fourth Amendment rights under the United States Constitution (or its equivalent in the Territory); (b) misappropriation of any personal information, (c) failure to obtain consents and approvals required by applicable Law for the use of any of the Cellebrite's Products or Software, or; (g) use of any Product or Software in breach of or to violate the terms of any other agreement with a Third Party; (ii) reimburse Cellebrite for any expenses, costs and liabilities (including without limitation legal expenses) incurred relating to such claim; and (iii) pay all settlements, damages and costs assessed against Cellebrite and attributable to such claim. The maximum liability of Buyer in relation to any claims under this Section 6 shall not exceed the amounts paid by Buyer to license the infringing Software or purchase Products including the infringing Software in the twelve (12) months immediately preceding the claim.

#

Buyer's obligations under this Section 6 are conditioned upon: (1) Cellebrite cooperating fully with Buyer to facilitate the defense or settlement of such claim; and (2) Cellebrite's substantial compliance with the Agreement.#

#

7. **CELLEBRITE INDEMNITY** – Cellebrite will, at its expense: (i) indemnify, defend and hold Buyer and its Affiliates and its and their officers and directors harmless from any Third Party claim to the extent alleging that any Software furnished under this Agreement directly infringes any patent, copyright or trademark or misappropriates any trade secret, in each case having legal effect in the Territory; (ii) reimburse Buyer for any expenses, costs and liabilities (including reasonable attorney's fees) incurred relating to such claim; and (iii) pay all settlements, damages and costs assessed against Buyer and attributable to such claim.#

In connection with satisfying its obligations hereunder, Cellebrite may, at its option and expense: (a) procure for Buyer and/or its customers the right to continue using such Software or any Product on which such Software is embedded; (b) replace or modify any such Software or any Product on which

Cellebrite EULA

such Software is embedded, to be free of such infringement; or (c) require return of such Software or any Product on which such Software is embedded, and refund the purchase price or license price depreciated on a straight-line basis over a three (3) year period from the delivery date.#

Cellebrite shall have no obligations under this Section 7 with respect to any Excluded Item. The maximum liability of Cellebrite in relation to any claims under this Section 7 shall not exceed the amounts paid by Buyer to license the infringing Software or purchase Products including the infringing Software in the twelve (12) months immediately preceding the claim. If there are any other indemnification obligations with respect to infringement of any patent, copyright or trademark or misappropriation of any trade secret under the Agreement, this Section 7 shall be of no force and effect.#

Cellebrite's obligations under this Section 7 are conditioned upon: (1) Buyer giving Cellebrite prompt written notice (within no more than thirty (30) days) after any such claim, unless Cellebrite would not be materially prejudiced thereby; (2) Cellebrite having complete control of the defense and settlement of such claim; (3) Buyer cooperating fully with Cellebrite to facilitate the defense or settlement of such claim; and (4) Buyer's substantial compliance with the Agreement.#

The sale of any Product by Cellebrite shall not in any way confer upon Buyer, or upon anyone claiming under Buyer, any license (expressly, by implication, by estoppel or otherwise) under any patent claim of Cellebrite or others covering or relating to any combination, machine or process in which such Product is or might be used, or to any process or method of making such Product.#

TO THE EXTENT PERMITTED BY STATE LAW, THE FOREGOING STATES THE SOLE AND EXCLUSIVE REMEDY AND OBLIGATION OF THE PARTIES HERETO FOR INFRINGEMENT OR OTHER VIOLATION OF ANY INTELLECTUAL PROPERTY RIGHTS ARISING OUT OF THIS AGREEMENT AND IS IN LIEU OF ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, IN REGARD THERETO.#

8. DISABLING CODE#

#

A. Disabling Code. Software may be provided to Buyer with code that allows Cellebrite to disable such Software. Except as provided in Section 8.B, Cellebrite will not invoke such disabling code without Buyer's prior consent.#

#

B. Invocation of Disabling Code. Notwithstanding anything to the contrary, Cellebrite may invoke the disabling code without Buyer's consent if (i) Cellebrite reasonably believes that such Software has been, is being, or will be used in violation of Laws; (ii) Cellebrite is required to do so because of a court or regulatory order; (iii) Buyer has not paid an outstanding invoice more than sixty (60) days after such invoice is due, or; (iv) Buyer has used the Software other than as authorized by Buyer's license. Cellebrite shall have no liability to Buyer for any good faith invocation of any such disabling code.#

#

9. TERM AND TERMINATION#

#

A. Term. The term of this EULA is while any Software is under Buyer's control or possession. The License Term shall be determined in a separate agreement between Cellebrite and the Buyer.#

#

B. Termination. Cellebrite or Buyer may terminate this EULA (i) upon thirty (30) days' prior written notice if either party has not cured any material breach of this EULA by the end of such thirty (30) day notice period or (ii) if Buyer has not paid any invoice sixty (60) days after such invoice is due. Upon termination or expiration of this EULA, (a) Buyer shall be responsible for payment for all

purchase orders delivered to Buyer by Cellebrite before the effective date of termination and (b) Buyer shall destroy all copies of any Software under Buyer's control or possession.#

#

C. Survival. The provisions of Sections 1-5, 6, 9, and 10-15 of this EULA shall survive any termination or expiration of this EULA.#

#

10. CHOICE OF LAW; JURISDICTION; GOVERNING LANGUAGE#

#

A. Choice of Law; Jurisdiction.#

#

i. The Parties agree to meet and discuss any dispute or claim relating to the Agreement prior to seeking any judicial resolution, for a period of at least thirty (30) days, during which either party may request confidential mediation. #

#

ii. This Agreement and any disputes or claims arising hereunder are governed by the Laws of the State of Tennessee and subject to the exclusive jurisdiction of the federal or state courts in Tennessee, without giving effect to any conflict of Law rules or principles. Cellebrite may, at its sole discretion, initiate any dispute or claim against Buyer, including for injunctive relief, in any jurisdiction permitted by applicable Law.#

#

#

B. Governing Language. The parties hereto have required that this EULA be drawn in the English language, and that the English language version shall control over any translations thereof. If Buyer is located in Quebec, the following sentence shall apply: Les parties convenient que cette EULA soient rediges en anglais.#

#

11. ASSIGNMENT – Except to the extent otherwise required by applicable Law or expressly provided for assignment generally in the Agreement, no license provided to Buyer is sublicensable, transferable or assignable by Buyer, including by operation of Law, change of control, merger, purchase or otherwise, without the prior written consent of Cellebrite in each instance. Other than as expressly permitted by the foregoing, any attempted sublicense, transfer or assignment by Buyer shall be null and void.#

#

12. NO-WAIVER – No course of dealing or failure of either party to strictly enforce any term, right or condition of the Agreement shall be construed as a waiver of such term, right or condition.#

#

13. ENTIRE AGREEMENT – The terms and conditions contained in this EULA supersede all prior oral or written understandings between the parties and shall constitute the entire agreement between the parties with respect to the subject matter of this EULA, except as provided for in the preamble to this EULA.#

#

14. CONSTRUCTION; SEVERABILITY – The headings used in this EULA are for reference purposes only and will not be deemed to limit, expand or in any way affect the interpretation of any term or provision hereof. If any provision of this EULA is held to be invalid or unenforceable for any reason, the validity, legality, and enforceability of the remaining provisions will not be affected or impaired. The parties shall interpret the affected provision in a manner that renders it enforceable while attempting to closely approximate the intent and effect of the affected provision.#

#

15. GOVERNMENT USE#

Cellebrite EULA

#

A. U.S. Government End Users. The Software was developed exclusively at private expense and qualifies as a "commercial item" consisting of "commercial computer software" and/or "computer software documentation" as such terms are defined and used at FAR (48 C.F.R.) 2.101. Use, duplication or disclosure of the Software by the U.S. Government are subject to restrictions set forth in this Agreement, in accordance with FAR 12.212 and/or DFARS 227.7202-4, as applicable.#

#

B. Incorporation of FAR. If the Licensee is a U.S. federal government entity (or agency thereof), these Terms incorporate the following FAR provisions by reference:#

52.222-50	52.233-3	52.222-54	52.222-21	52.222-26	52.203-6#
52.204-10	52.209-9	52.212-4	52.222-40	52.222-41	52.203-13#
52.222-36	52.222-37	52.233-4	52.212-5	52.209-10	52.222-35#
52.222-53	#				

#

16. INAPPLICABLE TERMS AND PROVISIONS – *VOID AB INITIO*. This Section ***only applies*** to U.S. local, county, state, governmental agencies and other U.S. law enforcement agencies that are state or federally funded by the United States Government. Subject to the foregoing statements, to the extent that any term or provision of the Agreement, is considered ***void ab initio***, or is otherwise unenforceable against the Licensee pursuant to applicable U.S. Law that expressly prohibits Licensee from agreeing to such term or condition, then such conflicting term or provision in this Agreement shall be struck to the extent to make such term or provision enforceable, and the remaining language, if any, shall remain in full force and effect. #

#

Any Licensee policies or procedures which are not expressly required by U.S. Law, shall not apply or be incorporated into the Agreement.#

This Section does *not* apply to any private enterprise, public or private corporation, law firm, consulting company, digital forensics company, non-law enforcement agency, private person, or any other corporate entity that is a Licensee. #

Last Updated: July 1, 2022#

#

Cellebrite EULA

#

* * *#

Appendix I#

#

CELLEBRITE'S STANDARD WARRANTY#

#

A. Hardware Warranty:#

Subject to the remaining Sections of this Appendix I, Cellebrite warrants that each Product, including all firmware but excluding 1) Software, for which the warranty is only as provided under Section B, 2) other Accessories, for which the warranty shall be as provided below, and 3) related services or prototypes of any Product, shall perform in substantial conformance with its Documentation for twelve (12) months after delivery (the "**Warranty Period**"). If any failure to conform to such specification ("**Defect**") is suspected in any Product during the Warranty Period, Licensee, after obtaining return authorisation information from Cellebrite, shall ship suspected defective samples of the Product to Cellebrite in accordance with Cellebrite's instructions at Licensee's expense. No Product will be accepted for repair, replacement, credit or refund without the written authorization of Cellebrite. Cellebrite shall analyse the Defect and any technical information provided by Licensee to verify whether any Defect appears in the Product. #

#

If a returned Product does not have a Defect, Licensee shall pay Cellebrite all costs of handling, inspection, repairs, and transportation at Cellebrite's then-prevailing rates. If a returned Product has a Defect, Cellebrite shall, at its option, either repair or replace the defective Product with the same or equivalent Product without charge. If, after a period of thirty days following Cellebrite's receipt of the returned Product, repair or replacement has not occurred then Cellebrite will credit or refund (at Cellebrite's option) the purchase price, provided: (i) Licensee notifies Cellebrite in writing of the claimed Defect within thirty (30) days after Licensee knows or reasonably should know of the claimed Defect, and (ii) the Defect appears within the Warranty Period. Cellebrite shall ship any replacement Product DAP, excluding Import VAT (Incoterms 2010), to Licensee's destination. Title to any replaced Product or replaced parts of any Product shall pass to Cellebrite upon delivery. #

#

In no event shall Cellebrite be responsible for deinstallation or reinstallation of any Product or for the expenses thereof. Repairs and replacements covered by the above warranty will perform in substantial conformance with the Documentation for a period of (i) six (6) months from the date of repair or replacement or (ii) until the expiration of the original Warranty Period, whichever is later. #

#

Accessories shall perform in substantial conformance with their Documentation for six (6) months after Licensee's receipt (the "**Accessories Warranty Period**"). If any Defect is suspected in any accessories during the Accessories Warranty Period, Licensee, after obtaining return authorisation information from Cellebrite, shall ship suspected defective Accessories to Cellebrite in accordance with Cellebrite's instructions. No Accessories will be accepted for repair or replacement without the written authorisation of Cellebrite. If returned Accessories do not have a Defect, Licensee shall pay Cellebrite all costs of handling, inspection, repairs and transportation at Cellebrite's then-prevailing rates. If returned Accessories have a Defect, Cellebrite shall either repair or replace the defective Accessories with the same or equivalent Accessories without charge. Title in any replaced Accessories shall pass to Cellebrite upon delivery of the replacement Accessories.#

#

Cellebrite EULA

"**Accessories**" shall mean using any peripheral equipment which accompanies, or is used in conjunction with, the Products, including without limitation, cables, kits, connectors or other accessories.#

#

B. Software Warranty:#

#

Cellebrite warrants to Licensee that for a period of sixty (60) days after the date of shipment, the Software will perform substantially in conformance with its Documentation. As Purchaser's sole and exclusive remedy, Cellebrite will, at its sole expense, and as its sole obligation, promptly repair or replace any Software that fails to meet this limited warranty .Software shall be provided with an initial twelve (12) months license which may be renewed by Purchaser for additional terms against payment of the applicable subscription fees to Cellebrite (the "**Software License Period**"). During the Software License Period Cellebrite shall provide Purchaser with periodical Software Updates, at Cellebrite's sole and absolute discretion. #

#

C. Exclusions:#

#

Cellebrite is not responsible for any claimed breach of any warranty caused by: (a) Licensee's use of the Products or Software in violation of Section 2(C) ("License Prohibitions"); (b) placement of the Products or Software in an operating environment contrary to specific written instructions and training materials provided by Cellebrite to Licensee; (c) Licensee's intentional or negligent actions or omissions, including physical damage, fire, loss or theft of a Product; (d) cosmetic damage to the outside of a Product, including ordinary wear and tear, cracks or scratches; (e) for any Product with a touch screen, any Defect in such a touch screen after thirty (30) days from the date of receipt of such Product, or any Defect caused in a touch screen by Licensee's negligence or wilful misconduct; (f) maintenance of the Products or Software in a manner that is contrary to written instructions provided by Cellebrite to Licensee; (g) a product or service not provided, authorised or approved by Cellebrite for use with the Products or Software; (h) any repair services not authorised or approved by Cellebrite; (i) any design, documentation, materials, test data or diagnostics supplied by Licensee that have not been authorised or approved by Cellebrite; (j) usage of any test units, experimental products, prototypes or units from risk lots (each of which is provided "AS IS" to the maximum extent permissible by law); (k) any third party original equipment manufacturer's restrictions on individual phones or models of phones that prevent the phones or models of phones from working with the Products or Software; (l) any damage to a third party device alleged to or actually caused by or as a result of use of a Product or Software with a device; (m) any Products that have had their serial numbers or month and year of manufacture or shipment removed, defected or altered; (n) any interactions or other effects relating to or arising out of the installation of copies of the Software beyond the number of copies authorised by an agreement between Cellebrite and Licensee; (o) use of Products or Software incorporated into a system, other than as authorised by Cellebrite; or (p) any Products or Software that has been resold or otherwise transferred to a third party by Licensee (any Product or Software affected by the cases in (a)-(p) is referred to hereinafter as an "**Excluded Item**"). The warranties herein do not apply to, and Cellebrite makes no warranties with respect to the computer or other platform on which the Software is installed or otherwise embedded.

#

#

Cellebrite EULA

D. Warranty Limitations:#

#

EXCEPT AS STATED IN THIS WARRANTY, TO THE MAXIMUM EXTENT PERMITTED BY STATE LAW, CELLEBRITE, ITS SUBSIDIARIES AND AFFILIATES, SUBCONTRACTORS AND SUPPLIERS EXPRESSLY DISCLAIM ALL OTHER REPRESENTATIONS, WARRANTIES, AND CONDITIONS, EXPRESS OR IMPLIED, AT COMMON LAW OR BY STATUTE, AND SPECIFICALLY DISCLAIM ANY WARRANTY AND/OR CONDITION RELATING TO THE PRODUCTS, SERVICES, OR THE CONFIDENTIAL INFORMATION, INCLUDING THOSE OF MERCHANTABILITY, ACCURACY, PATENT SUFFICIENCY, FITNESS FOR A PARTICULAR PURPOSE, USE, VALUE, NONVIOLATION OF PRIVACY RIGHTS, OR NONINFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, AND ALL WARRANTIES ARISING FROM ANY COURSE OF DEALING OR PERFORMANCE OR USAGE OF TRADE, AND THE EQUIVALENTS THEREOF UNDER THE LAWS OF ANY JURISDICTION OR THAT THE PRODUCTS WILL BE OF SATISFACTORY QUALITY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, LICENSEE'S SOLE AND EXCLUSIVE REMEDY FOR FAILURE OF AN ITEM TO CONFORM WITH ITS SPECIFICATIONS SHALL BE CELLEBRITE'S OBLIGATION (i) TO REPAIR OR (ii) TO REPLACE OR, (iii) IF NEITHER (i) NOR (ii) IS COMMERCIALLY FEASIBLE, TO CREDIT OR REFUND (AT CELLEBRITE'S OPTION) SUCH ITEM AS SET FORTH ABOVE. THIS DISCLAIMER AND EXCLUSION SHALL APPLY EVEN IF THE EXPRESS WARRANTY FAILS OF ITS ESSENTIAL PURPOSE.#

#

Cellebrite expressly disclaims and renounces any warranty or representation that the Products and/or the Software can work with all types of devices, any particular device, or with any particular version of any operating system. Licensee assumes the entire risk and all liabilities that the Product and/or the Software will not work with respect to any such device. THE LICENSEE'S BENEFITS FROM THE SERVICES ARE PROVIDED BY CELLEBRITE ON AN "AS-IS" AND "WHERE IS" BASIS AND WITH ALL FAULTS.#

#

E. Repaired or Replaced Products:#

#

Before returning a Product for service, Licensee will back up any data contained in such Product. IN NO EVENT WILL CELLEBRITE, ITS AFFILIATES OR SUPPLIERS BE LIABLE TO LICENSEE OR ANY THIRD PARTY FOR ANY DAMAGES OF ANY KIND WHATSOEVER RELATING TO OR ARISING OUT OF DAMAGE TO, LOSS OF, OR CORRUPTION OF, ANY RECORDS, PROGRAMS, DATA OR INFORMATION RESULTING FROM CELLEBRITE'S REPAIR OR REPLACEMENT SERVICES UNDER THIS WARRANTY, OR AS A RESULT OF A FAILURE OR MALFUNCTION OF A PRODUCT.#

Copyright and License

OpenStreetMap® is *open data*, licensed under the Open Data Commons Open Database License (ODbL) by the OpenStreetMap Foundation (OSMF).

You are free to copy, distribute, transmit and adapt our data, as long as you credit OpenStreetMap and its contributors. If you alter or build upon our data, you may distribute the result only under the same licence. The full legal code explains your rights and responsibilities.

Our documentation is licensed under the Creative Commons Attribution-ShareAlike 2.0 license (CC BY-SA 2.0).

How to credit OpenStreetMap

Where you use OpenStreetMap data, you are required to do the following two things:

- Provide credit to OpenStreetMap by displaying our copyright notice.
- Make clear that the data is available under the Open Database License.

For the copyright notice, we have different requirements on how this should be displayed, depending on how you are using our data. For example, different rules apply on how to show the copyright notice depending on whether you have created a browsable map, a printed map or a static image. Full details on the requirements can be found in the Attribution Guidelines.

To make clear that the data is available under the Open Database License, you may link to this copyright page. Alternatively, and as a requirement if you are distributing OSM in a data form, you can name and link directly to the license(s). In media where links are not possible (e.g. printed works), we suggest you direct your readers to openstreetmap.org (perhaps by expanding 'OpenStreetMap' to this full address) and to opendatacommons.org. In this example, the credit appears in the corner of the map.

Finding out more

Read more about using our data, and how to credit us, at the OSMF Licence page.

Although OpenStreetMap is open data, we cannot provide a free-of-charge map API for third-parties. See our API Usage Policy, Tile Usage Policy and Nominatim Usage Policy.

Our contributors

Our contributors are thousands of individuals. We also include openly-licensed data from national mapping agencies and other sources, among them:

- **Austria**: Contains data from Stadt Wien (under CC BY), Land Vorarlberg and Land Tirol (under CC BY AT with amendments).
- **Australia**: Incorporates or developed using Administrative Boundaries © Geoscape Australia licensed by the Commonwealth of Australia under Creative Commons Attribution 4.0 International licence (CC BY 4.0).
- **Canada**: Contains data from GeoBase®, GeoGratis (© Department of Natural Resources Canada), CanVec (© Department of Natural Resources Canada), and StatCan (Geography Division, Statistics Canada).
- **Finland**: Contains data from the National Land Survey of Finland's Topographic Database and other datasets, under the NLSFI License.
- **France**: Contains data sourced from Direction Générale des Impôts.
- **Netherlands**: Contains © AND data, 2007 (www.and.com)
- **New Zealand**: Contains data sourced from the LINZ Data Service and licensed for reuse under CC BY 4.0.
- **Slovenia**: Contains data from the Surveying and Mapping Authority and Ministry of Agriculture, Forestry and Food (public information of Slovenia).
- **Spain**: Contains data sourced from the Spanish National Geographic Institute (IGN) and National Cartographic System (SCNE) licensed for reuse under CC BY 4.0.
- **South Africa**: Contains data sourced from Chief Directorate: National Geo-Spatial Information, State copyright reserved.
- **United Kingdom**: Contains Ordnance Survey data © Crown copyright and database right 2010-19.

For further details of these, and other sources that have been used to help improve OpenStreetMap, please see the Contributors page on the OpenStreetMap Wiki.

Inclusion of data in OpenStreetMap does not imply that the original data provider endorses OpenStreetMap, provides any warranty, or accepts any liability.

Copyright infringement

OSM contributors are reminded never to add data from any copyrighted sources (e.g. Google Maps or printed maps) without explicit permission from the copyright holders.

If you believe that copyrighted material has been inappropriately added to the OpenStreetMap database or this site, please refer to our takedown procedure or file directly at our on-line filing page.

Trademarks

OpenStreetMap, the magnifying glass logo and State of the Map are registered trademarks of the OpenStreetMap Foundation. If you have questions about your use of the marks, please see our Trademark Policy.

Microsoft Bing Maps and Embedded Maps Service Terms of Use

Last Updated: November 1, 2021

These terms ("**Terms**") apply to your use of the Bing Maps web services and Bing Maps Embedded Maps. By accessing or otherwise using the Services, are agreeing to these Terms with Microsoft Corporation ("**Microsoft**," "**we**," "**us**," or "**our**"). You represent and warrant to us that you have the authority to accept these Terms on behalf of yourself, a company, or another entity, as applicable ("**you**," "**your**," or "**Company**"). We may change, amend, or cancel these Terms at any time. Your continued use of the Services after the changes become effective means you agree to the new Terms. If you do not agree to the new Terms, you must stop using the Services.

Section 1. Definitions.

- Wherever used in these Terms with the first letter capitalized, these terms have the following meanings:
- (a) "**Affiliate**" means, with respect to an entity, any person or entity that directly or indirectly owns, is owned by, or is under common ownership with that entity. For purposes of this definition, ownership means control of more than a 50% interest in an entity.
- (b) "**Bing Maps Brand Features**" mean the Bing logo, the Bing brand name, and any other images and/or text displayed within the Services from time to time;
- (c) "**Bing Maps Services**" means the Bing Maps web services, which provides mapping and location services;
- (d) "**Bing Maps Brand Features**" mean the Bing logo, the Bing brand name, and any other images and/or text displayed within the Services from time to time;
- (e) "**Content**" means any maps, images, geocodes, data, third-party content, or other content that Microsoft makes available to you via the Services;
- (f) "**Documentation**" means any documentation or other materials provided by Microsoft to you in connection with the provision of the Embedded Maps Service;

- (g) "**Embedded Maps Service**" means the Embedded Maps Service, which provides access to embed a range of mapping and location services. Mapping, address search, routing, and aerial imagery, are included in the Embedded Maps Service;
- (h) "**Guidelines**" means any rules governing the implementation and use of the Embedded Maps Service, as amended from time to time;
- (i) "**Services**" means the Bing Maps Services and Embedded Maps Services, collectively and/or independently.
- (j) "**Website**" means the website, mash-up, or service that you own or operate, which is located at the URL you provide to Microsoft, that makes use of the Embedded Maps Service.

Section 2. Use of the Services.

- (a) We reserve the right to include advertising in the Content served through the Services. You will not intentionally omit or obscure such advertising when displaying such Content to end users.
- (b) You promise not to, and will not permit any third party to, reverse engineer the Services, any of the XML or other calls made by the Services, or any software or services provided by Microsoft. You agree not to, and will not permit or encourage any third party to, copy, cache, or retain any maps, routes, images, or other data provided to you by Microsoft as part of the Services.
- (c) You may not use the Services in any situation that could lead to the death or serious bodily injury of any person or to severe physical or environmental damage.
- (d) As a condition of your permitted use of Services, you will not use Bing Maps Services for any purpose that is unlawful or prohibited by these Terms.
- (e) You may not use the Services in any manner that could damage, disable, overburden, or impair the Services (or the network(s) connected to the Services) or interfere with any other party's use and enjoyment of the Services. You may not attempt to gain unauthorized access to Services, other accounts, computer systems, or networks connected to the Services, through hacking, password mining, or any other means.
- (f) You may not obtain or attempt to obtain any materials or information through any means not intentionally made available through Services by Microsoft.
- (g) You acknowledge that Services, including the Content, is subject to applicable export control laws and regulations of the United States. You agree not to export or re-export Services, including the Content, directly or indirectly, to any countries that are subject to U.S. export restrictions.

- (h) You must comply with all laws and regulations applicable to you and your end user's use of the Services, including laws related to privacy, data protection, and U.S. export laws.

Section 3. Use of the Bing Maps Services.

- (a) Bing Maps Services are for your individual use, solely for internal use by you, for your business, or for your own personal use.
- (b) You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, sublicense, transfer, assign, rent, sell, or otherwise convey any information, software, products, or services obtained from Bing Maps Services without the prior written approval from Microsoft.

Section 4. Use of Embedded Maps Services.

- (a) You may not use the Embedded Maps Service for internal business applications. The site into which you integrate the Embedded Maps Service must be offered for free to users; you may not build paid-for services with the Embedded Maps Service.
- (b) The Embedded Maps Service may not be used as part of a mobile or wireless service; in any real-time tracking, guidance, or asset tracking applications; or routing services.
- (c) Use of the Embedded Maps Service is limited to 50,000 map deliveries per year. If your traffic requirement will exceed this limit, please contact maplic@microsoft.com.
- (d) You agree that Microsoft has the right to monitor your usage of the Embedded Maps Service, including traffic generated by you. This may include, for example, filtering to stop spam or increase security. These means may hinder or break your use of the Embedded Maps Service.
- (e) You may access and use the Embedded Maps Service only as documented in the implementation guidelines or other relevant Documentation.
- (f) You may not alter, block, or remove any copyright notice, logos, digital watermarks, terms of use links, or advertisements contained in or on the maps, images, or other components of the Embedded Maps Service.
- (g) You agree that you will not use Bird's Eye Imagery or Traffic data.
- (h) You may not use or integrate any element of the Embedded Maps Service with another supplier's mapping or location-related services.
    - (i) The Embedded Maps Service may not be used in conjunction with any materials, Websites, applications, or services that:

  - (i) are obscene, indecent, pornographic, or harmful to or exploitative of minors; or are otherwise illegal; or that breach another individual's right to privacy;
  - (ii) incite, advocate, or express hatred, bigotry, racism, or gratuitous violence;
  - (iii) are intended to threaten, stalk, defame, defraud, degrade, victimize, or intimidate an individual or group of individuals for any reason, including, without limitation, on the basis of age, gender, disability, ethnicity, sexual orientation, race, or religion, or to incite or encourage anyone else to do so;
  - (iv) transmit, sell, license, or deliver any infringing, defamatory, offensive, or illegal products, services, or materials;
  - (v) email, transmit, or upload viruses, worms, Trojan horses, spam, unsolicited messages, or advertisements;
  - (vi) upload files that contain software or other materials in breach of any intellectual property rights;
  - (vii) impersonate anyone else or otherwise misrepresent your identity or status;
  - viii) collect and process another's personal data;
  - (ix) violate local, state, federal, or other applicable consumer privacy regulations; or
  - (x) violate any applicable law or violate the rights of any third party (including, without limitation, rights of privacy or proprietary rights).
- (j) You may not use the Embedded Maps Service in ways that harm us, our Affiliates, or our suppliers.
- (k) You may not use any unauthorized means to modify or reroute, or attempt to modify or reroute, the Embedded Maps Service.
- (l) You may not sell, lease, or sublicense access to the Embedded Maps Service.
- (m) You may not attempt to make a local non-cache copy, or help a third party attempt to make a local non-cache copy, of any content provided through the Embedded Maps Service.
- (n) You agree that you will not capture or retain any geocodes produced by the Embedded Maps Service in any way, including an address look-up.
- (o) You may not use any automated process or service to access and/or use the Embedded Maps Service (such as a BOT, a spider, periodic caching of information provided through the Embedded Maps Service, or "meta-searching").
- (p) You may not falsify or alter any unique referral identifier in, or assigned to, an application or Website or otherwise obscure or alter the source of queries coming from an application or Website.

Section 5. Links to Third-Party Websites.

- (a) The Services may contain links to third party websites ("**Linked Sites**" or "**Linked Site**"). The Linked Sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any Linked Site, including without limitation any link contained in a Linked Site or any changes or updates to a Linked Site. Microsoft is not responsible for webcasting or any other form of transmission received from any Linked Site nor is Microsoft responsible if the Linked Site is not working appropriately. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement by Microsoft of the site or any association with its operators. You are responsible for viewing and abiding by the privacy statements and terms of use posted at the Linked Sites.
- (b) Any dealings with third parties (including advertisers) included within the Services or participation in promotions, including the delivery of and the payment for goods and services, and any other terms, conditions, warranties, or representations associated with such dealings or promotions, are solely between you and the advertiser or other third party. Microsoft is not responsible or liable for any part of any such dealings or promotions.

Section 6. Liability Disclaimer.

- (a) THE INFORMATION, CONTENT, AND SERVICES INCLUDED IN OR AVAILABLE THROUGH THE SERVICES MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY MADE TO THE SERVICES AND TO THE INFORMATION THEREIN. MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS MAY MAKE IMPROVEMENTS AND/OR CHANGES IN BING MAPS SERVICES AT ANY TIME, WITHOUT NOTICE. THE USER ASSUMES ALL RISK OF USE.
- (b) MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY, RELIABILITY, AVAILABILITY, TIMELINESS, LACK OF VIRUSES, OR OTHER HARMFUL COMPONENTS AND ACCURACY OF THE INFORMATION, CONTENT, SERVICES, AND RELATED GRAPHICS CONTAINED WITHIN THE SERVICES FOR ANY PURPOSE. ALL SUCH INFORMATION, CONTENT, SERVICES, AND RELATED GRAPHICS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, CONTENT, SERVICES, AND RELATED GRAPHICS, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORT, TITLE, AND NON-INFRINGEMENT.

- (c) YOU SPECIFICALLY AGREE THAT MICROSOFT SHALL NOT BE RESPONSIBLE FOR UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA, ANY MATERIAL OR DATA SENT OR RECEIVED OR NOT SENT OR RECEIVED, OR ANY TRANSACTIONS ENTERED INTO THROUGH THE SERVICES. YOU SPECIFICALLY AGREE THAT MICROSOFT IS NOT RESPONSIBLE OR LIABLE FOR ANY THREATENING, DEFAMATORY, OBSCENE, OFFENSIVE, OR ILLEGAL CONTENT OR CONDUCT OF ANY OTHER PARTY OR ANY INFRINGEMENT OF ANOTHER'S RIGHTS, INCLUDING INTELLECTUAL PROPERTY RIGHTS. YOU SPECIFICALLY AGREE THAT MICROSOFT IS NOT RESPONSIBLE FOR ANY CONTENT INCLUDED IN THE SERVICES BY ANY THIRD PARTY.
- (d) TO THE EXTENT PERMITTED BY LAW, IN NO EVENT SHALL MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF USE, DATA, OR PROFITS ARISING OUT OF OR IN ANY WAY CONNECTED WITH (I) THE USE OR PERFORMANCE OF THE SERVICES; (II) THE DELAY OR INABILITY TO USE THE SERVICES OR RELATED SERVICES; (III) THE PROVISION OF OR FAILURE TO PROVIDE SERVICES; OR (IV) FOR ANY INFORMATION, CONTENT, SERVICES, AND RELATED GRAPHICS OBTAINED THROUGH THE SERVICES OR OTHERWISE ARISING OUT OF THE USE OF THE SERVICES, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF MICROSOFT AND/OR ANY OF ITS RESPECTIVE SUPPLIERS HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Section 7. Copyright and Trademark Notices.

The Services are copyright © Microsoft Corporation and/or its respective suppliers, One Microsoft Way, Redmond, WA 98052, U.S.A. All rights reserved. The Terms incorporate Microsoft Trademark & Brand Guidelines (as amended from time to time). Microsoft and the names, logos, and icons of all Microsoft products, software, and services may be either unregistered or registered trademarks of the Microsoft group of companies in the United States and/or other jurisdictions. The following is a non-exhaustive list of Microsoft's trademarks. The names of actual companies and products may be the trademarks of their respective owners. Any rights not expressly granted in these Terms are reserved.

Section 8. Ownership.

- (a) You acknowledge and agree that Microsoft owns, or is the licensee of, all rights and interests in the Services, all underlying data and Intellectual Property, and the Bing Maps Brand Features.
- (b) Nothing in these Terms shall confer on you any right of ownership in the Embedded Maps Service or any underlying JavaScript, map data, other location data, or any other Intellectual Property. You will not, now or in the future, contest the validity of the Bing Maps Brand Features.
- (c) Without prejudice to any other rights or remedies that Microsoft may have, you acknowledge and agree that if any of the Services, the Documentation, or Microsoft's confidential information are used or disclosed (if applicable), unless in accordance with these Terms, the award of damages may not be an adequate remedy and Microsoft shall be entitled to seek injunctive or other equitable relief in respect of such breach.

Section 9. Your Responsibilities.

- (a) You warrant that you shall use the Embedded Maps Service in accordance with these Terms and will implement the Embedded Maps Service as instructed in the Guidelines and other Documentation.
- ~~(b) You will defend and indemnify Microsoft and its subsidiaries and respective suppliers against any expense, claim, or cost suffered by Microsoft, including legal fees, losses (actual and consequential), judgments, or damages, as a result of any breach by you of the warranties contained in Clause 6 or of any of the Terms.~~

Section 10. Privacy.

Your privacy is important to us. All access to and use of the Services is subject to the data practices set forth in the Microsoft Online Privacy Statement, which is incorporated as part of these Terms. You are responsible for providing end users with adequate notice of the privacy practices applicable to the Embedded Maps Service on your Website.

Section 11. Term and Termination.

- (a) These Terms shall commence on the date upon which you first use the Services and shall continue until terminated by either party.
- (b) Microsoft reserves the right to terminate or discontinue these Terms and your use of the Services at any time, without notice.

- (c) Microsoft may suspend the operation of the Services for repair or maintenance work or in order to update or upgrade the contents or functionality of the Services from time to time. Access to or use of the Services, or any pages linked to it, will not necessarily be uninterrupted or error free.
- (d) Microsoft shall be entitled to terminate these Terms effective immediately in the event that any act or omission by you, at Microsoft's sole discretion, results in damage to Microsoft, any of its Affiliates, or respective suppliers or brings Microsoft, any of its Affiliates, or respective suppliers into disrepute, whether in relation to the Services or otherwise.
- (e) You may terminate these Terms at any time by ceasing to use the Services.
- (f) In the event of the termination of these Terms, you agree to:
    - (i) cease using the Services immediately; and
    - (ii) destroy or return to Microsoft (as Microsoft shall direct) the Documentation and remove Bing Maps links, JavaScript, and other content from your Website, within 5 days of termination.
- (g) Either party's termination of these Terms shall not affect either party's accrued rights or liabilities nor shall it affect the coming into force, or the continuance in force, of any provision of the Terms which is intended (expressly or implicitly) to come into, or continue in, force on or after such termination.
- (h) Clauses 1, 6, 7, 8, 9, 10, 11, 13, 14 shall survive termination of these Terms.

Section 12. Notices.

- (a) These Terms are in electronic form. We may send you additional information, including legal notices and notices required by law, in electronic form. We may provide required information to you:
    - (i) by e-mail at the e-mail address you specified when you signed up for the Embedded Maps Service; or
    - (ii) by updating these Terms and posting them at http://www.microsoft.com/maps/assets/docs/terms.aspx or another website as Microsoft may designate from time to time.
- (b) Notices provided to you via e-mail will be deemed given and received on the transmission date of the email. As long as you can access and use the Services, you have the necessary software and hardware to receive these notices. If you do not consent to receive any notices electronically, you must stop using the Embedded Maps Service.
- (c) Any notice from you should be sent electronically to: maplic@microsoft.com.

Section 13. General.

- (a) You may not assign or delegate any rights or obligations under these Terms, including in connection with a change of control, without Microsoft's prior written consent. Any purported assignment and delegation will be ineffective. We may freely assign or delegate all rights and obligations under these Terms, fully or partially, without notice to you.
- (b) Neither Microsoft nor you will be in default if performance is delayed or prevented for reasons beyond our/your control, so long as we/you resumes performance as soon as practical.
- (c) Any delay or failure of either party to exercise a right or remedy will not result in a waiver of that, or any other, right or remedy. No waiver will be effective unless made in writing and signed by an authorized representative of the waiving party.
- (d) The invalidity, illegality, or unenforceability of any provision of these Terms shall not affect or impact the validity or enforceability of the remainder of these Terms.
    - The parties are operating as independent contractors, and nothing in these Terms will be construed as creating a partnership, franchise, joint venture, employer-employee, or agency relationship.
- (e) These Terms are solely for your and our benefit. These Terms are not for the benefit of any other person, except for permitted successors and assigns.
- (f) These Terms, and the documents referred to in it, constitutes the entire agreement between you and us regarding your use of the Services.

Section 14. Law and Jurisdiction.

If you are domiciled anywhere other than Europe: (i) ~~Washington~~ Tennessee State law governs the interpretation of these Terms and applies to claims for breach, regardless of conflict of laws principles; and (ii) you and we irrevocably consent to the exclusive jurisdiction and venue of the state or federal courts in ~~King County, Washington~~Davidson County, Tennessee, USA, for all disputes arising out of or relating to these Terms. If you are domiciled in Europe: (i) the laws of England and Wales govern the interpretation of these Terms and apply to claims for breach, regardless of conflict of laws principles; and (ii) you and we irrevocably consent to the exclusive jurisdiction and venue of the courts located in London, England, for all disputes arising out of or relating to these Terms. ~~The parties waive all defenses of lack of personal jurisdiction and forum non conveniens.~~ Process may be served on either party in the manner authorized by applicable law or court rule. ~~In any~~

~~dispute relating to the Services or these Terms, the prevailing party will be entitled to recover reasonable attorneys' fees and costs.~~

DOCUSIGN MASTER SERVICES AGREEMENT FOR PUBLIC SECTOR RESALE CUSTOMERS

This DocuSign Master Services Agreement for Public Sector Resale Customers ("**MSA**") is made between DocuSign, Inc., a Delaware corporation ("**DocuSign**"), and the customer identified on the Order Form or SOW ("**Customer**"), together referred to as the "**Parties**" and each individually as a "**Party**", as of the date of last signature below (the "**MSA Effective Date**"). The Parties hereby agree to the terms and conditions of this MSA, including any specific services terms, product details and any applicable license and/or subscription terms will be set forth in applicable DocuSign Service Schedule(s) and Attachments (located at https://www.docusign.com/company/terms-and-conditions/msa-service-schedules), Order Form(s) and SOW, each of which become binding on the Parties and are incorporated into this MSA upon the provisioning of any DocuSign Services (defined below) to Customer. All DocuSign Services provisioned to Customer are governed by and incorporate the following documents in effect as of the date of the last update of such documents, collectively referred to as the "**Agreement**":

1. The Master Agreement;
2. the Order Form and/or Statement of Work;
3. any attachments, addenda, and/or appendix(ices) to this MSA or a Service Schedule;
4. Service Schedule(s); and
5. this MSA.

The applicable attachment(s), addenda, appendix(ices), and Service Schedule(s) are determined by the DocuSign Service(s) provisioned to Customer. In the event of a conflict, the order of precedence is as set out above in descending order of control. This offer by DocuSign is expressly conditioned on assent to the terms and conditions of this Agreement, and any different or additional terms or conditions specified by Customer at any time in purchase orders or other documentation are hereby rejected.

Public Sector Resale MSA Version: May 2022

TABLE OF CONTENTS

1. DEFINITIONS

"**Account**" means a unique account established by Customer to enable its Authorized Users to access and use a DocuSign Service.

"**Account Administrator**" is an Authorized User who is assigned and expressly authorized by Customer as its agent to manage Customer's Account, including, without limitation, to configure administration settings, assign access and use authorizations, request different or additional services, provide usage and performance reports, manage templates, execute approved campaigns and events, assist in third-party product integrations, and to receive privacy disclosures. Customer may appoint an employee or a third-party business partner or contractor to act as its Account Administrator and may change its designation at any time through its Account.

"**Affiliate**" means any DocuSign entity that DocuSign directly or indirectly owns or controls more than fifty percent (50%) of the voting interests of the subject entity. Any legal entity will be considered a DocuSign Affiliate as long as that interest is maintained.

"**Authorized User**" means one individual natural person, whether an employee, business partner, contractor, or agent of Customer who is registered by Customer in Customer's Account to use the DocuSign Services. An Authorized User must be identified by a unique email address and user name, and two or more persons may not use the DocuSign Services as the same Authorized User. If the Authorized User is not an employee of Customer, use of the DocuSign Services will be allowed only if the user is under confidentiality obligations with Customer at least as restrictive as those in this Agreement and is accessing or using the DocuSign Services solely to support Customer's internal business purposes.

"**Confidential Information**" means: (a) for DocuSign and its Affiliates, the DocuSign Services, Documentation and other related technical information, security policies and processes, product roadmaps and pricing (to the extent allowable under applicable law); (b) for Customer, Customer Data; (c) any other information of a Party (or for DocuSign, its Affiliates) that is disclosed in writing or orally and is designated as confidential or proprietary at the time of disclosure to the Party receiving Confidential Information ("**Recipient**") (and, in the case of oral disclosures, summarized in writing and delivered to the Recipient within thirty (30) days of the initial disclosure), or that due to the nature of the information the Recipient should reasonably understand it to be confidential information of the disclosing Party.. Confidential Information does not include any information that: (i) was or becomes generally known to the public through no fault or breach of this Agreement by the Recipient; (ii) was rightfully in the Recipient's possession at the time of disclosure without restriction on use or disclosure; (iii) was independently developed by the Recipient without use of or reference to the disclosing Party's Confidential Information; (iv) was rightfully obtained by the Recipient from a third party not under a duty of confidentiality and without restriction on use or disclosure; or (v) is disclosed pursuant to law.

"Customer" means the entity that has contracted with the Reseller for the purchase of applicable DocuSign Services. Any Customer that is not a Public Sector Resale Customer will be subject to terms included in DocuSign's Master Services Agreement for Resell Customers, which is available at: https://www.docusign.com/company/terms-and-conditions/reseller.

"**Customer Data**" means any content, eDocuments, materials, data and information that Customer or its Authorized Users enter into the DocuSign Services, including, but not limited to, any Customer personal data and information contained in eDocuments. Customer Data does not include any component of the DocuSign Services or material provided by or on behalf of DocuSign.

"DFARS" means the Defense Federal Acquisition Regulation Supplement as set forth in Chapter 2 of Title 48 of the Code of Federal Regulations, 48 CFR 2.

"**Documentation**" means DocuSign's then-current technical and functional documentation for the DocuSign Services as made generally available by DocuSign.

"**DocuSign Service(s)**" means the services provided by DocuSign under an Order Form or SOW, and may include Professional Services, software, source code, or other technology licensed to DocuSign from third parties and embedded into the services that DocuSign provides to Customer. Notwithstanding the foregoing, DocuSign Services do not include Third-Party Services (defined below).

"DoD" means the United States Department of Defense.

"**eDocument**" refers to a contract, notice, disclosure, or other record or document deposited into the DocuSign Service by Customer for processing.

"FAR" means the Federal Acquisition Regulation as set forth in Chapter 1 of Title 48 of the Code of Federal Regulations, 48 CFR 1.

"**Order Form**" means the paper or online order form between DocuSign and Reseller that sets forth the DocuSign Services selected by Customer.

"Order End Date" means the end date for provision of a respective DocuSign Service specified in a corresponding Order Form or SOW.

"Order Start Date" means the start date for provision of a respective DocuSign Service specified in a corresponding Order Form or SOW.

"**Professional Services**" means any integration, consulting, architecture, training, transition, configuration, administration, and similar ancillary DocuSign Services that are set forth in an Order Form or Statement of Work ("**SOW**") between DocuSign and Reseller.

"Public Sector Resale Customers" are Customers authorized to use DocuSign Services pursuant to an Order Form and/or SOW and the Agreement and are: a United States Federal agency or department (as well as any eligible ordering activity purchasing through a Federal Supply Schedule Contract, as defined in GSA Order OGP 4800.2I (or its successor), state or local government or agency thereof, or (ii) a United States public school (including both K-12 and university institutions), but only to the extent the DocuSign Services are being used in an Authorized User's official capacity as a Federal, state, local government, or school official or employee ("**Official Use**"). Customers who are not bona fide Public Sector Resale Customers are not eligible to use DocuSign Services according to the terms of this MSA, but, instead, will be subject to terms included in DocuSign's Master Services Agreement for Resell Customers.

"Purchase Agreement" means any agreement between Customer and Reseller relating to Customer's purchase of DocuSign Services from that Reseller.

"Reseller" means an entity that has contracted with DocuSign or one of DocuSign's authorized distributors to resell DocuSign Services and with which Customer has contracted directly to purchase applicable DocuSign Services.

"**Service Schedule**" means the service-specific terms and conditions applicable to a particular DocuSign Service(s) provisioned to Customer.

"**System**" means the software systems and programs, the communication and network facilities, and the hardware and equipment used by DocuSign or its agents to make available the DocuSign Services via the Internet.

"Third-Party Services" means services, software, products, applications, integrations and other features or offerings that are provided by Customer or obtained by Customer from a third party.

2. USAGE AND ACCESS RIGHTS

2.1 Right to Use. DocuSign will provide the DocuSign Services to Customer as set forth in the Order Form and/or SOW. Subject to the terms and conditions of the Agreement, DocuSign grants to Customer a worldwide, limited, non-exclusive, non-transferable right and license during the Term, solely for its Official Use by Authorized Users for Customer's internal business purposes, and in accordance with the Documentation, to: (a) access and use the DocuSign Services; (b) implement, configure, and through its Account Administrator, permit its Authorized Users to access and use the DocuSign Services; and (c) access and use the Documentation. Customer will ensure that its Authorized Users using the DocuSign Services under its Account comply with all of Customer's obligations under the Agreement, and Customer is responsible for their acts and omissions relating to the Agreement as though they were those of Customer.

2.2 Restrictions. Customer shall not, and shall not permit its Authorized Users or others under its control to, do the following with respect to the DocuSign Services:

(a) use the DocuSign Services, or allow access to it, in a manner that circumvents contractual usage restrictions or that exceeds Customer's authorized use or usage metrics set forth in this Agreement, including the applicable Order Form or SOW;

(b) license, sub-license, sell, re-sell, rent, lease, transfer, distribute, time share or otherwise make any portion of the DocuSign Services or Documentation available for access by third parties except as otherwise expressly provided in this Agreement;

(c) access or use the DocuSign Services or Documentation for the purpose of: (i) developing or operating products or services intended to be offered to third parties in competition with the DocuSign Services, or (ii) allowing access to its Account or the DocuSign Services by a direct competitor of DocuSign;

(d) reverse engineer, decompile, disassemble, copy or otherwise attempt to derive source code or other trade secrets from or about any of the DocuSign Services or technologies, without DocuSign's written consent;

(e) use the DocuSign Services or Documentation in a way that: (i) violates or infringes upon the rights of a third party, including those pertaining to: contract, intellectual property, privacy, or publicity; or (ii) effects or facilitates the storage or transmission of libelous, tortious, or otherwise unlawful material including, but not limited to, material that is harassing, threatening, or obscene;

(f) fail to use commercially reasonable efforts to avoid interference with or disruption to the integrity, operation, performance, or use or enjoyment by others of the DocuSign Services;

(g) use the DocuSign Services to create, use, send, store, or run viruses or other harmful computer code, files, scripts, agents, or other programs, or circumvent or disclose the user authentication or security of the DocuSign Services or any host, network, or account related thereto or use any aspect of the DocuSign Services components other than those specifically identified in an Order Form or SOW, even if technically possible; or

(h) use, or allow the use of, the DocuSign Services by anyone located in, under the control of, or a resident of a U.S. embargoed country or territory or by a prohibited end user under Export Laws (as defined in Section 13.5).

2.3 Suspension of Access. DocuSign may suspend any use of the DocuSign Services or remove or disable any Account or content that DocuSign reasonably and in good faith believes violates the Agreement, unless DocuSign is prohibited from doing so by applicable law or regulation (e.g. FAR 52.233-1 as prescribed by FAR 33.215 or other agency supplemental terms as applicable to Customer). DocuSign will use commercially reasonable efforts to notify Customer prior to any such suspension or disablement, unless DocuSign reasonably believes that: (a) it is prohibited from doing so under applicable law, regulation or under legal process (such as court or government administrative agency processes, orders, mandates, and the like); or (b) it is necessary to delay notice in order to prevent imminent harm to the DocuSign Services or a third party. Under circumstances where notice is delayed, DocuSign will provide notice if and when the related restrictions in the previous sentence no longer apply.

2.4 Third-Party Services. Customer may choose to obtain Third-Party Services from third parties and/or DocuSign (for example, through a reseller arrangement or otherwise). Any acquisition by Customer of Third-Party Services is solely between Customer and the applicable Third-Party Service provider and DocuSign does not warrant, support, or assume any liability or other obligation with respect to such Third-Party Services, unless expressly provided otherwise in the Order Form or this Agreement. DocuSign assumes no responsibility for, and specifically disclaims any liability or obligation with respect to, any Third-Party Services. In the event Customer chooses to integrate or interoperate Third-Party Services with DocuSign Services in a manner that requires DocuSign or the DocuSign Services to exchange Customer Data with such Third-Party Service or Third-Party Service provider, Customer: (a) grants DocuSign permission to allow the Third-Party Service and Third-Party Service provider to access Customer Data and information about Customer's usage of the Third-Party Services as appropriate and necessary to enable the interoperation of that Third-Party Service with the DocuSign Services; (b) acknowledges that any exchange of data between Customer and any Third-Party Service is solely between Customer and the Third-Party Service provider and is subject to the Third-Party Service provider's terms and conditions governing the use and provision of such Third-Party Service (the presentation and manner of acceptance of which is controlled solely by the Third-Party Service provider); and (c) agrees that DocuSign is not responsible for any disclosure, modification or deletion of Customer Data resulting from access to such data by Third-Party Services and Third-Party Service providers.

3. OWNERSHIP

3.1 Customer Data. Customer Data processed using the DocuSign Services is and will remain, as between Customer and DocuSign, owned by Customer. Customer hereby grants DocuSign the right to process, transmit, store and/or disclose the Customer Data in order to provide the DocuSign Services to Customer, subject to the terms of Section 11.2 (Required Disclosure) below, to comply with any request of a governmental or regulatory body (including subpoenas or court orders) or as otherwise required by applicable law or regulation.

3.2 DocuSign Services. DocuSign, its Affiliates, or its licensors own all right, title, and interest in and to any and all copyrights, trademark rights, patent rights, database rights, and other intellectual property or other rights in and to the DocuSign Services and Documentation, any improvements, design contributions, or derivative works thereto, and any knowledge or processes related thereto (including any machine learning algorithms output from the DocuSign Services) and/or provided hereunder. Unless otherwise specified in the applicable SOW, all deliverables provided by or for DocuSign in the performance of Professional Services, excluding Customer Data and Customer Confidential Information, are owned by DocuSign and constitute part of the DocuSign Service(s) under this Agreement.

3.3 Feedback. DocuSign encourages Customer to provide suggestions, proposals, ideas, recommendations, or other feedback regarding improvements to DocuSign Services and related resources ("**Feedback**"). To the extent Customer provides Feedback, Customer grants to DocuSign and its Affiliates a royalty-free, fully paid, sub-licensable, transferable (notwithstanding Section 13.2 (Assignability)), non-exclusive, irrevocable, perpetual, worldwide right and license to make, use, sell, offer for sale, import, and otherwise exploit Feedback (including by incorporation of such feedback into the DocuSign Services) without restriction provided that: such Feedback does not identify Customer, or Authorized Users, or include any Customer Data without Customer's prior written consent.

4. SECURITY AND CUSTOMER DATA

4.1 Security. DocuSign will use commercially reasonable industry standard security technologies in providing the DocuSign Services. DocuSign has implemented and will maintain appropriate technical and organizational measures, including information security policies and safeguards, designed to preserve the security, integrity, and confidentiality of Customer Data and Customer personal data and to protect against unauthorized or unlawful disclosure or corruption of or access to such data in accordance with the Security Attachment for DocuSign Services found herein at: Additional or differing security obligations, if any, will be expressly set forth in the applicable Service Schedule, Order Form, or separate written agreement between the Parties.

4.2 Customer Data. Customer is responsible for Customer Data (including Customer personal data) as entered into, supplied or used by Customer and its Authorized Users in the DocuSign Services. Further, Customer is solely responsible for determining the suitability of the DocuSign Services for Customer's business and complying with any applicable data privacy and protection regulations, laws or conventions applicable to Customer Data and Customer's use of the DocuSign Services. Customer grants to DocuSign the non-exclusive right to process Customer Data (including personal data) in accordance with the Data Protection Attachment for DocuSign Services found herein I, for the sole purpose of and only to the extent necessary for DocuSign: (a) to provide the DocuSign Services; (b) to verify Customer's compliance with the restrictions set forth in Section 2.2 (Restrictions) if DocuSign has a reasonable belief of Customer's non-compliance; and (c) as otherwise set forth in the Agreement.

4.3 Usage Data. Customer agrees that DocuSign may collect and use quantitative data, derived from the use of the DocuSign Services for business purposes, including industry analysis, benchmarking, analytics, marketing, and other business purposes. All data collected, used and disclosed will be in aggregate form only and will not identify Customer, its Authorized Users, Customer Data, or any third parties utilizing the DocuSign Services.

5. PURCHASE AGREEMENT.

Customer will comply with the terms of the Purchase Agreement. Customer acknowledges that compliance with the terms of the Purchase Agreement is a material condition under this Agreement, and if Reseller notifies DocuSign that Customer is in breach of such Purchase Agreement, DocuSign may consider the Customer to be in breach of this Agreement.

6. RESERVED

7. TERM AND TERMINATION

7.1 Term. The term of an Order Form or SOW and any associated Service Schedule(s) is the period of time, including all renewals thereto, that begins on the Order Start Date and, unless terminated sooner as provided herein, will continue until the Order End Date, both dates as specified on the Order Form or SOW (the "**Term**"). In the case of a SOW for Professional Services, if no end date is specified in the SOW, then the SOW shall expire upon completion of Professional Services or early termination as permitted by the Agreement. The term of this MSA and this Agreement shall continue as long as an Order Form or SOW referencing or incorporated into this MSA remains valid and in effect or DocuSign Services are provisioned to Customer. Termination or expiration of any Order Form or SOW shall leave other Order Forms or SOWs unaffected. In no event can the term exceed the term of the Master Agreement.

7.2 Termination for Breach. If either Party commits a material breach or default in the performance of any of its obligations under the Agreement, then except as prohibited by applicable law or regulation, the other Party may terminate the Agreement in its entirety by giving the defaulting Party written notice of termination, unless the material breach or default in performance is cured within thirty (30) days after the defaulting Party receives notice thereof.

7.3 Post-Termination Obligations. If this Agreement expires or is terminated for any reason: (a) except as prohibited by applicable law or regulation, Customer will pay any amounts owed by Customer that have accrued before, and remain unpaid as of, the effective date of the expiration or termination; (b) any and all liabilities that have accrued before the effective date of the expiration or termination will survive; (c) licenses and use rights granted to Customer with respect to DocuSign Services and intellectual property will immediately terminate; (d) DocuSign's obligation to provide any further DocuSign Services to Customer under the Agreement will immediately terminate, except any such DocuSign Services that are expressly to be provided following the expiration or termination of this Agreement; and (e) the Parties' rights and obligations under Sections 4.3, 7.1, 7.3, 8.3 and 9 through 13 will survive. Except as otherwise expressly set forth herein and unless prohibited by applicable law or regulation, no termination for any reason shall entitle Customer or Reseller to a refund of any portion of the fees paid and any fees or charges incurred through the effective date of termination which shall become immediately due and payable.

8. WARRANTIES AND DISCLAIMERS

8.1 DocuSign Service Warranties. DocuSign warrants that during the applicable Term, the DocuSign Services, when used as authorized under this Agreement, will perform substantially in conformance with the Documentation associated with the applicable DocuSign Services. Customer's sole and exclusive remedy for any breach of this warranty by DocuSign is for DocuSign to repair or replace the affected DocuSign Services to make them conform, or, if DocuSign determines that the foregoing remedy is not commercially reasonable, then either Party may terminate this Agreement.

8.2 Mutual Warranties. Each Party represents and warrants that: (a) this Agreement has been duly executed and delivered and constitutes a valid and binding agreement enforceable against it in accordance with the terms of this Agreement.

8.3 DISCLAIMER. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN THE AGREEMENT, DOCUSIGN: (A) MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED IN FACT OR BY OPERATION OF LAW, OR STATUTORY, AS TO ANY MATTER WHATSOEVER; (B) DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND TITLE; AND (C) DOES NOT WARRANT THAT THE DOCUSIGN SERVICES ARE OR WILL BE ERROR-FREE OR MEET CUSTOMER'S REQUIREMENTS. CUSTOMER HAS NO RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTY ON BEHALF OF DOCUSIGN TO ANY THIRD PARTY.

9. THIRD PARTY CLAIM PROCEDURES, CONDITIONS AND REMEDIES

9.1 Procedures/Conditions. In the event applicable law or regulation requires DocuSign to indemnify Customer, then except as prohibited by applicable law or regulation, such indemnification is expressly conditioned on: (a) the Customer giving providing prompt written notice of the claim for which indemnification is sought hereunder (the "**Claim**"), and (b) DocuSign being given a full and complete opportunity to meaningfully participate in the defense and settlement of the Claim. NeitherDocusign nor Customer or Customer's authorized settlement authority (as applicable) will, without the other parties' prior written consent, agree to any settlement which includes either the obligation to pay any amounts, or any admissions of liability, whether civil or criminal. Notwithstanding anything herein to the contrary, and, except as prohibited by applicable law or regulation, DocuSign will not be responsible for any Claim due to Customer's or its Authorized User's combination of DocuSign Services with goods or services provided by third parties, including any Third-Party Services; adherence to specifications, designs, or instructions furnished by Customer; or Customer's modification of the DocuSign Services not described in the Documentation or otherwise expressly authorized by DocuSign in writing.

9.2 Infringement Remedy. If Customer is enjoined or otherwise prohibited from using any of the DocuSign Services or a portion thereof based on a Claim covered by DocuSign's indemnification obligations under applicable law or regulation, then DocuSign will, at its sole expense and option, except as prohibited by applicable law or regulation, either: (a) obtain for Customer the right to use the affected portions of the DocuSign Services; (b) modify the allegedly infringing portions of the DocuSign Services so as to avoid the Claim without substantially diminishing or impairing their functionality; or (c) replace the allegedly infringing portions of the DocuSign Services with items of substantially similar functionality so as to avoid the Claim. If DocuSign determines that the foregoing remedies are not commercially reasonable and notifies Customer of such determination, then either Party may terminate the Agreement, and in such case, DocuSign will provide a prorated refund to Customer for any prepaid fees for the infringing

DocuSign Services received by DocuSign under the Agreement that correspond to the unused portion of the Term. To the extent permitted by state law, the remedies set out in this Section 9.2 (Infringement Remedy) are Customer's sole and exclusive remedies for any actual or alleged infringement by the DocuSign Services of any third-party intellectual property right.

10. LIMITATION OF LIABILITY

10.1 Exclusion of Damages. TO THE EXTENT PERMITTED BY STATE LAW, EXCEPT FOR THE PARTIES' EXPRESS OBLIGATIONS UNDER SECTION 3.2 (DOCUSIGN SERVICES), UNDER NO CIRCUMSTANCES, AND REGARDLESS OF THE NATURE OF THE CLAIM, SHALL EITHER PARTY (OR THEIR RESPECTIVE AFFILIATES) BE LIABLE TO THE OTHER PARTY FOR LOSS OF PROFITS, SALES OR BUSINESS, LOSS OF ANTICIPATED SAVINGS, LOSS OF USE OR CORRUPTION OF SOFTWARE, DATA OR INFORMATION, WORK STOPPAGE OR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, COVER, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE AGREEMENT, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH LOSSES.

10.2 Limitation of Liability. TO THE EXTENT PERMITTED BY STATE LAW, EXCEPT FOR: (A) DAMAGES RESULTING FROM DEATH OR BODILY INJURY, OR PHYSICAL DAMAGE TO TANGIBLE REAL OR PERSONAL PROPERTY, CAUSED BY EITHER PARTY'S NEGLIGENCE; (B) DAMAGES RESULTING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; AND (C) DOCUSIGN'S RIGHT TO COLLECT UNPAID FEES DUE HEREUNDER, TO THE EXTENT PERMITTED BY LAW, THE TOTAL, CUMULATIVE LIABILITY OF EACH PARTY (AND THEIR RESPECTIVE AFFILIATES) ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE SERVICE(S) PROVIDED HEREUNDER WILL BE LIMITED TO THE AMOUNTS PAID BY CUSTOMER TO RESELLER FOR THE DOCUSIGN SERVICE(S) DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY. THE FOREGOING LIMITATION WILL APPLY WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR ANY OTHER LEGAL OR EQUITABLE THEORY. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE THIS CUMULATIVE LIMIT. THE PARTIES FURTHER ACKNOWLEDGE THAT CUSTOMER MAY HAVE STATUTORY RIGHTS AGAINST DOCUSIGN FRANCE SAS AND CUSTOMER ACKNOWLEDGES AND AGREES THAT ANY AMOUNTS RECOVERED BY CUSTOMER AGAINST DOCUSIGN FRANCE SAS PURSUANT TO SUCH RIGHTS SHALL BE AGGREGATED WITH ANY OTHER CLAIMS HEREUNDER FOR PURPOSES OF THE CAP ON DAMAGES SET FORTH ABOVE.

10.3 Independent Allocations of Risk. Each provision of this Agreement that provides for a limitation of liability, disclaimer of warranties, or exclusion of damages represents an agreed allocation of the risks of this Agreement between the Parties. This allocation is reflected in the pricing offered by DocuSign and is an essential element of the basis of the bargain between the Parties. Each of these provisions is severable and independent of all other provisions of the Agreement, and each of these provisions will apply even if the warranties in the Agreement have failed of their essential purpose.

11. CONFIDENTIALITY

11.1 Restricted Use and Nondisclosure. During and after the Term, Recipient will to the extent permissible according to applicable law or regulation: (a) use the Confidential Information of the disclosing Party solely for the purpose for which it is provided or for legal, regulatory or compliance purposes as required by applicable law or regulation; (b) not disclose such Confidential Information to a third party, except on a need-to-know basis to its Affiliates (where Recipient is DocuSign), attorneys, auditors, consultants, and service providers who are under confidentiality obligations at least as restrictive as those contained herein unless required by law; and (c) protect such Confidential Information from unauthorized use and disclosure to the same extent (but using no less than a reasonable degree of care) that it protects its own Confidential Information of a similar nature.

11.2 Required Disclosure. If Recipient is required by applicable law or regulation to disclose Confidential Information of the disclosing Party (such as but not limited to the terms of this Agreement), Recipient will give prompt written notice to the disclosing Party before making the disclosure, unless prohibited from doing so by applicable legal, regulatory (e.g. FAR or DFAR) or administrative process, and cooperate with the disclosing Party to obtain where reasonably available an order protecting the Confidential Information from public disclosure. Notwithstanding the foregoing, Customer may comply with any requirement under the Customer's applicable U.S. State law (for non-Federal U.S. Customers)

with respect to use and disclosure of public records including without limitation any applicable "Freedom of Information" laws. If Customer is required by applicable law to disclose any information that would be considered to be Confidential Information as set forth herein, Customer shall make reasonable efforts to notify DocuSign of such disclosure, to limit such disclosure to only that information that is required to be disclosed by applicable law and to cooperate in any effort reasonably made by DocuSign to prevent or limit such disclosure.

11.3 Ownership. Recipient acknowledges that, as between the Parties, all Confidential Information it receives from the disclosing Party, including all copies thereof in Recipient's possession or control, in any media, is proprietary to and exclusively owned by the disclosing Party. Nothing in this Agreement grants Recipient any right, title or interest in or to any of the disclosing Party's Confidential Information. Recipient's incorporation of the disclosing Party's Confidential Information into any of its own materials will not render Confidential Information non-confidential.

11.4 Remedies. Recipient acknowledges that any actual or threatened breach of this Section 10 (Confidentiality) may cause irreparable, non-monetary injury to the disclosing Party, the extent of which may be difficult to ascertain. Accordingly, the disclosing Party may be entitled under applicable law (but not required) to seek injunctive relief in addition to all remedies available to the disclosing Party at law and/or in equity, to prevent or mitigate any breaches of the Agreement or damages that may otherwise result from those breaches. Absent written consent of the disclosing Party to the disclosure, the Recipient, in the case of a breach of this Section 11 (Confidentiality), has the burden of proving that the disclosing Party's Confidential Information is not, or is no longer, confidential or a trade secret and that the disclosure does not otherwise violate this Section 11 (Confidentiality).

12. GOVERNING LAW, VENUE AND CLAIMS

12.1 Governing Law / Venue

(a) U.S. Federal and State/Local Customers. Notwithstanding anything herein to the contrary, provisions of the Agreement pertaining to governing law and venue such as Section 12.1(b) do not apply to Customer's Official Use of DocuSign Services in Customer's capacity as a state, local government, U.S. Federal Government agency, or school official or employee to the extent such provisions are prohibited by Customer's applicable State constitution or laws, or (as applicable) U.S. Federal law.

(b) All other Customers. Except as set forth in Section 12.1(a) (above), this Agreement is governed by the laws of the State of Tennessee, U.S.A., without reference to its choice of law rules to the contrary, and, the Parties hereby irrevocably consent to the exclusive jurisdiction of, and venue in, any Federal or state court of competent jurisdiction located in Davidson County, Tennessee, for the purposes of adjudicating any dispute arising out of this Agreement.

(c) Conventions / Equitable Relief. To the extent permitted by applicable law, choice of law rules, the 1980 U.N. Convention on Contracts for the International Sale of Goods, and the Uniform Computer Information Transactions Act as enacted, shall not apply. Notwithstanding the foregoing, and except as prohibited by applicable law or regulation, either Party may at any time seek and obtain appropriate legal or equitable relief in any court of competent jurisdiction for claims regarding such Party's intellectual property rights. Each Party hereby irrevocably waives, to the fullest extent permitted by law, any and all right to trial by jury in any legal proceeding arising out of or relating to this Agreement.

12.2 English Language. To the extent allowed by law, the English version of this Agreement is binding, and other translations are for convenience only.

12.3 Claims. If the Customer is an "executive agency" of the United States Government (as defined by 41 USC 7101-8), then all Claims (as defined in FAR 52.233-1-c) by DocuSign against the United States for any alleged breach of this Agreement must be brought as a dispute as set forth in the Contract Disputes Act (41 USC 7101).

13. GENERAL

13.1 Relationship. The Parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the Parties.

Except as expressly set forth in this Agreement, nothing in this Agreement, expressed or implied is intended to give rise to any third-party beneficiary.

13.2 Assignability. Neither Party may assign its rights or obligations under this Agreement without the other Party's prior written consent. Notwithstanding the foregoing, except as prohibited by applicable law or regulation, DocuSign may assign its rights and obligations under this Agreement to an Affiliate as part of a reorganization, or to a purchaser of its business entity or substantially all of its assets or business to which rights and obligations pertain, and Customer may assign to a successor agency as part of formal reorganization, provided that: (a) for Customers, if they are authorized to do so by FAR 42.1204 or State equivalent; and (b) any assignee is bound hereby. Other than the foregoing, any attempt by either Party to transfer its rights or obligations under the Agreement will be void.

13.3 Notices. Any notice required or permitted to be given in accordance with this Agreement will be effective only if it is in writing and sent using: (a) DocuSign Services; (b) certified or registered mail; or (c) a nationally recognized overnight courier, to the appropriate Party at the address set forth on the Order Form, with a copy, in the case of DocuSign, to legal@docusign.com. Each Party hereto expressly consents to service of process by registered mail. Either Party may change its address for receipt of notice by notice to the other Party through a notice provided in accordance with this Section 12.3 (Notices). Notices are deemed given upon receipt if delivered using DocuSign Services, or two (2) business days following the date of mailing, or one (1) business day following delivery to a courier.

13.4 Force Majeure. In the event that either Party is prevented from performing, or is unable to perform, any of its obligations under the Agreement due to any cause beyond the reasonable control of the Party invoking this provision and without its fault or negligence (including, without limitation, for causes due to war, fire, earthquake, flood, hurricane, riots, acts of God, telecommunications outage not caused by the obligated Party, or other similar causes) ("**Force Majeure Event**"), the affected Party's performance will be excused and the time for performance will be extended for the period of delay or inability to perform due to such occurrence; provided that the affected Party: (a) provides the other Party with prompt notice of the nature and expected duration of the Force Majeure Event, setting forth the full particulars in connection therewith; (b) uses commercially reasonable efforts to address and mitigate the cause and effect of such Force Majeure Event with all reasonable dispatch; (c) provides periodic notice of relevant developments; and (d) provides prompt notice of the end of such Force Majeure Event. Delays in fulfilling the obligations to pay hereunder are excused only to the extent that payments are entirely prevented by the Force Majeure Event.

13.5 Trade Restrictions. The DocuSign Services, Documentation, and the provision and any derivatives thereof are subject to the export control and sanctions laws and regulations of the United States and other countries that may prohibit or restrict access by certain persons or from certain countries or territories ("**Trade Restrictions**").

(a) Each Party shall comply with all applicable Trade Restrictions in performance of the Agreement. For the avoidance of doubt, nothing in this Agreement is intended to induce or require either Party to act in any manner which is penalized or prohibited under any applicable laws, rules, regulations or decrees.

(b) Customer represents that it is not a Restricted Party. "**Restricted Party**" means any person or entity that is: (i) located or organized in a country or territory subject to comprehensive U.S. sanctions (currently including Cuba, Crimea, Iran, North Korea, Syria) ("**Sanctioned Territory**"); (ii) owned or controlled by or acting on behalf of the government of a Sanctioned Territory; (iii) an entity organized in or a resident of a Sanctioned Territory; (iv) identified on any list of restricted parties targeted under U.S., EU or multilateral sanctions, including, but not limited to, the U.S. Department of the Treasury, Office of Foreign Assets Control's ("**OFAC**") List of Specially Designated Nationals and Other Blocked Persons, the OFAC Sectoral Sanctions List, the U.S. State Department's Nonproliferation Sanctions and other lists, the U.S. Commerce Department's Entity List or Denied Persons List located at https://www.export.gov/article?id=Consolidated-Screening-List, the consolidated list of persons, groups and entities subject to EU financial sanctions from time to time; or (v) owned or controlled by, or acting on behalf of, any of the foregoing.

(c) Customer acknowledges and agrees that it is solely responsible for complying with, and shall comply with, Trade Restrictions applicable to any of its own or its Authorized Users' content or Customer Data transmitted through the DocuSign Services. Customer shall not and shall not permit

any Authorized User to access, use, or make the DocuSign Services available to or by any Restricted Party or to or from within any Sanctioned Territory.

13.6 Anti-Corruption. In connection with the DocuSign Services performed under this Agreement and Customer's use of DocuSign's services, the Parties agree to comply with all applicable anti-corruption and anti-bribery related laws, statutes, and regulations. Customer agrees that it has not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of DocuSign employees or agents in connection with an Order Form, SOW or this Agreement.

13.7 U.S. Government Rights. All DocuSign Services, including Documentation, and any software as may be provided under an applicable Service Schedule, are deemed to be "commercial computer software" and "commercial computer software documentation". "Commercial computer software" has the meaning set forth in FAR section 2.101 for US. Federal civilian agency purchases and DFARS 252.227-7014(a)(1) for U.S. Federal defense agency purchases. If the software is licensed or the DocuSign Services are acquired by or on behalf of a U.S. Federal civilian agency, including acquisitions via GSA contract, DocuSign provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of this Agreement as required in FAR 12.212 (Computer Software) and FAR 12.211 (Technical Data) and their successors. If the software is licensed or the DocuSign Services are acquired by or on behalf of any agency within the DOD, DocuSign provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of this Agreement as specified in DFARS 227.7202-3 and its successors. Only if this is a DOD prime contract or DOD subcontract, the Government acquires additional rights in technical data as set forth in DFARS 252.227-7015. Except as otherwise set forth in an applicable Service Schedule, this Section 13.7 (U.S. Government Rights) is in lieu of, and supersedes, any other FAR, DFARS or other clause or provision that addresses U.S. Government rights in computer software or technical data.

13.8 Publicity. DocuSign agrees that Customer's seals, trademarks, logos, service marks, trade names, and the fact that Customer has a presence on one of DocuSign's websites or uses the DocuSign Services, will not be used by DocuSign without Customer's prior written consent in such a manner as to state or imply that DocuSign's products or services are endorsed, sponsored or recommended by Customer or are considered by Customer to be superior to any other products or services without prior approval from Customer or by other relevant government authority. Except for pages whose design and content is under the control of the Customer, or for links to or promotion of such pages, DocuSign agrees not to display any Customer or government seals, trademarks, logos, service marks, and trade names on our homepage or elsewhere on one of DocuSign's hosted sites unless permission to do so has been granted by Customer or by other relevant government authority. Notwithstanding the foregoing, Customer hereby agrees that DocuSign may list Customer's name in a publicly available customer list on a DocuSign website or elsewhere so long as the name is not displayed in a more prominent fashion than that of any other third-party customer name or is displayed in a manner that implies endorsement or approval by the Customer of DocuSign Services.

13.9 Waiver. The waiver by either Party of any breach of any provision of this Agreement does not waive any other breach. The failure of any Party to insist on strict performance of any covenant or obligation in accordance with this Agreement will not be a waiver of such Party's right to demand strict compliance in the future, nor will the same be construed as a novation of this Agreement.

13.10 Severability. If any part of this Agreement is found to be illegal, unenforceable, or invalid, the remaining portions of the Agreement will remain in full force and effect.

13.11 Entire Agreement. This Agreement is the final, complete, and exclusive expression of the agreement between the Parties regarding the DocuSign Services provided under this Agreement. This Agreement supersedes and replaces, and the Parties disclaim any reliance on, all previous oral and written communications (including any confidentiality agreements pertaining to the DocuSign Services under this Agreement), representations, proposals, understandings, undertakings, and negotiations with respect to the subject matter hereof and apply to the exclusion of any other terms that Customer seeks to impose or incorporate, or which are implied by trade, custom, practice, or course of dealing. This Agreement may be changed only by a written agreement signed by an authorized agent of both Parties. This Agreement will prevail over terms and conditions of any Customer-issued purchase order or other ordering documents, which will have no force and effect, even if DocuSign accepts or does not otherwise reject the purchase order or other ordering document.

The below signatories are authorized to sign on behalf of their respective Party(ies) and to agree to the terms of this MSA and any documents incorporated herein as of the MSA Effective Date.

Customer	**DocuSign, Inc.**
Signature:	Signature:
Name: Title: Date:	Name: Title: Date:

DATA PROTECTION ATTACHMENT FOR DOCUSIGN SERVICES

Version Date: December 1, 2022

This Data Protection Addendum for DocuSign Services ("**DPA")** is incorporated into and made part of the Agreement. Unless otherwise defined in this DPA, capitalized terms will have the meaning given to them in the Agreement. In the event of any conflict between these documents, the following order of precedence applies (in descending order): (a) Binding Corporate Rules; (b) the Standard Contractual Clauses as provided in herein; (c) the body of the DPA; (d) any documents attached to the DPA; and (e) the Agreement.

1. DEFINITIONS. For purposes of this DPA:

"**Binding Corporate Rules**" means DocuSign's Binding Corporate Rules for Processors, the most current version of which is available on DocuSign's website at https://trust.docusign.com/en-us/trust-certifications/gdpr/bcr-p-processor-privacy-code/.

"**Controller,**" "**Business**," "**Processor,**" and "**Service Provider**" (or equivalent terms) have the meanings set forth under Data Protection Laws.

"**Data Breach**" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data managed by DocuSign.

"**Data Protection Laws**" means all applicable laws, regulations, and other legally binding requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, that apply to DocuSign's Processing of Personal Data, including, without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and any associated regulations and amendments, including, when effective, the California Privacy Rights Act amendments ("**CCPA**"); the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"); the Swiss Federal Act on Data Protection ("**FADP**"); the United Kingdom Data Protection Act of 2018 ("**UK GDPR**"); the Australian Privacy Act (No. 119, 1988) (as amended) ("**the Privacy Act**"); the Canadian Personal Information Protection and Electronic Documents Act (**"PIPEDA"**);Law No. 13.709 of 14

August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) (”**LGPD”**); and the Singapore Personal Data Protection Act 2012 (No. 26 of 2012)(“**PDPA**”).

“**Data Subject**” means an identified or identifiable natural person about whom Personal Data relates (or equivalent term under Data Protection Laws).

“**EU SCCs**” means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, located http://data.europa.eu/eli/dec_impl/2021/914/oj, and completed as set forth in Section 7 below.

“**Personal Data**” includes “personal data,” “personal information,” “personally identifiable information,” or equivalent terms that is Processed by DocuSign in connection with providing DocuSign Services under the Agreement, and such terms shall have the same meaning as defined by Data Protection Laws.

“**Process**” and “**Processing**” has the meaning set forth under Data Protection Laws and the Security Attachment for DocuSign Services, and includes any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2. SCOPE AND PURPOSES OF PROCESSING.

2.1 Depending on Data Protection Laws, Customer is a Controller or Business and DocuSign is a Processor or Service Provider with respect to DocuSign’s Processing of Personal Data to provide the DocuSign Services under the Agreement. This DPA applies to DocuSign’s Processing of Personal Data on Customer’s or Customer Affiliate’s behalf (as applicable) for the provision of the DocuSign Services as specified in the Agreement.

2.2 The scope, nature, purposes, and duration of the processing, the types of Personal Data Processed, and the Data Subjects concerned are set forth in this DPA, including its Schedule A. The details provided in Schedule A are deemed to satisfy any requirement to provide such details under any Data Protection Laws.

2.3 DocuSign will Process Personal Data solely: (a) to fulfill its obligations to Customer under the Agreement, including this DPA; (b) on Customer's behalf pursuant to Customer's instructions; and (c) in compliance with Data Protection Laws. DocuSign will not "sell" Personal Data (as such term in quotation marks is defined in Data Protection Laws), "share" or Process Personal Data for purposes of "cross-context behavioral advertising" or "targeted advertising" (as such terms are defined in Data Protection Laws), or otherwise Process Personal Data for any purpose other than for the specific purposes set forth herein or outside of the direct business relationship with Customer. DocuSign will not attempt to link, identify, or otherwise create a relationship between Personal Data and non-personal data or any other data without the express authorization of Customer.

2.4 Customer will ensure that: (a) all such notices have been given, and all such authorizations have been obtained, as required under Data Protection Laws, for DocuSign (and its Affiliates and Subprocessors) to process Personal Data as contemplated by the Agreement and this DPA; (b) it has complied, and will continue to comply, with all Data Protection Laws; and (c) it has, and will continue to have, the right to transfer, or provide access to, Personal Data to DocuSign for Processing in accordance with the terms of the Agreement and this DPA.

2.5 Unless otherwise specified in the Agreement, Customer agrees it will not provide DocuSign with any sensitive or special categories of Personal Data that impose specific data security or data protection obligations on DocuSign in addition to or different from those specified in this DPA (including any appendix to the DPA) or Agreement.

3. PERSONAL DATA PROCESSING REQUIREMENTS. DocuSign will:

(a) Ensure that the persons it authorizes to Process the Personal Data are subject to confidentiality obligations regarding such activity or are under an appropriate statutory obligation of confidentiality.

(b) Promptly notify Customer of: (i) any third-party or Data Subject complaints regarding the Processing of Personal Data; or (ii) any government request for access to or information about DocuSign's Processing of Personal Data on Customer's behalf, unless prohibited by applicable laws. DocuSign will provide Customer with commercially reasonable cooperation and assistance in relation to any such request. If DocuSign is prohibited by applicable laws from disclosing the details of a government request to Customer, DocuSign shall use all available legal mechanisms to challenge any demands

for data access through the applicable government process that it receives, as well as any non-disclosure provisions attached thereto as set forth in DocuSign's Law Enforcement Guidelines, available at https://www.docusign.com/legal/law-enforcement.

(c) Provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by Data Protection Laws.

(d) Provide commercially reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to DocuSign under Data Protection Laws to consult with a regulatory authority in relation to DocuSign's Processing or proposed Processing of Personal Data.

(e) Comply with the CCPA's restrictions pursuant to 1798.140 (e)(6) regarding combining Personal Data with personal data received from, or on behalf of, another person or persons for the purposes enumerated in the CCPA. With respect to its obligations under CCPA, DocuSign certifies that it will comply with them under this DPA (including, without limitation to, the restrictions under Sections 2 and 3).

(f) Promptly notify Customer if it determines that: (i) it can no longer meet its obligations under this DPA or Data Protection Laws; or (ii) in its opinion, an instruction from Customer infringes Data Protection Laws.

4. DATA SUBJECT REQUESTS.

4.1 If DocuSign receives a direct request from a Data Subject regarding rights under Data Protection Laws, DocuSign will promptly notify the request to Customer if the Data Subject has identified Customer as Controller of the Personal Data subject to the request and may inform the Data Subject that it has done so. DocuSign will provide reasonable assistance to Customer in fulfilling its obligations under Data Protection Laws to respond to Data Subject requests, but Customer understands and agrees that, as a Controller, Customer is solely responsible for responding to such Data Subject's requests or inquiries and that DocuSign has no responsibility to respond to a Data Subject for or on behalf of Customer.

4.2 If Customer receives a request or inquiry from a Data Subject related to Personal Data Processed by DocuSign, Customer can either: (a) access its DocuSign Services containing Personal Data to address the request or inquiry; or (b) to the extent such access is not available to Customer, contact DocuSign customer support for additional assistance to enable Customer to address the request or inquiry.

5. DATA SECURITY.

5.1 DocuSign will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data. Details regarding the specific security measures that apply to the DocuSign Services are as described in the Binding Corporate Rules, the Agreement and in the Security Attachment for DocuSign Services. Customer acknowledges that DocuSign's security measures are subject to technical progress and development and that DocuSign may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the DocuSign Services purchased by Customer.

5.2 Customer shall be responsible for properly implementing access and use controls and configuring certain features and functionalities of the DocuSign Services that Customer may elect to use and agrees that it will do so in accordance with this DPA and the Agreement in such manner that Customer deems adequate, including, without limitation, maintaining appropriate security, protection, deletion, and backup of its own Personal Data.

6. DATA BREACH. DocuSign will notify Customer without undue delay upon becoming aware of any Data Breach and will assist Customer in Customer's compliance with its Data Breach-related obligations, including, without limitation, by:

(a) Taking commercially reasonable steps to mitigate the effects of the Data Breach and reduce the risk to Data Subjects whose Personal Data was involved; and

(b) Providing Customer with the following information, to the extent known:

(i) The nature of the Data Breach, including, where possible, how the Data Breach occurred, the potential categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

(ii) The likely consequences of the Data Breach; and

(iii) Measures taken or proposed to be taken by DocuSign to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects and causes.

(c) DocuSign's obligation to report a Data Breach under this DPA is not and will not be construed as an acknowledgement by DocuSign of any fault or liability of DocuSign with respect to such Data Breach. Customer is solely responsible for determining whether to notify impacted Data Subjects and for providing such notice, and for determining whether relevant supervisory authorities need to be notified of a Data Breach as may be required for Customer's own business and activities. Notwithstanding the foregoing, Customer agrees to reasonably coordinate with DocuSign on the content of Customer's intended public statements or required notices for affected Data Subjects and/or notices to relevant supervisory authorities regarding the Data Breach.

7. SUBPROCESSORS.

7.1 Customer acknowledges and agrees that DocuSign may use DocuSign Affiliates and other Subprocessors (as defined in Data Protection Law) to Process Personal Data in accordance with the provisions within this DPA and Data Protection Laws. Where DocuSign subcontracts any of its rights or obligations concerning Personal Data, including to any Affiliate, DocuSign will take steps to select and retain Subprocessors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with Data Protection Laws and this DPA and will remain liable for the performance of all its obligations under the Agreement and this DPA, whether or not performed by DocuSign, its Affiliates or Subprocessors.

7.2 DocuSign's Services Subprocessor List is available on DocuSign's website at https://www.docusign.com/trust/privacy/subprocessors-list (the "**Subprocessor List**"), and notice regarding new DocuSign Service Subprocessors is made available through a subscription mechanism as described on the DocuSign website. Customer agrees to subscribe to the Subprocessor List for DocuSign to notify Customer of new Subprocessor(s) for the applicable DocuSign Services. DocuSign will maintain an up-to-date list of its Subprocessors, and it will provide Customer with thirty (30) days' prior notice of any new Subprocessor added to the list. In the event Customer has a commercially reasonable objection to a new Subprocessor, DocuSign will use reasonable efforts to make available to Customer a change in the

DocuSign Services or recommend a commercially reasonable change to Customer's use of the DocuSign Services to avoid Processing of Personal Data by the objected-to Subprocessor without a material change to Customer's use of the affected DocuSign Services. Customer may, in its sole discretion, terminate the Agreement in the event that DocuSign is not able to provide a reasonable change to cure Customer's Subprocessor objection.

8. INTERNATIONAL DATA TRANSFERS.

8.1 DocuSign will not engage in any cross-border Processing of Personal Data, or transmit, directly or indirectly, any Personal Data to any country outside of the country from which such Personal Data was collected, without complying with Data Protection Laws. Where DocuSign engages in an onward transfer of Personal Data, DocuSign shall ensure that a lawful data transfer mechanism is in place prior to transferring Personal Data from one country to another.

8.2 To the extent DocuSign's cross-border Processing of Personal Data involves a transfer of Personal Data subject to cross-border transfer obligations under Data Protection Laws, the Binding Corporate Rules apply to the Processing of Personal Data by DocuSign and/or its Affiliates as part of the provision of DocuSign Services under the Agreement. The Binding Corporate Rules are incorporated by reference into this DPA, and DocuSign agrees to use commercially reasonable efforts to maintain the regulatory authorization of the Binding Corporate Rules or other appropriate cross-border transfer safeguards for the duration of the Agreement.

8.3 Notwithstanding section 8.2 above, to the extent legally required, by signing this DPA, Customer and DocuSign are deemed to have signed the EU SCCs as an additional safeguard, which form part of this DPA and (except as described in Section 7(d) and (e) below) will be deemed completed as follows:

(a) Module 2 of the EU SCCs applies to transfers of Personal Data from Customer (as a Controller) to DocuSign (as a Processor) and Module 3 applies to transfers of Personal Data from Customer (as a Processor) to DocuSign (as a Subprocessor);

(b) Clause 7 (the optional docking clause) is included;

(c) Under Clause 9 (Use of Subprocessors), the Parties select Option 2 (General written authorization);

(d) Under Clause 11 (Redress), the optional language requiring that Data Subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;

(e) Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the laws of Ireland;

(f) Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;

(g) Annex I(A) and I(B) (List of Parties) is completed as set forth in Schedule A;

(h) Under Annex I(C) (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission;

(i) Annex II (Technical and organizational measures) is completed as provided in Schedule A of this DPA; and

(j) Annex III (List of Subprocessors) is not applicable as the Parties have chosen General Authorization under Clause 9; however, DocuSign's Subprocessor list can be viewed as described above in Section 6.

8.4 With respect to Personal Data transferred from the United Kingdom, for which the UK GDPR (and not the GDPR or FADP) governs the international nature of the transfer, the International Data Transfer DPA to the EU SCCs (available as of the Effective Date at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) ("**UK SCCs**") forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK SCCs. Undefined capitalized terms used in this provision shall mean the definitions in the UK SCCs. The UK SCCs shall be deemed complete as follows: (a) the Parties' details shall be the Parties and their Affiliates to the extent any of them are involved in such transfer; (b) the Key Contacts shall be the contacts set forth in the Agreement; (c) the Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties; (d) either Party may end this DPA as set out in Section 19 of the UK SCCs; and (e) by entering into this DPA, the Parties are deemed to be signing the UK SCCs.

8.5 For transfers of Personal Data that are subject to the FADP, the EU SCCs form part of this DPA as set forth in Section 8.3 of this DPA, but with the following differences, to the extent required by the FADP: (a) references to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (b) references to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; (c) the term "Member State" in EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs; and (d) the relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the EU SCCs (where the FADP and GDPR apply, respectively).

9. AUDITS. To the extent required by Data Protection Laws, DocuSign shall make available such information reasonably requested by Customer to confirm DocuSign's compliance with this DPA (e.g., SOC, ISO, NIST, PCI DSS, similar audit reports issued by a qualified third-party auditor, "**Audit Report**"), or with the Security Attachment for DocuSign Services. Except as provided otherwise in the Agreement or Security Attachment regarding audits, if Customer has a reasonable basis to conclude that an Audit Report provided by DocuSign is not satisfactory to confirm such compliance, Customer may, at Customer's sole expense, upon thirty (30) days' prior notice, request an audit during normal business hours of those DocuSign systems and records relevant to DocuSign's Processing of Personal Data on Customer's behalf. Customer shall limit its exercise of audit rights to not more than once in any twelve (12) calendar month period.

10. RETURN OR DESTRUCTION OF PERSONAL DATA. Prior to termination or expiration of the Agreement, Customer may retrieve Personal Data processed by DocuSign in accordance with the terms of the Agreement and at Customer's request, DocuSign will promptly delete or all Personal Data in its possession or control as soon as reasonably practicable, save that this requirement will not apply to the extent that DocuSign is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data DocuSign will securely isolate and protect from any further processing, except to the extent required by applicable law. For Personal Data stored in Customer's service environment, or for the DocuSign Services for which no bulk data retrieval

functionality is provided by DocuSign as part of the DocuSign Services, Customer acknowledges that it is required to take appropriate action to back up or otherwise store separately any Personal Data while the DocuSign Services environment is still active prior to termination and acknowledges that if Customer elects to have Personal Data returned, Customer acknowledges that DocuSign does not offer bulk data retrieval as part of the DocuSign Services and Customer will be required to engage DocuSign Professional Services or customer support at a reasonable fee payable by Customer to DocuSign.

11. MISCELLANEOUS PROVISIONS.

Notwithstanding anything else to the contrary in the Agreement, DocuSign reserves the right to make any modification to this DPA as may be required to comply with Data Protection Law so long as any such modification shall not degrade any service functionalities or safeguards associated with providing the DocuSign Services.

Any claims brought under this DPA shall be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

This DPA will remain in force and effect through the term of the Agreement, or for as long as DocuSign is Processing Personal Data subject to this DPA, whichever is longer.

Schedule A

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

The exporter (Controller) is Customer and Customer’s contact details and signature are as provided in the Agreement and the DPA.

Data importer(s):

The importer (Processor) is DocuSign, Inc. and DocuSign’s contact details and signature are as provided in the Agreement and the DPA.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Any data subjects whose Personal Data is contained in Data Exporter's data being used in the DocuSign Services, as set out in the Agreement which describes the provision of DocuSign Services to Customer, including Customer's Account Administrator, Authorized Users, representatives, and end users, including, without limitation, Customer's employees, contractors, partners, suppliers, customers, and clients.

Categories of personal data transferred:

Any Personal Data that is provided by Data Exporter to Data Importer in connection with the Agreement and the DPA, including, without limitation, contact information such as name, address, telephone or mobile number, email address, and passwords.

Sensitive data transferred (if applicable): N/A.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

On a continuous basis as needed to provide the DocuSign Services to Customer for the term of the Agreement.

Nature of the processing:

The nature of the Processing is set out in the Agreement between the parties.

Purpose(s) of the data transfer and further processing:

The purposes of the data transfer are for DocuSign to provide the DocuSign Services pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The data will be retained for the time period needed to accomplish the purposes of Processing, unless otherwise required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Please see Section 6 for information about how to access a list of DocuSign's Subprocessors and the nature of the services they provide. All transfers will last for the duration of the Agreement between the parties.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:

The Data Exporter's competent supervisory authority will be determined in accordance with Data Protection Law and, where possible, will be the Irish Data Protection Commissioner.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

SECURITY ATTACHMENT FOR DOCUSIGN SERVICES

Version date: September 20, 2021

This Security Attachment for DocuSign Services ("**Security Attachment**") sets forth DocuSign's commitments for the protection of Customer Data and is made part of Agreement. Unless otherwise defined in this Security Attachment, capitalized terms will have the meaning given to them in the Agreement.

1. DEFINITIONS

"Personnel" means all employees and agents of DocuSign engaged in the performance of DocuSign Services to Customer.

"Process" or **"Processing"** means, with respect to this Security Attachment, any operation or set of operations that is performed upon Customer Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Production Environment" means the System setting where software, hardware, data, processes, and programs are executed for their final and intended operations by end users of DocuSign Services.

"Subcontractor" means a third party that DocuSign has engaged to perform all or a portion of DocuSign Services on behalf of DocuSign.

2. INFORMATION SECURITY PROGRAM

2.1 Information Security Program. DocuSign maintains and will continue to maintain a written information security program that includes policies, procedures, and controls governing the Processing of Customer Data through DocuSign Services ("**Information Security Program**"). The Information Security Program is designed to protect the confidentiality, integrity, and availability of Customer Data by using a multi-tiered technical, procedural, and people-related control approach in accordance with industry best practices and applicable laws and regulations.

2.2 Permitted Use of Customer Data. DocuSign will not Process Customer Data in any manner other than as permitted or required by the Agreement.

2.3 Acknowledgement of Shared Responsibilities. The security of data and information that is accessed, stored, shared, or otherwise Processed via the DocuSign Services are shared responsibilities between DocuSign and Customer. DocuSign is responsible for the implementation and operation of the Information Security Program and the protection measures described in the Agreement and this Security Attachment. Customer is responsible for properly implementing access and use controls and configuring certain features and functionalities of DocuSign Services that Customer may elect to use DocuSign Services in the manner that Customer deems adequate to maintain appropriate security, protection, deletion, and backup of Customer Data.

2.4 Applicability to Customer Data. This Security Attachment and the Information Security Program apply specifically to the Customer Data Processed via DocuSign Services and does not extend to data held on Customer's systems or environments or to any on-premise solutions that may be offered by DocuSign. To the extent Customer exchanges data and information with DocuSign that does not meet the definition of "Customer Data," DocuSign will treat such data and information in accordance with the confidentiality terms set forth in the Agreement.

3. SECURITY MANAGEMENT

3.1 Maintenance of Information Security Program. DocuSign will take and implement appropriate technical and organizational measures to protect Customer Data located in DocuSign Services and will maintain the Information Security Program in accordance with ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001. DocuSign may update or modify the Information Security Program from time to time provided that such updates and modifications do not result in the degradation of the overall security of DocuSign Services.

3.2 Background Checks and Training. DocuSign will ensure that reasonable and appropriate background investigations are conducted on all Personnel in accordance with applicable laws and regulations. Personnel must pass DocuSign's background check requirements prior to being assigned to positions in which they will, or DocuSign reasonably expects them to, have access to Customer Data. DocuSign will conduct annual mandatory security awareness training to inform its Personnel on procedures and policies

relevant to the Information Security Program and of the consequences of violating such procedures and policies. DocuSign will conduct an offboarding or exit process with respect to any Personnel upon termination of employment, which will include the removal of the terminated Personnel's access to Customer Data and DocuSign's sensitive systems and assets.

3.3 Subcontractors. DocuSign will evaluate all Subcontractors to ensure that Subcontractors maintain adequate physical, technical, organizational, and administrative controls, based on the risk tier appropriate to their subcontracted services, that support DocuSign's compliance with the requirements of the Agreement and this Security Attachment. DocuSign will remain responsible for the acts and omissions of its Subcontractors as they relate to the services performed under the Agreement as if it had performed the acts or omissions itself and any subcontracting will not reduce DocuSign's obligations to Customer under the Agreement.

3.4 Risk and Security Assurance Framework Contact. Customer's account management team at DocuSign will be Customer's first point of contact for information and support related to the Information Security Program. The DocuSign account management team will work directly with Customer to escalate Customer's questions, issues, and requests to DocuSign's internal teams as necessary.

4. PHYSICAL SECURITY MEASURES

4.1 General. DocuSign will maintain appropriate physical security measures designed to protect the tangible items, such as physical computer systems, networks, servers, and devices, that Process Customer Data. DocuSign will ensure that commercial grade security software and hardware are utilized to protect DocuSign Services and the Production Environment.

4.2 Facility Access. DocuSign will ensure that: (a) access to DocuSign's corporate facilities is tightly controlled through, at a minimum, physical access card identification; (b) all visitors to its corporate facilities sign in, agree to confidentiality obligations, and be escorted by Personnel while on premises at all times; and (c) visitor logs are reviewed by DocuSign's security team on a regular basis. DocuSign will revoke Personnel's physical access to DocuSign's corporate facilities upon termination of employment.

4.3 Data Centers. DocuSign will use commercial-grade data center service providers in providing the DocuSign Services and will ensure that all data

centers conform to ISO 27001 or equivalent certification. At minimum, all data centers must meet the following requirements:

(a) Multi-factor physical security measures, including auditable entry/exit mechanisms that record the identity of any individual who enters and leaves the facility must be maintained.

(b) Access must be limited to authorized personnel. Third-party vendors and guests must be escorted at all times by authorized personnel while in the data center.

(c) Environmental security controls must be in place, including: (i) uninterruptible power supplies and secondary power supplies on all key systems; (ii) temperature and humidity controls for the heating, ventilation, and air conditioning equipment; (iii) heat and smoke detection devices and fire suppression systems; and (iv) periodic inspections by a fire marshal or similar safety official.

5. LOGICAL SECURITY

5.1 Access Controls. DocuSign will maintain a formal access control policy and employ a centralized access management system to control Personnel access to the Production Environment.

(a) DocuSign will ensure that all access to the Production Environment is subject to successful two-factor authentication globally from both corporate and remote locations and is restricted to authorized Personnel who demonstrate a legitimate business need for such access. DocuSign will maintain an associated access control process for reviewing and implementing Personnel access requests. DocuSign will regularly review the access rights of authorized Personnel and, upon change in scope of employment necessitating removal or employment termination, remove or modify such access rights as appropriate.

(b) DocuSign will monitor and assess the efficacy of access restrictions applicable to the control of DocuSign's system administrators in the Production Environment, which will entail generating system individual administrator activity information and retaining such information for a period of at least twelve (12) months.

(c) DocuSign will not use Customer Data from the Production Environment in non-production environments without Customer’s express permission.

5.2 Auditing and Logging. With respect to system auditing and logging in the Production Environment:

(a) DocuSign will use and maintain an auditing and logging mechanism that, at a minimum, captures and records successful and failed user logons and logoffs (with a date and time stamp, user ID, application name, and pass/fail indicator). User access activities will be logged and audited periodically by DocuSign to identify unauthorized access and to determine possible flaws in DocuSign's access control system.

(b) All application components that have logging capabilities (such as operating systems, databases, web servers, and applications) will be configured to produce a security audit log.

(c) Audit logs will be configured for sufficient log storage capacity.

(d) Each log will be configured so that it cannot be disabled without proper authorization and will send alerts for the success or failure of each auditable event.

(e) Access to security log files will be limited to authorized Personnel.

5.3 Network Security. DocuSign will maintain a defense-in-depth approach to hardening the Production Environment against exposure and attack. DocuSign will maintain an isolated Production Environment that includes commercial grade network management controls such as load balancers, firewalls, intrusion detection systems distributed across production networks, and malware protections. DocuSign will complement its Production Environment architecture with prevention and detection technologies that monitor all activity generated and send risk-based alerts to the relevant security groups.

5.4 Malicious Code Protection. DocuSign will ensure that: (a) its information systems and file transfer operations have effective and operational anti-virus software; (b) all anti-virus software is configured for deployment and automatic update; and (c) applicable anti-virus software is integrated with processes and will automatically generate alerts to DocuSign's Cyber Incident Response Team if potentially harmful code is detected for their investigation and analysis.

5.5 Code Reviews. DocuSign will maintain a formal software development lifecycle that includes secure coding practices against OWASP and related

standards and will perform both manual and automated code reviews. DocuSign's engineering, product development, and product operations management teams will review changes included in production releases to verify that developers have performed automated and manual code reviews designed to minimize associated risks. In the event that a significant issue is identified in a code review, such issue will be brought to DocuSign senior management's attention and will be closely monitored until resolution prior to release into the Production Environment.

5.6 Vulnerability Scans and Penetration Tests. DocuSign will perform both internal and external vulnerability scanning and application scanning. External scans and penetration tests against DocuSign Services and the Production Environment will be conducted by external qualified, credentialed, and industry recognized organizations on a frequency based on risk but, at a minimum, on an annual basis. DocuSign will remedy vulnerabilities identified during scans and penetration tests in a commercially reasonable manner and timeframe based upon classified and prioritized severity level. DocuSign will make available all third-party attestations resulting from vulnerability scans and penetration tests per independent external audit reports. For clarification, under no circumstance will Customer be permitted to conduct any vulnerability scans or penetration testing against the Production Environment.

6. STORAGE, ENCRYPTION, AND DISPOSAL

6.1 Storage & Separation. Customer Data will be stored within the physical and logical infrastructure for the DocuSign Services at DocuSign's colocation or data center facilities. Exceptions with respect to storage may only be made with Customer's written authorization for specific purposes, such as, for example, extraction of Customer Data for storage on encrypted portable media. DocuSign will logically separate Customer Data located in the Production Environment from other DocuSign customer data.

6.2 Encryption Technologies. DocuSign will encrypt Customer Data in accordance with the Documentation, using industry accepted standards, strong encryption techniques, and current security protocols. Electronic transmission or exchange of Customer Data with DocuSign Services will be conducted via secure means.

6.3 Disposal. DocuSign will implement industry recognized processes and procedures for equipment management and secure media disposal under the guidelines identified in the National Institute of Standards' Guidelines for Media Sanitization, SP800-88.

7. BUSINESS CONTINUITY AND DISASTER RECOVERY

7.1 Continuity Plan. DocuSign will maintain written business continuity and disaster recovery plans that address the availability of DocuSign Services (**"Continuity Plans"**). The Continuity Plans will include elements such as: (a) crisis management, plan and team activation, event and communication process documentation; (b) business recovery, alternative site locations, and call tree testing; and (c) infrastructure, technology, system(s) details, recovery activities, and identification of the Personnel and teams required for such recovery. DocuSign will, at a minimum, conduct a test of the Continuity Plan on an annual basis. DocuSign's Continuity Plans shall provide for remediation of any deficiencies discovered during any such Continuity Plan testing within timeframes reasonably commensurate with the level of risk posed by the deficiency. The internal and independent audit reports described in Section 9.1 (Independent Assurances) will evidence or report on the execution of DocuSign's Continuity Plan's tests and any resulting remedial actions.

7.2 DocuSign Service Continuity. DocuSign's production architecture for DocuSign Services is designed to perform secure replication in near real-time to multiple active systems in geographically distributed and physically secure data centers. DocuSign will ensure that: (a) infrastructure systems for DocuSign Services have been designed to eliminate single points of failure and to minimize the impact of anticipated environmental risks; (b) each data center supporting DocuSign Services includes full redundancy and fault tolerance infrastructure for electrical, cooling, and network systems; and (c) Production Environment servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability.

7.3 Disaster Recovery. In the event of a failure of critical services or material business disruption, DocuSign will promptly invoke its Continuity Plans and will restore critical service capability and the production capability of critical information technology infrastructure of the DocuSign Services (including, but not limited to, data centers, hardware, software and power systems, and critical voice, data, and e-commerce communications links), and, except as otherwise provided in the applicable Continuity Plan, DocuSign will use commercially reasonable efforts to promptly notify Customer's Account Administrators of the issue. It is DocuSign's responsibility to cause any of its Subcontractors or outsourcers performing activities that could impact critical processes of DocuSign Services to have plans in place that meet the same standards as required of DocuSign hereunder. Notwithstanding anything to the contrary in the Agreement (including this Security Attachment) and without limiting any of DocuSign's responsibilities

thereunder, DocuSign will not be required to provide business continuity or disaster recovery plans for its colocation or data center facilities to Customer. However, publicly available information and references to the capabilities of any such colocation or data center facility will be provided by DocuSign upon request.

8. DATA INCIDENT RESPONSE AND NOTIFICATION

8.1 General. DocuSign will maintain a tested incident response program, which will be managed and run by DocuSign's dedicated Global Incident Response Team. DocuSign's Global Incident Response Team will operate to a mature framework that includes incident management and breach notification policies and associated processes. DocuSign's incident response program will include, at a minimum, initial detection; initial tactical response; initial briefing; incident briefing; refined response; communication and message; formal containment; formal incident report; and postmortem/trend analysis.

8.2 Data Incident Notification. DocuSign will comply with all applicable security breach notification laws and regulations in its provision of the DocuSign Services and, in any event, will notify Customer without undue delay upon becoming aware of any breach of DocuSign's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data on systems managed by DocuSign (a "**Data Incident**"). Without limiting the generality of the foregoing, the Parties acknowledge and agree that Data Incidents do not include unsuccessful attempts, everyday security alerts, or other events that do not materially compromise the security or availability of Customer Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems. DocuSign's notification of a Data Incident under this section is not an acknowledgement by DocuSign of any fault or liability with respect to the Data Incident.

8.3 Data Incident Response. DocuSign shall take reasonable measures to mitigate the cause of any Data Incident and shall take reasonable corrective measures to prevent the same Data Incident from occurring in the future. As information is collected or otherwise becomes available to DocuSign and unless prohibited by law, DocuSign shall provide information regarding the nature and consequences of the Data Incident that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Due to the encryption configuration and security controls associated with DocuSign Services, DocuSign may not have access to or

know the nature of the information contained within Customer Data and, as such, the Parties acknowledge that it may not be possible for DocuSign to provide Customer with a description of the type of information or the identity of individuals who may be affected by a Data Incident. Customer is solely responsible for determining whether to notify impacted individuals and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer's use of DocuSign Services need to be notified of a Data Incident.

9. INDEPENDENT ASSURANCES AND AUDITS

9.1 Independent Assurances. DocuSign uses independent external auditors to verify the adequacy of its Information Security Program. DocuSign will provide or make available to Customer third-party attestations, certifications, and reports relevant to the establishment, implementation, and control of the Information Security Program, including, where applicable, ISO 27001 certifications, PCI DSS certifications, and Service Organization Controls (SOC) reports.

9.2 Additional Requirements. To the extent Customer requires additional audit information or assistance from DocuSign beyond those set forth in Section 9.1 (Independent Assurances) as required under applicable laws and regulations, Customer may submit its request for such additional information and assistance, which shall include information regarding the applicable laws or regulations forming the basis of the request, to its account management representative. DocuSign will work with Customer to reach mutually agreed upon terms regarding the scope, timing, duration, and other details regarding such additionally requested information and assistance.

9.3 Audit for Data Incident. Following a Data Incident, DocuSign will within a reasonable timeframe, engage a third-party independent auditor, selected by DocuSign and at DocuSign's expense, to conduct an on-site audit of DocuSign's Information Security Program. Upon request, DocuSign will provide or make available a report of such audit to Customer.

9.4 Conditions of Audit.

(a) Any audits conducted pursuant to this Security Attachment must: (i) be conducted during reasonable times and be of reasonable duration; (ii) not unreasonably interfere with DocuSign's day-to-day operations; and (iii) be conducted under mutually agreed upon terms and in accordance with DocuSign's security policies and procedures. DocuSign reserves the right to

limit an audit of configuration settings, sensors, monitors, network devices and equipment, files, or other items if DocuSign, in its reasonable discretion, determines that such an audit may compromise the security of DocuSign Services or the data of other DocuSign customers. Customer's audit rights do not include penetration testing or active vulnerability assessments of the Production Environment or DocuSign Systems within their scope.

(b) In the event Customer conducts an audit through a third-party independent contractor, such independent contractor must enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect DocuSign's confidential information.

(c) Customer must promptly provide DocuSign with any audit, security assessment, compliance assessment reports, and associated findings prepared by it or its third-party contractors for comment and input prior to formalization and/or sharing such information with a third party.

9.5 Remediation and Response Timeline. If any audit performed pursuant to this Security Attachment reveals or identifies any non-compliance by DocuSign of its obligations under the Agreement and this Security Attachment, then (a) DocuSign will work to correct such issues; and (b) for no more than sixty (60) days after the date upon which such audit was conducted, Customer may request feedback and information regarding corrective and remedial actions taken in relation to such audit.

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
9/15/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Marsh & McLennan Agency LLC
5500 Cherokee Avenue, Suite 300
Alexandria VA 22312

CONTACT NAME:
PHONE (A/C, No, Ext): 800-274-0268 **FAX (A/C, No):**
E-MAIL ADDRESS: macertificates@marshmma.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : The Cincinnati Insurance Company	10677
INSURER B : Endurance Assurance Corporation	11551
INSURER C : Hartford Fire Insurance Company	19682
INSURER D :	
INSURER E :	
INSURER F :	

INSURED CARAHTECHN
Carahsoft Technology Corp.
FedResults, Inc.
11493 Sunset Hills Road
Suite 100
Reston VA 20190

COVERAGES **CERTIFICATE NUMBER:** 423607571 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X **COMMERCIAL GENERAL LIABILITY** CLAIMS-MADE X OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: POLICY PRO-JECT X LOC OTHER:	Y	Y	ENP0651059	4/19/2023	4/19/2024	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$ 1,000,000 $ 500,000 $ 10,000 $ 1,000,000 $ 2,000,000 $ 2,000,000
A	**AUTOMOBILE LIABILITY** X ANY AUTO OWNED AUTOS ONLY SCHEDULED AUTOS X HIRED AUTOS ONLY X NON-OWNED AUTOS ONLY	Y	Y	EBA0651059	4/19/2023	4/19/2024	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$ 1,000,000 $ $ $
A	X **UMBRELLA LIAB** X OCCUR **EXCESS LIAB** CLAIMS-MADE DED RETENTION $	Y	Y	ENP0651059	4/19/2023	4/19/2024	EACH OCCURRENCE AGGREGATE	$ 5,000,000 $ 5,000,000
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A					PER STATUTE OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ $ $
B C	Cyber & Professional Liability Crime	Y	Y	NRO30043701400 30TP032740921	8/27/2023 2/6/2023	8/27/2024 2/6/2024	$10,000,000 Occ $5,000,000 Limit	$10,000,000 Agg $50,000 Deductible

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Metropolitan Government of Nashville and Davidson County, its officials, officers, employees, and volunteers are named as additional insureds per general liability additional insured endorsement and automobile liability additional insured endorsement.Contract Number 6508243

CERTIFICATE HOLDER

Metropolitan Government of Nashville and Davidson County
Metro Courthouse
Nashville, TN 37201

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

SOMPO INTERNATIONAL
INSURANCE

US Insurance

Premier Professional Liability and Network Risk Insurance

Policy Number: NRO30043701400
Effective Dates: August 27, 2023 To: August 27, 2024
Endurance Assurance Corporation

Issuing Office:
161 Washington Street
Suite 1600
Conshohocken, PA 19428
www.sompo-intl.com

PN 0027 0221

POLICYHOLDER NOTICE

VIRGINIA CLAIMS - MADE POLICY NOTICE

You have purchased claims-made liability insurance. When this insurance terminates, the insurer will send an offer with the available options for purchasing the supplemental extended reporting period. You may be entitled to receive information on claims under this policy. If you have any questions regarding your claims-made coverage or the importance of purchasing the supplemental extended reporting period, please contact your insurance company or your insurance agent.

SOMPO INTERNATIONAL

NOTICE TO POLICYHOLDERS
Sompo International Breach Assist Hotline

R +1 844 347 7077
Mullen Coughlin LLC

This Notice shall be construed to be a part of your policy, but no coverage is provided by this Notice, and it cannot be construed to replace any provisions of your policy.

If you know or suspect that your organization has suffered a Ransomware event, security breach, or a data breach, please contact the Sompo International Breach Assist Hotline above as soon as possible for immediate assistance.

The Sompo International Breach Assist Hotline is an actively monitored voicemail box. Under normal circumstances, you will be contacted by Sompo International Breach Assist counsel between two and four business hours from the time you leave your message, which should include your organization's name, your Sompo International policy number (if available), and the name and contact information of an individual authorized to discuss the suspected breach.

Your initial call will include a discussion of the Sompo International Breach Assist counsel's role as well as an overview of the incident response process.

Information requested on the initial call typically includes:

- Some general information about your organization
- Details, to the extent known, regarding the data exposure event (e.g. what happened, when the event occurred, when was the event discovered)
- How the event was discovered (e.g. internal discovery or contact from a customer , regulator or credit card company)
- Whether the event has been contained or is potentially ongoing
- The type of data involved and the number of known or potentially affected individuals
- Whether or not there has been any contact with law enforcement
- Whether any party other than Sompo International has been notified

PLEASE NOTE: PROMPT REPORTING OF A BREACH IS CRITICAL. EVEN IF YOU DO NOT YET HAVE ALL OF THE INFORMATION LISTED ABOVE, PLEASE CONTACT THE SOMPO INTERNATIONAL BREACH ASSIST HOTLINE IMMEDIATELY IF A BREACH IS SUSPECTED

Sompo International makes no representation, guarantee or warranty, express or implied, concerning the services or products of any vendors, including any warranty of fitness for a particular purpose, accuracy , reliability, or efficiency of such services or products. Vendors identified by Sompo International in this Notice or in any other materials relating to your policy are independent contractors, and Sompo International has no control over the services rendered or products provided. Your use of the vendors is at the your sole risk, and under no circumstances shall Sompo International be liable for any damages arising from any services rendered or failed to be rendered or any products provided by any vendor identified in this Notice or any other materials.

SOMPO INTERNATIONAL

NOTICE TO POLICYHOLDERS
SOMPO INTERNATIONAL BREACH ASSIST HOTLINE

This Notice shall be construed to be a part of your policy, but no coverage is provided by this Notice, and it cannot be construed to replace any provisions of your policy.

If you know or suspect that your organization has suffered a data breach, or if you have been notified by a third party that you have suffered a breach, please contact the Sompo International Breach Assist Hotline below as soon as possible for immediate assistance.

Sompo International
Breach Assist Hotline
+1 844 347 7077
Mullen Coughlin LLC

The Sompo International Breach Assist Hotline is an actively monitored voicemail box. Under normal circumstances, you will be contacted by Sompo International Breach Assist counsel between two and four business hours from the time you leave your message, which should include your organization's name, your Sompo International policy number (if available), and the name and contact information of an individual authorized to discuss the suspected breach.

Your initial call will include a discussion of the Sompo International Breach Assist counsel's role as well as an overview of the incident response process.

Information requested on the initial call typically includes:

- some general information about your organization;
- details, to the extent known, regarding the data exposure event (e.g. what happened, when the event occurred, when was the event discovered);
- how the event was discovered (e.g. internal discovery or contact from a customer, regulator or credit card company);
- whether the event has been contained or is potentially ongoing;
- the type of data involved and the number of known or potentially affected individuals;
- whether or not there has been any contact with law enforcement; and
- whether any party other than Sompo International has been notified.

PLEASE NOTE: PROMPT REPORTING OF A BREACH IS CRITICAL. EVEN IF YOU DO NOT YET HAVE ALL OF THE INFORMATION LISTED ABOVE, PLEASE CONTACT THE SOMPO INTERNATIONAL BREACH ASSIST HOTLINE IMMEDIATELY IF A BREACH IS SUSPECTED

Sompo International makes no representation, guarantee or warranty, express or implied, concerning the services or products of any vendors, including any warranty of fitness for a particular purpose, accuracy, reliability, or efficiency of such services or products. The vendors identified by Sompo International in this Notice or in any other materials relating to your policy are independent contractors, and Sompo International has no control over the services rendered or products provided. Your use of the vendors is at your sole risk, and under no circumstances shall Sompo International be liable for any damages arising from any services rendered or failed to be rendered or any products provided by any vendor identified in this Notice or any other materials.

SOMPO INTERNATIONAL

SOMPO INTERNATIONAL CYBER RISK PORTAL AND RISK MANAGEMENT RESOURCES NOTICE TO POLICYHOLDERS

This Notice shall be construed to be a part of your policy, but no coverage is provided by this Notice, and it cannot be construed to replace any provisions of your policy.

This Notice provides general information regarding access to and the use of Sompo International's proprietary 24/7 Cyber Risk Portal. The Cyber Risk Portal is a secure, web-based tool provided with your Sompo International policy to help your organization manage network risk and privacy exposures, and to provide information regarding what to do in the event of a privacy incident or network attack. Hosted by NetDiligence, a network security and privacy consulting organization, the Cyber Risk Portal contains network security and data management news, tools, and vendor information.

Once registered, Sompo International insureds have immediate access to risk management resources allowing you to better understand the current state of your organization's network security controls and identify immediate threats to both your network and your company. Many of these services are provided by vendors at no charge to you.

In addition, this site contains contact information for the breach assist experts, who can be retained through the Breach Assist Counsel immediately in the event of a known or suspected privacy incident, ransomware or other network event. Please note that these services are provided by a third-party legal services firm and in most cases any legal advice provided will be subject to that firm's billable rates per hour.

The Cyber Risk Portal is a proprietary service for Sompo International customers only. It contains information regarding a variety of network security and privacy consultants and service providers. Access credentials should not be shared with anyone outside of your organization.

To register for Sompo International's Cyber Risk Portal:

1. Go to https://somposecure.com
2. Complete the registration form using your one time access code: 13177

Once registered, you can access the portal immediately.

If you experience issues using the Cyber Risk Portal or have any related questions, please contact Sompo International directly at: cyberportal@sompo-intl.com.

SOMPO INTERNATIONAL

Sompo International Ransomware and Breach Response Management Resources

Sompo International identifies the leading providers of legal, forensic, and response vendors to assist our clients in the event of a ransomware or data breach incident and offers their services at the most competitive rates. Your first call after learning of an actual or potential breach should be to Sompo International Breach Assist Counsel, who will coordinate the engagement of these firms after consultation with you and Sompo International.

Breach Assist Counsel

Mullen Coughlin LLC
McDonald Hopkins LLC

Credit Monitoring/Mail and Call Center

Kroll
Experian
Epiq
TransUnion

Forensic Investigation/ Restoration

Ankura
Charles River Associates
CrowdStrike
Kivu
Kroll
Mox5
Stroz Friedberg
Tracepoint
Unit 42
West Monroe

Legal/Defense

Baker Hostetler LLP
Ballard Spahr LLP
Davis Wright Tremaine LLP
Holland & Knight LLP
Mullen Coughlin LLC
McDonald Hopkins LLC
Norton Rose Fulbright LLP

Sompo International Risk Management Resources

Sompo International is pleased to provide risk management resources to our insureds to enable you to better understand your current risks and to provide actionable information allowing you to secure network and data resources. The below services are ***offered free of charge*** and ordered through the Sompo International Cyber Risk Portal.

Bait and Phish Social Engineering Testing and Phishing Campaign BAIT&PHISH	Bait and Phish performs a social engineering test of your organization, including a comprehensive email spoofing and phishing campaign. Bait and Phish sends bogus emails with attachments and embedded hyperlinks to ascertain the rates at which employees open these emails and click on links and attachments. In addition, Bait and Phish performs pretext phone-based testing of users in an attempt to gain confidential information such as username and passwords from a defined set of users in the organization. Insureds are provided summary reports at the end of the campaign.
Quiet Audit- Common Vulnerabilities and Exposures Survey NetDiligence®	Sompo International has partnered with NetDiligence ® to provide an easy- to-use online self-assessment that will enable insureds to confirm that their organizations have addressed the most common critical vulnerabilities.
Breach Plan Connect® NetDiligence®	The NetDiligence® solution guides organizations through an online process to develop a data breach-focused Incident Response Plan. NetDiligence hosts the plan providing your organization anytime, anywhere access from any device.

Sompo International makes no representation, guarantee or warranty, express or implied, concerning the services or products of any vendors, including any warranty of fitness for a particular purpose, accuracy, reliability, or efficiency of such services or products. The vendors identified in this Notice and at https://somposecure.com are independent contractors, and Sompo International has no control over the services rendered or products provided. Your use of the vendors is at your sole risk, and under no circumstances shall Sompo International be liable for any damages arising from any services rendered or failed to be rendered or any products provided by any vendor identified in this Notice and at https://somposecure.com.

SOMPO INTERNATIONAL

UNIT 42 BY PALO ALTO NETWORKS

Best Practice Microsoft Office Configuration to Minimize Phishing Risks

Sompo International has partnered with Unit 42, a leading cyber security consulting firm, to provide breach readiness reviews for our Sompo Premier Professional insureds.

With an increase in the number of cyber security compromises as a result of phishing attacks, Unit 42 identified best practices which companies using Microsoft Office 365 can follow to prevent or mitigate the damage from these incidents. Common phishing attacks rely on email system vulnerabilities to obtain sensitive information such as email credentials which can then be used to maliciously alter messages or redirect payments.

We recommend enabling as many of the following Microsoft tools as practical to configure your Office 365 environment to minimize risk. Note that many of the tools referenced below are available at no cost; however, some tools may require a subscription.

Enable multi-factor authentication (MFA)	In conjunction with a strong password policy (password complexity enabled, password rotation etc.) multi-factor authentication adds an extra layer of protection by requiring users to acknowledge an additional challenge to access their account. This lessens the likelihood of a compromise even if a password has been stolen and/or compromised. Details on MFA and an implementation guide are found here: https://support.office.com/en-us/article/set-up-multifactor-authentication-for-office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6
Enable the unified audit log and mailbox audit logging	The Office 365 unified audit log provides a centralized logging facility that includes activities from Azure Active Directory, Exchange Online, SharePoint Online, OneDrive for Business, and other applications. Note that the unified audit log is not currently enabled by default and needs to be manually enabled. Details on enabling the unified audit log and an implementation guide are found here: https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c Mailbox auditing generates additional logs that include mailbox activities performed by the owner, a delegated user, or an administrator. Note that mailbox auditing is not currently enabled by default and needs to be manually enabled. Details on the mailbox activities tracked by mailbox auditing are found here: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/mailboxaudit-logging Details on enabling mailbox auditing and an implementation guide are found here: https://go.microsoft.com/fwlink/p/?LinkID=626109

Configure and enable Data Loss Prevention (DLP)	Data Loss Prevention allows an administrator to identify and create policies to prevent users from accidentally or intentionally sharing sensitive information. DLP can be implemented across all Office 365 applications, SharePoint, and OneDrive. Details on enabling DLP and an implementation guide are found here: https://support.office.com/en-us/article/overview -of-data-loss-prevention-policies -1966b2a7-d1e2-4d92-ab61-42efbb137f5e
Enable Office 365 Cloud Application Security	Microsoft's Cloud Application Security enables an administrator to investigate suspicious activities. Office 365 consists of multiple tools that enable an organization to track a number of suspicious activities from unauthorized users, track ransomware activity, and much more. Note: Office 365 Cloud Application Security is only available to Enterprises Licensees. Details on Office 365 Cloud Application can be found here: https://support.office.com/en-us/article/overview-of-office-365-cloud-app-securit y-81f0ee9a-9645-45ab-ba56-de9cbccab475?ui=en-US&rs=en-US&ad=US
Enable Secure Score	Microsoft's Secure Score is a security analytics score that analyzes an Office 365 settings and activities and compares them to a baseline. A score is calculated which shows whether an organization is aligned with best security practices. Secure Score requires an Enterprise subscription and an administrator account. Details on obtaining, enabling Secure Score and an implementation guide are found here: https://support.office.com/en-us/article/introducing-the-office-365-secure-score-c 9e7160f-2c34-4bd0-a548-5ddcc862eaef

About Unit 42

Unit 42 is a cyber security consulting firm. Our consultants are information security experts with a diverse set of information security skills and experience. We are security engineers, digital forensic experts, malware reversers, penetration testers, and data breach incident responders. We work with organizations to proactively identify and mitigate enterprise risk and to respond to sophisticated network intrusions. We have responded to and managed investigations of complex data breach incidents for global organizations, including attacks by nation-state actors, insiders, and cyber criminals looking to steal confidential, sensitive or proprietary data. In all of our engagements our findings and conclusions are measured against industry best practice, rooted in fact, and designed to withstand opposing party scrutiny.

SOMPO INTERNATIONAL

PREMIER PROFESSIONAL LIABILITY AND NETWORK RISK INSURANCE POLICY DECLARATIONS

CERTAIN INSURING AGREEMENTS OF THIS POLICY PROVIDE COVERAGE ON A CLAIMS-MADE BASIS. EXCEPT AS OTHERWISE PROVIDED HEREIN, THIS POLICY COVERS ONLY CLAIMS FIRST MADE AGAINST THE INSUREDS DURING THE POLICY PERIOD OR THE EXTENDED REPORTING PERIOD, IF APPLICABLE. THE LIMITS OF LIABILITY AVAILABLE TO PAY JUDGMENTS OR SETTLEMENTS SHALL BE REDUCED AND MAY BE EXHAUSTED BY CLAIM EXPENSES. PLEASE READ THIS POLICY CAREFULLY.

POLICY NUMBER: NRO30043701400

INSURER: Endurance Assurance Corporation

Item 1. Named Insured: Carahsoft Technology Corporation
Address: 11493 Sunset Hills Road
Suite 100
Reston, VA 20190

Item 2. Policy Period: From: August 27, 2023 To: August 27, 2024
(Both dates at 12:01 AM at the address of the Named Insured)

Item 3. Coverage Schedule:

	Third-Party Coverage	Each Claim Limit	Insuring Agreement Aggregate Limit	Retention	Retroactive Date
A.	Professional Services Liability	Not Applicable	Not Applicable	Not Applicable	Not Applicable
B.	Technology Services Liability	$5,000,000	$5,000,000	$1,000,000	08/27/2014
C.	Media Liability	$5,000,000	$5,000,000	$1,000,000	08/27/2014
D.	Privacy and Network Security Liability	$5,000,000	$5,000,000	$1,000,000	Full Prior Acts
	First-Party Coverage	**Each Cyber Event Limit**	**Insuring Agreement Aggregate Limit**	**Retention**	
E.	Privacy and Network Security Breach Costs	$5,000,000	$5,000,000	$1,000,000	
F.	Direct Business Interruption Loss	$5,000,000	$5,000,000	$1,000,000	
G.	Contingent Business Interruption Loss	$5,000,000	$5,000,000	$1,000,000	
H.	Digital Asset Loss	$5,000,000	$5,000,000	$1,000,000	
I.	Cyber Extortion Threat	$5,000,000	$5,000,000	$1,000,000	

If no Limit is specified for an Insuring Agreement, then no coverage is provided for that Insuring Agreement.

Item 4. PCI Fines and Penalties Limit: $5,000,000

Item 5. Reward Payments Limit: $50,000

Item 6. Maximum Aggregate Limit of Liability: $5,000,000

Item 7. Continuity Date: August 27, 2023

Item 8. Waiting Period:

A. Direct Business Interruption Loss:	15 Hours
B. Contingent Business Interruption Loss:	15 Hours

Item 9. Optional Extended Reporting Period:

Additional Period:	Additional Premium (Percent of Annual Premium):
3 Year	300%

Item 10. Professional Services:

Not applicable

Item 11. Total Premium: [redacted]

Item 12. Producer: MMA Northeast

Address: 5500 Cherokee Avenue
Suite 300
Alexandria, VA 22312

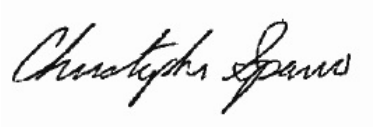
Item 13. Notice:

A. Claims, Circumstances, Cyber Events, and Proof of Loss:	Sompo Pro Attn: Claims Department 1221 Avenue of The Americas New York, NY 10020 Insuranceclaims@sompo-intl.com 1-877-676-7575
B. Breach Assist Hotline:	(844) 347-7077
C. All Other Notices:	Sompo Pro Attn: Professional Lines Underwriting Department 1221 Avenue of The Americas New York, NY 10020

Item 14. Forms and Endorsements Effective at Inception:
See attached Forms and Endorsements Schedule.

This Policy shall constitute the contract between the Insureds and the Insurer.

The Insurer hereby causes this Policy to be signed on the Declarations page by a duly authorized representative of the Insurer.



Authorized Representative

September 13, 2023

Date

FORMS AND ENDORSEMENT SCHEDULE

PREMIER PROFESSIONAL LIABILITY AND NETWORK RISK INSURANCE

End. No.	Title	Number
	Virginia Policyholder Notice	PN 0003 1018 VA
	Premier Professional Liability and Network Risk Insurance Policy Declarations	SPP 1001 0119
	Forms and Endorsement Schedule	IL 0101 0712
1	Computer Property Damage Endorsement	SPP 3024 0119
2	Consequential Reputational Loss Coverage Endorsement	SPP 3027 0119
3	Contingent Business Interruption System Failure Coverage Endorsement	SPP 3031 0119
4	Cyber Terrorist Attack Amended Endorsement	SPP 3123 0119
5	False Claims Act Exclusion Endorsement	SPP 3193 0223
	Important Information Regarding Your Insurance	SIL PN 069 0321
6	Interruption of Service Amended - Voluntary Shutdown Endorsement	SPP 3059 0119
7	Nuclear Energy Liability Exclusion Endorsement	SPP 3076 0119
8	Ransomware Support Endorsement	SPP 3153 0121
	Premier Professional Liability and Network Risk Insurance Policy	SPP 2001 0119
	Signature Page	IL 1007 1222
	U.S. Treasury Department's Office of Foreign Assets Control (OFAC)	PN 0001 0721

The titles of the endorsements listed above are solely for convenience and form no part of the terms and conditions of coverage.

ENDORSEMENT

Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	August 27, 2023 12:01 AM Standard Time at the address of the Named Insured as shown in the Declarations.	Endorsement Number:	1

COMPUTER PROPERTY DAMAGE ENDORSEMENT

It is agreed that:

I. Item 3. of the Declarations is amended by the addition of the following:

Computer System Property Damage Each Cyber Event Limit: $5,000,000
Computer System Property Damage Insuring Agreement Aggregate Limit: $5,000,000

Computer System Property Damage Retention: $1,000,000

II. Section I. INSURING AGREEMENTS is amended by the addition of the following:

Computer System Property Damage Insuring Agreement

The Insurer shall pay the Company for Computer System Property Damage that is directly attributable to a Computer System Property Damage Event first Discovered during the Policy Period.

III. Section III. DEFINITIONS is amended as follows:

A. The Definition of Cyber Event is amended by the addition of the following:

Cyber Event also means a Computer System Property Damage Event.

B. The Definition of Loss is amended by the addition of the following:

Solely with respect to the Computer System Property Damage Insuring Agreement, Loss means only Computer System Property Damage.

C. The following Definitions are added:

Computer System Property Damage means the reasonable and necessary costs to repair or replace a Computer System or a component of a Computer System resulting from a Computer System Property Damage Event.

Computer System Property Damage Event means injury to, or loss or destruction of, a Computer System owned and managed by the Insured if such injury or loss or destruction is caused by the Unauthorized Access or Use of, or the transmission of Malicious Code to, such Computer System.

IV. Exclusion IV.A.1. Bodily Injury and Property Damage is amended by the addition of the following:

Solely with respect to the Computer System Property Damage Insuring Agreement, Paragraph b. of this Exclusion shall not apply to Computer System Property Damage.

V. Subsection VI.C. Cooperation with respect to Cyber Events is amended by the addition of the following:

The Insured agrees to take all reasonable steps and measures to limit or mitigate Computer System Property Damage.

VI. Section VII. NOTICE AND PROOF OF LOSS is amended by the addition of the following:

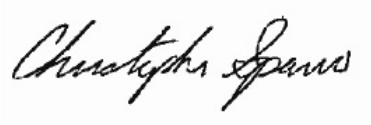
Notice of a Computer System Property Damage Event

As a condition precedent to coverage for Computer System Property Damage, the Insured shall provide written notice to the Insurer of the Computer System Property Damage Event giving rise to such Computer System Property Damage as soon as practicable after such Computer System Property Damage Event is Discovered.

VII. Section XI. GENERAL CONDITIONS is amended by the addition of the following:

Calculation of Computer System Property Damage

For purposes of determining Computer System Property Damage, the amount of Computer System Property Damage the Insurer shall pay shall be the lesser of either the cost to repair or the cost to replace a Computer System or a component of a Computer System that is affected by a Computer System Property Damage Event. Any such Computer System or component shall be valued at actual cash value as of the time of the Computer System Property Damage Event, and shall not include any costs or expenses incurred to update, restore, replace, or otherwise improve the Computer System to a level of functionality beyond that which existed prior to the Computer System Property Damage Event.



Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ENDORSEMENT

Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	August 27, 2023 12:01 AM Standard Time at the address of the Named Insured as shown in the Declarations.	Endorsement Number:	2

CONSEQUENTIAL REPUTATIONAL LOSS COVERAGE ENDORSEMENT

It is agreed that:

I. The Declarations is amended by the addition of the following:

Consequential Reputational Loss Insuring Agreement Aggregate Limit: $5,000,000
Consequential Reputational Loss Each Cyber Event Limit: $5,000,000
Consequential Reputational Loss Retention: $1,000,000
Reputational Loss Waiting Period: Fourteen (14) Days

II. Section I. INSURING AGREEMENTS is amended by the addition of the following:

Consequential Reputational Loss Insuring Agreement

The Insurer shall pay the Company for Consequential Reputational Loss, incurred during the Reputational Loss Coverage Period, that is directly attributable to a Privacy Event or Network Security Event first Discovered during the Policy Period.

III. Section III. DEFINITIONS is amended as follows:

A. The Definition of Loss is amended by the addition of the following:

Solely with respect to the Consequential Reputational Loss Insuring Agreement, Loss means only Consequential Reputational Loss.

B. The following Definitions are added:

Adverse Media means any report or communication published or broadcast in any medium to the general public concerning a Privacy Event or Network Security Event of the Company that is first Discovered during the Policy Period.

Consequential Reputational Loss means the net profit before taxes that the Insured does not realize as a direct result of reputational harm to the Company that is directly attributable to Adverse Media first published or broadcast during the Policy Period.

Consequential Reputational Loss does not include:

1. Breach Costs;

2. any loss arising out of any liability to any third party;

3. any legal costs or legal expenses of any type;

4. any regular or overtime wages, salaries, fees, or benefits of the Insured Persons of, or overhead expenses of, the Company; or

5. any loss incurred as a result of unfavorable business conditions, loss of market, or any other consequential loss.

Reputational Loss Coverage Period means the thirty (30) day period beginning the date and time that the Reputational Loss Waiting Period concludes.

Reputational Loss Waiting Period means the period of time set forth in the Declarations beginning the date and time that Adverse Media is first published or broadcast.

IV. Subsection V.C. Related Claims and Cyber Events is amended by the addition of the following:

All Adverse Media in connection with the same Network Security Event or Privacy Event or any Interrelated matters shall be deemed to have been first published or broadcast at the time the first of such Adverse Media is published or broadcast.

V. Section VII. NOTICE AND PROOF OF LOSS is amended by the addition of the following:

Notice of Consequential Reputational Loss

As a condition precedent to coverage under this Policy for Consequential Reputational Loss, the Insured shall:

1. provide the Insurer written notice of the Network Security Event or Privacy Event giving rise to such Consequential Reputational Loss as soon as practicable , but in no event later than sixty (60) days, after the Insured first becomes aware of such Network Security Event or Privacy Event;

2. furnish affirmative proof of the Consequential Reputational Loss with full particulars to the Insurer as soon as practicable, but in no event later than sixty (60) days, after the Insured incurs the Consequential Reputational Loss;

3. submit to examination under oath at the Insurer's request;

4. produce all pertinent records at such reasonable times and places as the Insurer shall designate; and

5. provide full cooperation with the Insurer in all matters pertaining to the Consequential Reputational Loss.

VI. Section XI. GENERAL CONDITIONS is amended by the addition of the following:

Consequential Reputational Loss Valuation

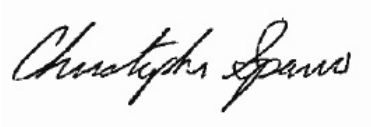
In determining the amount of Consequential Reputational Loss covered under the Consequential Reputational Loss Insuring Agreement, the Insurer shall give due consideration to the net profit or loss of the Company prior to the Reputational Loss Coverage Period and the probable net profit or loss of the Company if the Network Security Event or Privacy Event had not occurred. Such net profit or loss calculations shall not include any net income that would likely have been earned as a result of an increase in the volume of the Company's business due to favorable business conditions caused by the impact of any event similar to such Network Security Event or Privacy Event suffered by other businesses. The Company shall provide the Insurer with access to all relevant sources of information, including, but not limited to:

1. the Company's financial records, tax returns, and accounting procedures;

2. bills, invoices, and other vouchers; and

3. deeds, liens, and contracts;

within ninety (90) days of the end of the Reputational Loss Coverage Period.



Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ENDORSEMENT

Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	August 27, 2023 12:01 AM Standard Time at the address of the Named Insured as shown in the Declarations.	Endorsement Number:	3

CONTINGENT BUSINESS INTERRUPTION SYSTEM FAILURE COVERAGE ENDORSEMENT

It is agreed that:

I. The Declarations is amended by the addition of the following:

Contingent Business Interruption System Failure Sublimit: $5,000,000
Contingent Business Interruption System Failure Each Event Limit: $5,000,000

II. Section III. DEFINITIONS is amended as follows:

A. The Definition of Contingent Business Income Loss is replaced with the following:

Contingent Business Income Loss means Business Income Loss incurred by the Company as a result of an Interruption of Service caused solely and directly by:

1. a network security event impacting the Computer System of a Qualified Service Provider, but only if such network security event would have been covered under this Policy had such network security event directly impacted the Insured's Computer System; or

2. a System Failure Event.

B. The Definition of System Failure Event is amended by the addition of the following:

Solely for purposes of Insuring Agreement G., System Failure Event means only an error or omission committed by a Qualified Service Provider in the management of the Computer System of a Qualified Service Provider that gives rise to an Interruption of Service.

III. Subsection V.A. Limits of Liability is amended by the addition of the following:

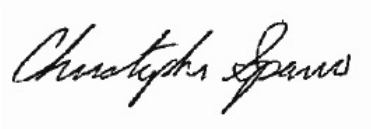
Contingent Business Interruption System Failure Sublimit

The Insurer's maximum liability for all Contingent Business Income Loss on account of all System Failure Events shall be limited to the amount set forth in the Declarations as the Contingent Business Interruption System Failure Sublimit, which is part of, and not in addition to, the Insuring Agreement Aggregate Limit applicable to Insuring Agreement G. set forth in Item 3. of the Declarations. If the Contingent Business Interruption System Failure Sublimit is exhausted, then the

Insurer's obligations with respect to the payment of any and all Contingent Business Income Loss on account of all System Failure Events shall be completely fulfilled and extinguished.

Contingent Business Interruption System Failure Each Event Limit

Notwithstanding anything to the contrary in this Policy, the Insurer's maximum liability for all Contingent Business Income Loss on account of each Interruption of Service caused by a System Failure Event under Insuring Agreement G. shall not exceed the Contingent Business Interruption System Failure Each Event Limit set forth in the Declarations, which is part of, and not in addition to, the Contingent Business Interruption System Failure Sublimit.



Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ENDORSEMENT

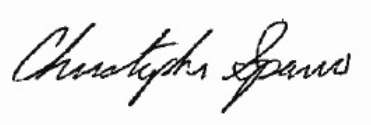
Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	August 27, 2023 12:01 AM Standard Time at the address of the Named Insured as shown in the Declarations.	Endorsement Number:	4

CYBER TERRORIST ATTACK AMENDED ENDORSEMENT

It is agreed that:

The Definition of Cyber Terrorist Attack is replaced with the following:

> Cyber Terrorist Attack means an actual or threatened network-based attack against a Computer System by a person or group of people, known or unknown, for the purposes of influencing the government of any nation or political division thereof (whether such government is *de jure* or *de facto*), or in pursuit of political, religious, ideological, social, or economic objectives or to cause harm to or intimidate any person or entity in furtherance of such objectives.



Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ENDORSEMENT

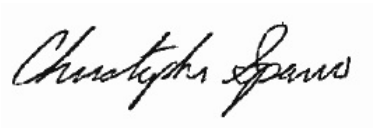
Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	August 27, 2023 12:01 AM Standard Time at the address of the Named Insured as shown in the Declarations.	Endorsement Number:	5

FALSE CLAIMS ACT EXCLUSION ENDORSEMENT

It is agreed that:

Subsection C. of Section IV. EXCLUSIONS is amended by the addition of the following:

The Insurer shall not be liable for Loss on account of any Claim based upon, arising out of, or attributable to any actual or alleged violation of the False Claims Act (31 U.S.C. §§ 3729-3733), or any similar provision of any federal, state, local, or foreign law.



Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

SOMPO INTERNATIONAL

IMPORTANT INFORMATION REGARDING YOUR INSURANCE

In the event you need to contact someone about this insurance for any reason, please contact your agent. If no agent was involved in the sale of this insurance, or if you have additional questions, you may contact the insurance company issuing this insurance at the following address and telephone number:

Sompo International
1221 Ave of the Americas 18th floor
New York City, NY, 10020

Telephone: 877-734-3722

If you have been unable to contact or obtain satisfaction from the company or agent, you may contact the Virginia State Corporate Commission's Bureau of Insurance at:

Bureau of Insurance
P.O. Box 1157
Richmond, VA 23218-1157

Telephone: 804-371-9185

Written correspondence is preferable so that a record of your inquiry is maintained. When contacting your agent, company or the Bureau of Insurance, have your policy number available.

ENDORSEMENT

Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	August 27, 2023 12:01 AM Standard Time at the address of the Named Insured as shown in the Declarations.	Endorsement Number:	6

INTERRUPTION OF SERVICE AMENDED - VOLUNTARY SHUTDOWN ENDORSEMENT

It is agreed that:

The Definition of Interruption of Service is amended by the addition of the following:

Solely with respect to Insuring Agreement F., Interruption of Service also means any reasonable and necessary voluntary shutdown of the Insured's Computer System to prevent or mitigate the effects of a Network Security Event.

Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ENDORSEMENT

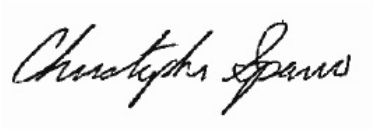
Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	August 27, 2023 12:01 AM Standard Time at the address of the Named Insured as shown in the Declarations.	Endorsement Number:	7

NUCLEAR ENERGY LIABILITY EXCLUSION ENDORSEMENT

It is agreed that:

Section IV. EXCLUSIONS is amended by the addition of the following:

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to any radioactive, toxic, explosive, or other hazardous properties of any nuclear material, nuclear assembly, or nuclear component thereof.



Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ENDORSEMENT

Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	August 27, 2023 12:01 AM Standard Time at the address of the Named Insured as shown in the Declarations.	Endorsement Number:	8

RANSOMWARE SUPPORT ENDORSEMENT

It is agreed that:

I. Section III. DEFINITIONS is amended as follows:

A. The Definition of Cyber Extortion Threat is amended by the addition of the following:

Cyber Extortion Threat also means a Ransomware Event.

B. The Definition of Digital Asset Replacement Expenses is amended by the addition of the following:

Notwithstanding any provision of this Policy to the contrary, when incurred in connection with a Digital Asset Loss Event caused by a Ransomware Event, Digital Asset Replacement Expenses must be incurred through a Breach Response Vendor with the prior consent of the Insurer, which shall not be unreasonably withheld.

C. The Definition of Extortion Expenses is replaced with the following:

Extortion Expenses means reasonable and necessary expenses, other than Extortion Payments or Reward Payments:

1. with respect to Cyber Extortion Threats other than Ransomware Events, incurred by the Company and resulting directly from such Cyber Extortion Threat;

2. with respect to Ransomware Events, incurred by the Company through a Breach Response Vendor solely in order to obtain or to electronically transact an Extortion Payment resulting directly from a Ransomware Event;

and incurred with the prior consent of the Insurer, which shall not be unreasonably withheld.

D. The Definition of Extortion Payments is replaced with the following:

Extortion Payments means monies or digital currency paid by the Company, with the prior consent of the Insurer, to a third party whom the Company reasonably believes to be responsible for a Cyber Extortion Threat, in order to terminate the Cyber Extortion Threat; provided that the Insurer shall not be liable to reimburse the Company for any Extortion Payment if in the opinion of the Insurer such payment could violate any applicable law or regulation.

E. The Definition of Extra Expenses is amended by the addition of the following:

Notwithstanding any provision of this Policy to the contrary, when incurred in connection with an Interruption of Service caused by a Ransomware Event or by Ransomware that impacts a Computer System of a Qualified Service Provider, Extra Expenses must be incurred through a Breach Response Vendor with the prior consent of the Insurer, which shall not be unreasonably withheld.

F. The following Definitions are added:

Ransomware means malware incorporating cryptography that is used to threaten to publish data accessed through a Computer System or to prevent access to data or a Computer System unless a ransom is paid.

Ransomware Event means the introduction of Ransomware into the Insured's Computer System without the active assistance or participation of a Control Group Member of a Company.

II. Section XI. GENERAL CONDITIONS is amended by the addition of the following:

Notwithstanding any provision of this Policy to the contrary, the Insurer shall not be liable to reimburse the Company for any Extortion Payment if in the opinion of the Insurer such payment could violate any applicable law or regulation.

Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

PREMIER PROFESSIONAL LIABILITY AND NETWORK RISK INSURANCE POLICY

In consideration of the payment of premium and subject to all provisions of this Policy, including the Application and all forms attached hereto, the Insureds and the Insurer agree as follows:

I. INSURING AGREEMENTS

A. Professional Services Liability

If Insuring Agreement A. is purchased, the Insurer shall pay Loss on behalf of an Insured on account of a Claim first made against such Insured during the Policy Period or the Extended Reporting Period, if applicable, for a Professional Services Wrongful Act that first takes place on or after the Retroactive Date and before the end of the Policy Period.

B. Technology Services Liability

If Insuring Agreement B. is purchased, the Insurer shall pay Loss on behalf of an Insured on account of a Claim first made against such Insured during the Policy Period or the Extended Reporting Period, if applicable, for a Technology Wrongful Act that first takes place on or after the Retroactive Date and before the end of the Policy Period.

C. Media Liability

If Insuring Agreement C. is purchased, the Insurer shall pay Loss on behalf of an Insured on account of a Claim first made against such Insured during the Policy Period or the Extended Reporting Period, if applicable, for a Media Wrongful Act that takes place on or after the Retroactive Date and before the end of the Policy Period.

D. Privacy and Network Security Liability

If Insuring Agreement D. is purchased, the Insurer shall pay Loss on behalf of an Insured on account of a Claim first made against such Insured during the Policy Period or the Extended Reporting Period, if applicable, for a Privacy Event or Network Security Event that takes place on or after the Retroactive Date and before the end of the Policy Period.

E. Privacy and Network Security Breach Costs

If Insuring Agreement E. is purchased, the Insurer shall pay the Company for Breach Costs that are directly attributable to a Privacy Event or Network Security Event first Discovered during the Policy Period.

F. Direct Business Interruption Loss

If Insuring Agreement F. is purchased, the Insurer shall pay the Company for Direct Business Income Loss and Extra Expenses incurred during the Period of Restoration due to an Interruption of Service that first occurs during the Policy Period, if the length of the Interruption of Service exceeds the Waiting Period set forth in the Declarations.

G. Contingent Business Interruption Loss

If Insuring Agreement G. is purchased, the Insurer shall pay the Company for Contingent Business Income Loss and Extra Expenses incurred during the Period of Restoration due to an Interruption of Service that first occurs during the Policy Period, if the length of the Interruption of Service exceeds the Waiting Period set forth in the Declarations.

H. Digital Asset Loss

If Insuring Agreement H. is purchased, the Insurer shall pay the Company for Digital Asset Replacement Expenses that are directly attributable to a Digital Asset Loss Event first Discovered during the Policy Period.

I. Cyber Extortion Threat

If Insuring Agreement I. is purchased, the Insurer shall pay the Company for Extortion Expenses, Extortion Payments, and Reward Payments that are directly attributable to a Cyber Extortion Threat first received by the Company during the Policy Period.

II. EXTENSIONS

A. Spouses, Domestic Partners, Estates, Heirs, Assigns and Legal Representatives

Subject to all other terms and conditions of this Policy, coverage under this Policy extends to a Claim made against:

1. the lawful spouse or Domestic Partner of an Insured Person, but only for a Claim against that spouse or Domestic Partner due to his or her status as such, or due to such spouse's or Domestic Partner's ownership interest in property from which the claimant seeks recovery; or

2. the estates, heirs, legal representatives, or assigns of an Insured Person who is deceased, legally incompetent, bankrupt, or insolvent;

but only for a Wrongful Act of, or a Privacy Event or Network Security Event directly involving, an Insured Person. This extension of coverage shall not apply to Loss attributable to any act, error, or omission of a spouse, Domestic Partner, estate, heir, legal representative, or assignee of any Insured Person. Each Claim to which this extension of coverage applies shall be treated as a Claim against an Insured Person for purposes of applying the provisions of this Policy.

B. Extended Reporting Periods

1. Automatic Extended Reporting Period

If the Insurer cancels or nonrenews this Policy for reasons other than fraud or non-payment of premium or the Named Insured cancels or nonrenews this Policy, then the Insurer shall provide the Insureds with an automatic Extended Reporting Period of sixty (60) days to immediately follow the end of the Policy Period. The automatic Extended Reporting Period shall not apply to any Claim covered under any policy of insurance that the Insured has purchased to replace the insurance provided by this Policy, or that would be covered under any such policy of insurance but for the application of a retention or the exhaustion of the limit of liability of such insurance.

2. Optional Extended Reporting Period

   a. If the Insurer cancels or nonrenews this Policy for reasons other than fraud or non-payment of premium or the Named Insured cancels or nonrenews this Policy, then the Named Insured shall have the right to purchase an optional Extended Reporting Period to immediately follow the end of the Policy Period.

   b. The right to purchase the optional Extended Reporting Period will lapse unless, within thirty (30) days following the end of the Policy Period, the Insurer receives written notice of the Extended Reporting Period option elected along with payment of the additional premium for such optional Extended Reporting Period, as set forth in the Declarations.

   c. If purchased, the optional Extended Reporting Period cannot be canceled by the Insured and cannot be canceled by the Insurer, except for non-payment of premium.

   d. As a condition precedent to the Named Insured's option to elect the optional Extended Reporting Period, any and all premiums and Retentions that are due must have been paid and the Named Insured must have complied with all other terms and conditions of this Policy.

   e. If the optional Extended Reporting Period is purchased, it shall run concurrently with the automatic Extended Reporting Period.

3. Coverage under any Extended Reporting Period applies only to Claims first made during the Extended Reporting Period, and only for Wrongful Acts, Privacy Events, or Network Security Events actually or allegedly taking place on or after the Retroactive Date and before the end of the Policy Period. Any such Claim will be deemed to have been made during the Policy Period.

4. The Extended Reporting Periods shall be subject to all other terms and conditions of this Policy.

III. DEFINITIONS

Whether in the singular or plural:

Additional Insured means any person or entity that a Company is required by written contract to add as an Insured to this Policy.

Application means all applications, including any written application and all attachments, and all other materials and information provided by or on behalf of the Insured to the Insurer for purposes of underwriting this Policy or any policy of which this Policy is a direct or indirect renewal or replacement.

Bodily Injury means physical injury, sickness, disease, or death of any person, and emotional distress or mental anguish arising out of the foregoing.

Breach Costs means reasonable and necessary fees, costs, charges, and expenses, charged by a Breach Response Vendor and incurred by the Company within twelve (12) months after a Privacy Event or Network Security Event is Discovered, to:

1. conduct any investigation, including a computer forensic investigation, and analysis of the Insured's Computer System to determine the cause and extent of such Privacy Event or Network Security Event;

2. determine indemnification obligations of any third party to the Company, or of the Company to any third party, under any written contract in connection with a Privacy Event or Network Security Event;

3. determine if the Company is obligated to notify those affected or applicable regulatory agencies of such Privacy Event or Network Security Event;

4. respond to the Privacy Event or Network Security Event in a way that complies with the applicable Privacy Regulation that is most favorable to those affected;

5. notify and consult with those affected by the Privacy Event or Network Security Event or applicable regulatory agencies of such Privacy Event or Network Security Event, including, without limitation, mailing list development, mailing list cleansing, postage fees, and related call center services, including any of the foregoing undertaken voluntarily by the Company to prevent or mitigate potential liability on account of a Privacy Event or Network Security Event;

6. plan, implement, execute, and manage a public relations campaign to counter or mitigate any actual or anticipated adverse effects of negative publicity from such Privacy Event or Network Security Event or to protect the Company's business reputation in response to negative publicity following such Privacy Event or Network Security Event;

7. provide credit monitoring or identity monitoring and restoration services and related call center services for the individuals affected by the Privacy Event or Network Security Event, including, without limitation, credit monitoring or identity monitoring and restoration services purchased voluntarily by the Company to prevent or mitigate potential liability on account of such Privacy Event or Network Security Event; or

8. provide any other services not included in 1.-7. above in connection with such Privacy Event or Network Security Event with the prior consent of the Insurer.

Breach Costs do not include:

a. regular or overtime wages, salaries, fees, or other compensation of the Executives or Employees of a Company, or any overhead of the Company;

b. the cost to comply with any injunctive or other non-monetary relief; or

c. taxes, fines, sanctions, or penalties.

Breach Response Vendor means a vendor on the Insurer's pre-approved panel of breach response vendors.

Business Income Loss means, if incurred during the Period of Restoration as a result of an Interruption of Service, the sum of:

1. net profit or loss before taxes that the Company does not realize due to such Interruption of Service; and

2. any normal operating expenses incurred by the Company, including payroll, but only if such operating expenses must continue during the Period of Restoration.

Business Income Loss does not include any increase in the amount of the foregoing due to an increase in the length of an Interruption of Service or the Period of Restoration resulting from the enforcement of any law, ordinance, or regulation.

Claim means:

1. a written demand received by an Insured for monetary or non-monetary relief, including a demand for injunctive relief, commenced by receipt of such demand;

2. a civil proceeding commenced by the service of a complaint or similar pleading on an Insured;

3. an arbitration, mediation, or other formal alternative dispute resolution proceeding commenced by receipt by an Insured of a written demand or similar document;

or an appeal of any of the foregoing;

4. a written request received by an Insured to toll or waive a statute of limitations with respect to a Wrongful Act or a Privacy Event or Network Security Event; or

5. solely with respect to Insuring Agreement D., a Regulatory Proceeding commenced by receipt by an Insured of a written request for information, subpoena, investigative demand, complaint, or similar document.

Claim Expenses means reasonable and necessary costs, fees (including, without limitation, attorneys' fees and experts' fees), and expenses (other than compensation or benefits of any Executives or Employees of, or any overhead expenses of, the Company) incurred by or on behalf of an Insured in investigating defending, settling, or appealing Claims, and the premiums for appeal, attachment, or similar bonds. However the Insurer has no obligation to furnish any such bonds. Claim Expenses do not include any amount incurred by an Insured in any matter that is not at that time a Claim.

Company means the Named Insured and any Subsidiaries, including any of the foregoing as a debtor-in-possession under the United States bankruptcy law or an equivalent status under foreign law, and solely for purposes of Insuring Agreements A., B., C., and D., any Additional Insured that is not a natural person, but only for Wrongful Acts of an Insured other than an Additional Insured, or acts or omissions of an Insured, other than an Additional Insured, that give rise to a Cyber Event.

Computer System means computers, wireless and mobile communications devices, and associated software, input and output devices, data storage devices and the data stored on such devices, networking equipment, telecommunications equipment, closed circuit television equipment, and back up facilities.

Consumer Redress Funds means money the Company is legally required to deposit in a fund established and administered solely for the payment of consumer claims due to a settlement of, or an adverse judgment in, a Regulatory Proceeding.

Contingent Business Income Loss means Business Income Loss incurred by the Company as a result of an Interruption of Service caused solely and directly by a network security event impacting the Computer System of a Qualified Service Provider, but only if such network security event would have been covered under this Policy had such network security event directly impacted the Insured's Computer System.

Control Group Member means a principal, partner, member of the board of directors, corporate officer, in-house general counsel, risk manager, or the functional equivalent of any of the foregoing positions in an organization.

Cyber Event means a Network Security Event, a Privacy Event, an Interruption of Service, a System Failure Event, a Digital Asset Loss Event, and a Cyber Extortion Threat.

Cyber Extortion Threat means:

1. a credible threat or connected series of threats to cause a Privacy Event, Network Security Event, Digital Asset Loss Event, or the unauthorized disclosure of Digital Assets of the Company; or

2. a credible threat or connected series of threats to prevent, or an attack that prevents, access by the Insured to its Digital Assets;

made by someone other than a Control Group Member of a Company.

Cyber Terrorist Attack means a network-based attack against an Insured's Computer System by a person or group of people, known or unknown, for the purposes of influencing the government of any nation or political division thereof (whether such government is *de jure* or *de facto*), or in pursuit of political, religious, ideological, social, or economic objectives.

Damages means compensatory sums, monetary judgments or settlements, punitive, exemplary, or multiple damages, and pre-judgment and post-judgment interest, that the Insured is legally obligated to pay on account of a Claim.

Damages do not include:

1. amounts for which the Insureds are legally absolved from payment;

2. taxes, sanctions, fines, or penalties levied against the Insured, whether imposed by law or otherwise, except punitive or exemplary damages as described in this Definition;

3. the costs to comply with orders granting equitable relief, including, without limitation, injunctions, temporary restraining orders, specific performance, or any agreement to provide such relief;

4. the return, reduction, or restitution of fees, commissions, royalties, expenses, or costs, or the offset of any future fees to be charged by or owed to an Insured;

5. disgorgement of any profit, remuneration, or financial advantage to which the Insured was not legally entitled;

6. liquidated damages or penalties of any nature pursuant to a contract or agreement of any kind, except to the extent that the Insured would have been liable for such damages in the absence of such contract or agreement;

7. the Insured's cost of correcting, re-printing, or completing Media Material, including any media or products containing such Media Material, or correcting, re-performing, or completing Professional Services, Technology Services, or Media Communications;

8. future profits, future royalties, or costs of licensing; or

9. amounts uninsurable under the law pursuant to which this Policy is construed.

In determining the insurability of punitive, exemplary, or multiple damages, the law of an applicable jurisdiction most favorable to the insurability of such amounts shall apply, provided that such jurisdiction has a substantial relationship to the Insured, the Insurer, this Policy, or the Claim.

Digital Asset means software and data in electronic form stored on a Computer System.

Digital Asset Loss Event means the alteration, corruption, or destruction of Digital Assets stored on the Insured's Computer System resulting from a Network Security Event.

Digital Asset Replacement Expenses means reasonable and necessary costs and expenses incurred by the Company to restore or recollect Digital Assets from written records or partially or fully matching electronic data due to a Digital Asset Loss Event, including costs and expenses incurred in disaster recovery or computer forensic investigation efforts. If Digital Assets cannot be restored or recollected from written records or partially or fully matching electronic data, then Digital Asset Replacement Expenses shall be limited to the reasonable and necessary costs incurred to make that determination.

Digital Asset Replacement Expenses do not include:

1. any cost or expense incurred to update, replace, restore, or improve Digital Assets to a level beyond that which existed immediately prior to the Digital Asset Loss Event;

2. any cost or expense incurred to identify or remediate software program errors or vulnerabilities, or costs to update, replace, upgrade, restore, maintain, or improve any Computer System;

3. any cost or expense incurred to research or develop Digital Assets;

4. the economic or market value of Digital Assets, including trade secrets; or

5. other consequential loss or damages.

Direct Business Income Loss means Business Income Loss incurred by the Company as a result of an Interruption of Service caused solely and directly by a Network Security Event or System Failure Event impacting the Insured's Computer System.

Discovered means a Control Group Member of a Company becoming aware of a Claim or Cyber Event, as applicable.

Domestic Partner means any natural person recognized by federal, state, local, or foreign law, or by the Company, as a domestic partner or a party to a civil union.

Employee means a natural person other than an Executive whose labor or service an organization has the right to direct and control, including any employee, intern, or volunteer.

Executive means a director, officer, trustee, principal, partner, risk manager, in-house general counsel, or the functional equivalent of any of the foregoing in an organization.

Extortion Expenses means the reasonable and necessary expenses, other than Extortion Payments or Reward Payments, incurred by the Company with the prior consent of the Insurer, which shall not be unreasonably withheld, resulting directly from a Cyber Extortion Threat.

Extortion Payments means monies or digital currency paid by the Company with the prior consent of the Insurer, which shall not be unreasonably withheld, to a third party whom the Company reasonably believes to be responsible for a Cyber Extortion Threat, in order to terminate the Cyber Extortion Threat.

Extra Expenses means reasonable and necessary expenses incurred by the Company to minimize, avoid, or reduce an Interruption of Service or a Period of Restoration, including, without limitation, computer forensic investigation expenses, and forensic accounting expenses to determine the amount of Business Income Loss, but only to the extent that such expenses are over and above the Company's normal operating and payroll expenses.

Extra Expenses does not include:

1. any costs or expenses to prevent a future loss;

2. any costs or expenses to correct any deficiencies or problems with any Computer System that might cause or contribute to a Claim;

3. any costs or expenses to remediate software errors or vulnerabilities;

4. any costs or expenses to update, restore, or replace any Computer System, or improve any Computer System to a level beyond that which existed immediately before the Interruption of Service; or

5. any contractual penalties.

Insured means the Company and each Insured Person.

Insured Person means any natural person who was, now is, or will become:

1. an Executive or Employee of the Company in his or her capacity as such;

2. a leased employee of the Company but only while acting under the direct supervision and exclusively on behalf of the Company or an Executive or Employee of the Company;

3. an independent contractor of the Company but only in the performance of services on behalf of and at the direction of the Company or an Executive or Employee of the Company; and

4. solely for purposes of Insuring Agreements A., B., C., and D., an Additional Insured, but only for Wrongful Acts of an Insured other than an Additional Insured, or acts or omissions of an Insured other than an Additional Insured that give rise to a Cyber Event.

Insured's Computer System means a Computer System:

1. operated by, and either owned by or leased to, the Company; or

2. operated by an IT Service Provider for or on behalf of the Company;

in either case including the websites of the Company and the Media Material stored thereon; or

3. that is a wireless or mobile communication device owned by an Executive or Employee of the Company and that:

    a. is approved by the Company for use in the performance of the regularly assigned duties of such Executive or Employee; and

    b. complies with the Company's policy with respect to the use of such devices.

Interrelated means having as a common nexus any fact, circumstance, situation, event, transaction, or cause, or series of causally or logically connected facts, circumstances, situations, events, transactions, or causes.

Interruption of Service means the actual and measurable interruption, suspension, failure, degradation, or delay in the performance of:

1. with respect to Insuring Agreement F., the Insured's Computer System; and

2. with respect to Insuring Agreement G., a Computer System of a Qualified Service Provider.

IT Service Provider means a business that the Company does not own, operate, or control, but that the Company hires pursuant to a written contract to perform the following computer-related services for the Company:

1. maintaining, managing, or controlling the Insured's Computer System;

2. hosting or facilitating the Insured's internet website; or

3. providing network infrastructure, including, without limitation, cloud-based software applications, platforms, and storage.

IT Service Provider shall not include any provider of services as an internet service provider (including, without limitation, any provider of internet connectivity), any public utility (including, without limitation, a provider of electric, gas, water, or telecommunication services), or any securities exchange or market.

Loss means:

1. with respect to Insuring Agreements A., B., and C., only Damages and Claim Expenses;

2. with respect to Insuring Agreement D., only Damages, Claim Expenses, Consumer Redress Funds, Regulatory Fines and Penalties, and PCI Fines and Penalties;

3. with respect to Insuring Agreement E., only Breach Costs;

4. with respect to Insuring Agreement F., only Direct Business Income Loss and Extra Expenses;

5. with respect to Insuring Agreement G., only Contingent Business Income Loss and Extra Expenses;

6. with respect to Insuring Agreement H., only Digital Asset Replacement Expenses; and

7. with respect to Insuring Agreement I., only Extortion Payments, Extortion Expenses, and Reward Payments.

Malicious Code means unauthorized, corrupting, or harmful software code, including, without limitation, computer viruses, Trojan horses, keystroke loggers, spyware, adware, worms, and logic bombs.

Management Control means:

1. ownership of more than fifty percent (50%) of the ownership interests representing the voting, appointment, or designation power for the selection of the directors of a corporation, the management committee members of a joint venture or partnership, or the members of the board of managers of a limited liability company; or

2. possession of the right, pursuant to written contract, or the by-laws, charter, operating agreement, or similar document of an organization, to elect, appoint, or designate a majority of the board of directors of a corporation, the management committee members of a joint venture or partnership, or the members of the board of managers of a limited liability company.

Media Communications means the display, broadcast, dissemination, distribution, or release of Media Material, including, without limitation, the dissemination of Media Material over the internet.

Media Material means any data, text, sounds, graphics, images, or similar matter, including advertisements. Media Material does not include computer software, software technology, or products, goods, or services, including those depicted or described in the foregoing Media Material, or any name, image, or mark associated with, or intended to identify or distinguish, the Company or its products, goods, or services.

Media Wrongful Act means any act, error, omission, misstatement, misleading statement, misrepresentation, neglect, or breach of duty actually or allegedly committed or attempted by an Insured in connection with the rendering or failure to render Media Communications. Media Wrongful Acts include, but are not limited to:

1. Personal Injury Torts;

2. plagiarism, piracy, or the misappropriation, theft, or unauthorized use of ideas or information, advertising material, titles, literary or artistic formats, styles, performances, names, or likenesses;

3. the infringement of any copyright, domain name, trademark, trade name, trade dress, title, slogan, service mark, or service name;

4. improper deep linking or framing;

5. wrongful publication, product or service disparagement, or trade libel;

6. unfair competition or unfair trade practices, solely when alleged in connection with any of the foregoing; or

7. negligent or intentional infliction of emotional distress, outrage, or *prima facie* tort in connection with Media Communications.

Named Insured means the entity identified as such in the Declarations.

Network Security means measures taken to protect against Unauthorized Access or Use of, a denial of service attack directed against, or the transmission of Malicious Code to or from, a Computer System.

Network Security Event means an actual or suspected failure of the Network Security of the Company that results in or does not prevent:

1. the theft, alteration, or destruction of electronic data or software on the Insured's Computer System;

2. the Unauthorized Access or Use of the Insured's Computer System;

3. a denial of service attack against, or restriction or inhibition of access to, the Insured's Computer System;

4. the participation by the Insured's Computer System in a denial of service attack directed against a third party's Computer System; or

5. the transmission of Malicious Code to the Insured's Computer System, or from the Insured's Computer System to a third party's Computer System.

PCI Fines and Penalties means monetary amounts owed by, or assessments against, an Insured under the terms of a Payment Card Industry Merchant Services Agreement between a Company and a financial institution, credit or debit card company, credit or debit card processor, or independent service operator that enables a Company to accept credit cards, debit cards, or other payment cards for payments or donations, where such amounts directly result from a Privacy Event or a Network Security Event. PCI Fines and Penalties do not include chargebacks, interchange fees, discount fees, or other fees not related to a Privacy Event or Network Security Event.

Period of Restoration means the period from the date and time that a Computer System first suffers an Interruption of Service to the date and time such Computer System was restored, or could have been restored with reasonable diligence, to substantially the level of operation that had existed immediately prior to such Interruption of Service; provided that in no event shall such period exceed one hundred eighty (180) days.

Personal Information means:

1. an individual's name, social security number, medical or healthcare data, biometric data, driver's license number, state identification number, credit card number, debit card number, address, e-mail address, IP address, geolocation tag, telephone number, bank or other financial institution account number, account history, account password, or any other legally protected personal information, in any format; and

2. other nonpublic personal information, in any format, subject to protection under Privacy Regulations.

Personal Injury Tort means:

1. libel, slander, defamation, or other tort related to the disparagement of, or harm to the reputation or character of, any person or organization;

2. wrongful entry or eviction, trespass, or eavesdropping;

3. false arrest or false imprisonment;

4. malicious prosecution; or

5. invasion, infringement, or interference with the right to privacy, including false light, public disclosure of private facts, intrusion upon seclusion, or commercial appropriation of name or likeness.

Policy Period means the period designated as such in the Declarations, subject to prior termination in accordance with the terms of this Policy.

Pollutant means any solid, liquid, or gaseous irritant or contaminant, including, without limitation, smoke, vapors, soot, fumes, acids, alkalis, chemicals, odors, waste materials, infectious or medical waste, asbestos or asbestos-containing products, biological materials, organisms or viruses, and nuclear or radiological irritants or contaminants.

Privacy Event means an actual or suspected:

1. unauthorized disclosure, loss, or theft of:

   a. Personal Information for which the Insured is legally responsible that is in the care, custody, or control of any Insured or a third-party service provider; or

   b. other information of a third party that is not available to the general public, that the Insured is legally responsible to maintain the confidentiality of, and that is in the care, custody, or control of any Insured or a third-party service provider;

2. unauthorized collection of Personal Information; or

3. violation of any Privacy Regulation.

Privacy Regulation means the provisions of any federal, state, local, or foreign identity theft or privacy protection law or regulation that require commercial entities that collect Personal Information or other confidential information, to post privacy policies, adopt specific privacy or security controls, provide notice as to how Personal Information or other confidential information is used, or notify individuals in the event that Personal Information or other confidential information is compromised or is potentially compromised, and any amendments thereto, including, without limitation, the following:

1. the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act;

2. the Gramm-Leach-Bliley Act of 1999;

3. the California Security Breach Notification Act (CA SB 1386) and Massachusetts 201 CMR 17;

4. the California Consumer Privacy Act of 2018 (CA AB 375);

5. Identity Theft Red Flags under the Fair and Accurate Credit Transactions Act of 2003;

6. Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), but solely for alleged unfair or deceptive acts or practices in or affecting commerce; and

7. EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Professional Services means those services defined as Professional Services in the Declarations that are provided by an Insured to others.

Professional Services Wrongful Act means any act, error, omission, misstatement, misleading statement, neglect, breach of duty, or Personal Injury Tort actually or allegedly committed or attempted by an Insured in the performance of or failure to perform Professional Services.

Property Damage means:

1. physical injury to or destruction of any tangible property, or the loss of use thereof; or

2. loss of use of tangible property which has not been physically injured or destroyed;

provided that tangible property does not include electronic data or software.

Qualified Service Provider means a business the Company does not own, operate, or control, but that the Company hires pursuant to a written contract to perform services related to the conduct of the Company's business. Qualified Service Provider does not include an IT Service Provider.

Regulatory Fines and Penalties means any civil monetary fine or penalty imposed by a federal, state, local, or foreign governmental entity in such entity's administrative, regulatory, or other similar official capacity in connection with a Regulatory Proceeding. Regulatory Fines and Penalties do not include any criminal fines, disgorgement of profits, punitive, exemplary, or multiple damages, or civil monetary fines or penalties where such civil monetary fines or penalties are not insurable by law.

Regulatory Proceeding means:

1. a request for information or investigation of an Insured by a federal, state, local, or foreign governmental administrative or regulatory agency or body concerning a Privacy Event or Network Security Event; or

2. an administrative adjudicative proceeding against an Insured by a federal, state, local, or foreign governmental administrative or regulatory agency or body for a Privacy Event or Network Security Event, including an appeal thereof.

Related Entity means any organization:

1. in which any Company owns or controls fifteen percent (15%) or more of the issued and outstanding shares, units, or other portions of the equity of such organization;

2. that owns more than fifteen percent (15%) of the Named Insured; or

3. that is under common ownership or control with the Named Insured.

Retroactive Date means the applicable date set forth in the Declarations.

Reward Payment means any reward the Company pays to any person or entity for information leading to the arrest and conviction of any person who is making or has made any Cyber Extortion Threat, provided that the Company obtains the consent of the Insurer, which shall not be unreasonably withheld, prior to offering any such reward.

Subsidiary means an organization during the time that the Named Insured directly or indirectly has or had Management Control of such organization.

System Failure Event means any error or omission committed by the Insured or an IT Service Provider in the management of the Insured's Computer System that gives rise to an Interruption of Service.

Technology Products means computer or telecommunications hardware, software, firmware, or related electronic equipment, and the associated design, development, manufacturing, assembly, distribution, licensing, leasing, sale, installation, repair, or maintenance thereof.

Technology Services means any electronic or computer-based network services, including:

1. analysis, design, development, integration, installation, programming, conversion, service, Network Security, support, maintenance, repair, sale, or resale of computer systems, computer networks, computer software, computer hardware, input and output devices, storage devices or computer firmware, and related electronic systems;

2. database design and the collection, compilation, processing, warehousing, mining, storage, management, or analysis of electronic data;

3. provision of network infrastructure, including, without limitation, cloud-based software applications, platforms, and storage;

4. information technology consulting, management, education, or training;

5. Telecommunications Services; and

6. internet services, including, without limitation, the design, programming, hosting, management, or maintenance of websites and e-commerce platforms.

Technology Wrongful Act means any act, error, omission, misstatement, misleading statement, neglect, or breach of duty actually or allegedly committed or attempted by an Insured in connection with:

1. the Insured's performance of or the failure to perform Technology Services for others; or

2. the failure of the Insured's Technology Products to perform the function or serve the purpose for which they are intended;

including, without limitation, copyright infringement of software resulting from 1. or 2. above, but only if such infringement arises out of the Insured's performance of or failure to perform Technology Services, or software developed or created by the Insured.

Telecommunications Services means local, regional, and long distance wireline and wireless dial tone access and switching services, toll free services, voicemail, call forwarding, call waiting and caller ID; ground based satellite communication services; DSL, ISDN and VoIP services; video conferencing services;

paging services; basic wire maintenance; 911 emergency services; directory services and operator assistance; analysis, design, integration and conversion of telecommunications systems; directory publishing; or project management or consulting services related to any matter described in this Definition.

Unauthorized Access or Use means:

1. access to a Computer System by an unauthorized person or persons, or by an authorized person or persons in an unauthorized manner; or

2. use of a Computer System by an unauthorized person or persons, or by an authorized person or persons for a purpose that was not intended.

Waiting Hours Retention means the dollar amount of Business Income Loss and Extra Expenses incurred by the Company during the Waiting Period set forth in the Declarations.

Wrongful Act means:

1. with respect only to Insuring Agreement A., a Professional Services Wrongful Act;

2. with respect only to Insuring Agreement B., a Technology Wrongful Act; and

3. with respect only to Insuring Agreement C., a Media Wrongful Act.

IV. EXCLUSIONS

A. The following Exclusions apply to all Insuring Agreements:

1. Bodily Injury and Property Damage

The Insurer shall not be liable for Loss based upon, arising from, or attributable to any actual or alleged:

a. Bodily Injury; or

b. Property Damage;

except that Subparagraph a. of this Exclusion shall not apply to a Claim for a Technology Wrongful Act in the performance of or the failure to perform 911 emergency services.

2. Conduct

The Insurer shall not be liable for Loss based upon, arising from, or attributable to any actual or alleged dishonest, criminal, malicious, or fraudulent act, error, or omission, or any willful violation of any statute, rule, or law by any Insured; provided that this Exclusion shall not apply to Claims unless a final and non-appealable judgment or adjudication adverse to such Insured establishes such conduct, in which case the Insured shall reimburse the Insurer for any Claim Expenses paid by the Insurer prior to such judgment or adjudication. For purposes of determining the applicability of this Exclusion, the conduct of one Insured Person shall not be imputed to any other Insured

Person, and only the conduct of a Control Group Member of a Company shall be imputed to the Company.

3. Improper Profit

The Insurer shall not be liable for Loss based upon, arising from, or attributable to any Insured actually or allegedly gaining any profit, remuneration, or advantage to which such Insured was not legally entitled; except that this Exclusion shall not apply to Claims unless a final and non-appealable judgment or adjudication adverse to such Insured establishes that the Insured was not entitled to such profit, remuneration, or advantage, in which case the Insured shall reimburse the Insurer for any Claim Expenses paid by the Insurer prior to such judgment or adjudication. For purposes of determining the applicability of this Exclusion, the conduct of one Insured Person shall not be imputed to any other Insured Person, and only the conduct of a Control Group Member of a Company shall be imputed to the Company.

4. Infrastructure Failure and Physical Perils

The Insurer shall not be liable for Loss based upon, arising from, or attributable to any:

a. failure or malfunction of any securities exchange or financial market, or gas, water, electrical, telecommunications, internet, cable, or satellite service or utility, however caused, including without limitation, any electrical power interruption, short-circuit, surge, brownout, or blackout; or

b. fire, flood, volcanic eruption, tornado, explosion, lightning, wind, hail, tidal wave, landslide, solar storm, act of God, or other physical event;

except that Subparagraph a. of this Exclusion shall not apply to any such failure or malfunction if such exchange, market, service, or utility is under the operational control of the Insured.

5. Intellectual Property

The Insurer shall not be liable for Loss based upon, arising from, or attributable to any actual or alleged infringement, misappropriation, or violation of any intellectual property rights, including, without limitation, copyright, patent, trademark, service mark, trade name, trade dress, trade secret, or idea; except that this Exclusion shall not apply to:

a. a Claim for a Media Wrongful Act other than a Claim alleging infringement, misappropriation, or violation of intellectual property rights in patents or trade secrets;

b. a Claim for a Technology Wrongful Act arising from the infringement of any copyright relating to software; or

c. the disclosure, loss, or theft of a trade secret or idea resulting from a Privacy Event.

6. Prior Knowledge

The Insurer shall not be liable for Loss based upon, arising from, or attributable to a Wrongful Act or Cyber Event of which a Control Group Member of a Company had knowledge before the date set forth in the Declarations as the Continuity Date, and, solely with respect to Insuring

Agreements A., B., C., and D., that, as of the Continuity Date, such Control Group Member knew, or reasonably could have foreseen, that such Wrongful Act or Cyber Event could lead to a Claim.

7. Prior Notice

The Insurer shall not be liable for Loss based upon, arising from, or attributable to any fact, circumstance, or situation that was the subject of any notice given under any policy of insurance before the inception of the Policy Period.

8. Theft and Funds Transfer

The Insurer shall not be liable for Loss based upon, arising from, or attributable to:

a. loss, transfer, or theft of money, digital currencies or cryptocurrencies, or securities of the Insured, or of others in the care, custody, and control of the Insured; or

b. the monetary value of an electronic fund transfer or transaction by an Insured or on an Insured's behalf, which is lost or diminished during transfer into, out of, or between accounts.

9. Unlawful Collection of Personal Information

The Insurer shall not be liable for Loss based upon, arising from, or attributable to the actual or alleged unlawful collection of Personal Information by the Insured; except that this Exclusion shall apply to Insuring Agreements D. and E. only if a Control Group Member of a Company was aware of such unlawful collection of Personal Information.

10. War

The Insurer shall not be liable for Loss based upon, arising from, or attributable to war, including undeclared or civil war; warlike action by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign, or other authority using military personnel or other agents; or insurrection, rebellion, revolution, usurped power, or action taken by governmental authority in hindering or defending against any of these; except that this Exclusion shall not apply to a Cyber Terrorist Attack.

B. The following Exclusions apply to Insuring Agreements A., B., C., and D. only:

1. Claims by Affiliated Persons or Entities

The Insurer shall not be liable for Loss on account of any Claim brought by, on behalf of, or in the right of:

a. any Insured; or

b. any Related Entity;

except that Subparagraph a. of this Exclusion shall not apply to a Claim brought by an Additional Insured or a Claim by or on behalf of an Insured Person for a Privacy Event involving the Personal Information of such Insured Person.

2. Contractual Liability

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to breach of contract, warranty, guarantee, or promise, or any actual or alleged liability assumed by the Insured in any contract; except that this Exclusion shall not apply to:

a. liability of the Insured that would exist in the absence of such contract, warranty, guarantee, or promise;

b. liability assumed by the Insured under a written hold harmless or indemnity agreement regarding the content of Media Material used in Media Communications if such agreement exists before the Wrongful Act giving rise to such liability occurs;

c. liability of the Insured for PCI Fines and Penalties; or

d. breach of confidentiality of a third party arising from a Privacy Event.

3. Employee Benefits Law

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to any actual or alleged violation of the Employee Retirement Income Security Act of 1974, any amendments thereto, or any similar federal, state, local, or foreign statute or common law relating to an employee welfare or benefit plan established for the benefit of the Company or its employees; except that this Exclusion shall not apply to a Claim for a Privacy Event involving the Personal Information of an Insured Person.

4. Employment Practices and Discrimination

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to:

a. the employment or prospective employment of any person, or any employment practice, or any employment-related tort, including, without limitation, wrongful termination, dismissal or discharge, employment discrimination, employment-related harassment or defamation, or breach of employment contract, except that this Subparagraph shall not apply to a Claim for a Privacy Event involving the Personal Information of an Insured Person; or

b. any actual or alleged discrimination against any person or entity.

5. Fee Disputes

The Insurer shall not be liable for Loss on account of any Claim for any actual or alleged fees, expenses, or costs paid to or charged by the Insured.

6. Product Recall

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to the recall, repair, replacement, upgrade, supplement, or removal of any of the Insured's products, including products which incorporate the Insured's products or services, from the marketplace.

7. RICO

   The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to any actual or alleged violation of the Organized Crime Control Act of 1970 (commonly known as the Racketeer Influenced and Corrupt Organizations Act, or "RICO"), as amended, or any regulation promulgated thereunder, or any federal, state, or local law similar to the foregoing, whether such law is statutory, regulatory, or common law.

8. Securities Law

   The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to any actual or alleged violation of the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940, the Investment Advisers Act of 1940, any state blue sky securities law, each as amended, or any other federal, state, local, or foreign securities law, any rules or regulations promulgated thereunder, or any common law used to impose liability in connection with the purchase or sale or offer to purchase or sell securities.

9. Unfair Business Practices and Antitrust

   The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to any actual or alleged:

   a. false, deceptive, or unfair business practices, unfair trade practices, or unfair competition other than unfair trade practices or unfair competition as part of a Media Wrongful Act;

   b. violation of consumer protection laws; or

   c. price fixing, restraint of trade, monopolization, or any violation of the Federal Trade Commission Act, the Sherman Anti-Trust Act, the Clayton Act, each as amended, or any other federal, state, local, or foreign laws, regulations, or common law pertaining to antitrust, monopoly, price fixing, price discrimination, predatory pricing, or restraint of trade, or that otherwise protect competition;

   except that this Exclusion shall not apply to a Claim for a Privacy Event or a Network Security Event.

10. Unsolicited Communications

    The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to any actual or alleged unsolicited e-mail, unsolicited telephone calls, unsolicited text messages, or other unsolicited communication, distribution, publication, or transmission, including, without limitation, actual or alleged violations of the Telephone Consumer Protection Act of 1991, the U.S. CAN-SPAM Act of 2003, or any other federal state, local, or foreign law, any amendment thereto, any regulations promulgated thereunder, or violation of any order or ruling issued pursuant to any such law or regulation that regulates such communications; except that this Exclusion shall not apply to a Claim for a Network Security Event.

C. The following Exclusions apply to Insuring Agreements A., B., and C. only:

1. Actuarial Services

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to the performance of or the failure to perform actuarial services.

2. Bankruptcy or Cease and Desist Order

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to the insolvency, bankruptcy, receivership, or liquidation of any person or entity, any loss of license, or any cease and desist order.

3. Contests, Sweepstakes, and Lotteries

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to lotteries, sweepstakes, contests, or games of chance, or any misstatements or misrepresentations that appear in any promotional materials, including, without limitation, price discounts, gift cards, store debit or credit cards, prizes, awards, or other value given in connection with any lotteries, sweepstakes, contests, or games of chance.

4. False Advertising, Cost Guarantees, and Faulty Estimates

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to any actual or alleged:

a. inaccurate, inadequate, or incomplete description of the price of goods, products, or services;

b. cost guarantees, cost representations, or contract price estimates of probable costs, or cost estimates being exceeded;

c. failure of goods, products, or services to conform with any represented quality, performance, or authenticity contained in advertising; or

d. false or deceptive advertising or promotion, or deceptive trade practices in the sale of products, goods, or services.

5. Pollution

The Insurer shall not be liable for Loss on account of any Claim based upon, arising from, or attributable to the actual, alleged, or threatened discharge, release, escape, seepage, migration, or disposal of Pollutants, or any direction, request, demand, or order that the Insureds test for, monitor, clean up, remove, contain, treat, detoxify, or neutralize Pollutants, or any voluntary decision to do so.

6. Regulatory and Licensing Bodies

The Insurer shall not be liable for Loss on account of any Claim brought by or on behalf of:

a. any federal, state, local, or foreign regulatory agency or authority; or

b. the American Society of Composers, Authors and Publishers (ASCAP), Broadcast Music, Inc. (BMI), or Society of European Stage Authors and Composers (SESAC) or other intellectual property licensing or rights organization;

except that this Exclusion shall not apply to a Claim by any such agency, authority, or organization in its capacity as a customer or client of the Company.

D. The following Exclusion applies to Insuring Agreements E., F., G., H., and I. only:

Governmental Action

The Insurer shall not be liable for Loss based upon, arising from, or attributable to seizure, confiscation, expropriation, nationalization, or destruction of any Computer System or Digital Assets by order of any governmental authority.

V. LIMITS OF LIABILITY AND RETENTIONS

A. Limits of Liability

1. The Insurer's maximum aggregate liability for all Loss on account of all Claims and all Cyber Events under all Insuring Agreements combined is the Maximum Aggregate Limit of Liability set forth in the Declarations. If the Maximum Aggregate Limit of Liability is exhausted by the payment of Loss, then the Insurer's obligations with respect to the payment of Loss under this Policy shall be completely fulfilled and extinguished.

2. The Insurer's maximum liability for all Loss on account of each Claim under this Policy shall not exceed the applicable Each Claim Limit set forth in the Declarations.

3. The Insurer's maximum liability for all Loss on account of each Cyber Event under this Policy shall not exceed the applicable Each Cyber Event Limit set forth in the Declarations.

4. The Insurer's maximum liability for all Loss on account of all Claims and all Cyber Events under a particular Insuring Agreement of this Policy shall not exceed the applicable Insuring Agreement Aggregate Limit set forth in the Declarations.

5. The Each Claim Limit and Each Cyber Event Limit are each part of, and not in addition to, the applicable Insuring Agreement Aggregate Limit, which is part of, and not in addition to, the Maximum Aggregate Limit of Liability.

6. The Limits of Liability for any Extended Reporting Period shall be the remaining portion, if any, of the applicable Limits of Liability for the Policy Period. Such limits shall be part of, and not in addition to, the applicable Limits of Liability for the Policy Period. The purchase of the Extended Reporting Period shall not increase or reinstate any applicable Limit of Liability.

7. If a single Claim is subject to more than one Each Claim Limit, or a single Cyber Event is subject to more than one Each Cyber Event Limit, then the relevant Limits of Liability shall be applied separately to the different parts of such Claim or Cyber Event, but the Insurer's maximum aggregate liability for a single Claim or a single Cyber Event shall not exceed the largest applicable Each Claim Limit or Each Cyber Event Limit.

8. The Insurer's maximum liability for all PCI Fines and Penalties on account of all Claims shall not exceed the amount set forth in the Declarations as the PCI Fines and Penalties Limit, which is part of, and not in addition to, the Each Claim Limit and the Insuring Agreement Aggregate Limit for Insuring Agreement D.

9. The Insurer's maximum liability for all Reward Payments on account of all Cyber Extortion Threats shall not exceed the amount set forth in the Declarations as the Reward Payments Limit, which is part of, and not in addition to, the Each Cyber Event Limit and the Insuring Agreement Aggregate Limit for Insuring Agreement I.

B. Retentions

1. The Insurer's liability for Loss on account of each Claim or each Cyber Event other than an Interruption of Service shall apply only to that part of Loss that is excess of the applicable Retention amount set forth in the Declarations. Such Retention shall be borne by the Named Insured uninsured and at the risk of all Insureds, and shall be paid by the Insured as a condition precedent to payment of any Loss under this Policy.

2. The Insurer's liability for Loss on account of each Interruption of Service shall apply only to that part of Loss that is excess of the greater of either the Retention applicable to the relevant Insuring Agreement set forth in the Declarations or the applicable Waiting Hours Retention.

3. If multiple Retentions apply to a single Claim or Cyber Event, then each Retention shall apply separately to each part of the Claim or Cyber Event, but the total Retention shall not exceed the largest applicable Retention.

C. Related Claims and Cyber Events

The inclusion herein of more than one Insured with respect to any Claim or Cyber Event shall not operate to increase the Limits of Liability of this Policy.

Claims based upon, arising from, or attributable to Wrongful Acts that are Interrelated shall be treated as a single Claim. All such Claims shall be deemed first made when the earliest such Claim is made, whether before or during the Policy Period.

Cyber Events based upon, arising from, or attributable to Interrelated facts, circumstances, situations, or events shall be treated as a single Cyber Event. All such Cyber Events shall be deemed to have first occurred, or deemed to have been Discovered, as applicable, when the earliest such Cyber Event occurs or is Discovered, whether before or during the Policy Period.

With respect to Claims and Cyber Events based upon, arising from, or attributable to Interrelated facts, circumstances, situations, events, or Wrongful Acts:

1. all such Claims shall be deemed first made on the earlier of either the date that the first such Claim

is made or the date that the first such Cyber Event occurs or is Discovered, as applicable, whether before or during the Policy Period; and

2. all such Cyber Events shall be deemed to have first occurred, or deemed to have been Discovered, as applicable, on the earlier of either the date that the first such Cyber Event occurs or is Discovered, or the date that the first such Claim is made, whether before or during the Policy Period.

VI. DEFENSE, SETTLEMENT, AND COOPERATION

A. Defense and Settlement of Claims

The Insurer shall have the right and the duty to select defense counsel and defend any Claim, even if any of the allegations of the Claim are groundless, false, or fraudulent. The Insureds shall not incur Claim Expenses without the prior written consent of the Insurer, which shall not be unreasonably withheld. The Insurer's duty to defend any Claim shall cease upon exhaustion of the applicable Limits of Liability. In such event, the Insurer may tender control of the defense of such Claim to the Insured, and the Insured agrees, as a condition precedent to the coverage of such Claim under this Policy, to accept such tender.

The Insureds shall not settle or offer to settle any Claim, incur Claim Expenses, admit any liability, stipulate to any judgment, or otherwise assume any obligation with respect to any Claim without the prior written consent of the Insurer, which shall not be unreasonably withheld. The Insurer shall not be liable for Loss as a result of any offer to settle, settlement, assumed obligation, admission of liability, stipulated judgment, or Claim Expenses to which it has not consented. However, if the Insureds are able to fully and finally settle, with prejudice, all Claims subject to a single Retention for an aggregate amount, including Claim Expenses, that does not exceed such Retention, then the Insurer's consent is not required for such settlement.

The Insurer shall have the right to make any investigation it deems necessary and, with the written consent of the Insured, make any settlement of a Claim covered by this Policy. If the Insurer recommends settlement of a Claim, the claimant is willing to agree to such settlement, and the Insured refuses to give written consent to settlement as recommended by the Insurer, then the Insured thereafter shall negotiate or defend such Claim independently of the Insurer and on the Insured's own behalf. In such event, the Insurer's liability for any such Claim shall be limited to the amount of the proposed settlement, Claim Expenses incurred until the time that the Insured refused to settle the Claim, plus fifty percent (50%) of all Loss, including Claim Expenses, incurred over such amount.

B. Cooperation with Respect to Claims

The Insureds agree to provide the Insurer with all information, assistance, and cooperation that the Insurer reasonably requests with respect to any Claim, and agree that they will not knowingly take any action that will prejudice the Insurer's position or its potential or actual rights of recovery with respect to any Loss paid under this Policy. The Insureds shall forward to the Insurer every demand, pleading, notice, or other process received by or on behalf of the Insured in connection with any Claim.

C. Cooperation with Respect to Cyber Events

The Insureds shall cooperate with the Insurer, and shall provide any additional information reasonably requested by the Insurer in connection with a Cyber Event, including in investigating any Cyber Event, enforcing the legal rights the Insured or the Insurer may have against any party that may be liable to the Insured, and conducting a forensic accounting exercise to calculate Business Income Loss. The Insured agrees to take all reasonable steps and measures to limit or mitigate Business Income Loss, Digital Asset Replacement Expenses, and Loss on account of a Cyber Extortion Threat.

Except as otherwise provided in the Definition of Breach Costs, the Insured has the right to incur Breach Costs without the prior consent of the Insurer. However, the Insurer shall, at its sole and absolute discretion and in good faith, reimburse the Insured only for such Breach Costs that the Insurer deems to be reasonable and necessary.

VII. NOTICE AND PROOF OF LOSS

A. Notice of Claims

As a condition precedent to coverage under this Policy for any Claim, the Insured shall provide written notice to the Insurer of such Claim as soon as practicable after such Claim is Discovered, but in no event later than:

1. the end of the Policy Period with respect to a Claim first made against an Insured more than forty-five (45) days before the end of the Policy Period; or

2. sixty (60) days following the end of the Policy Period with respect to a Claim first made against an Insured less than forty-five (45) days before the end of the Policy Period; or

3. with respect to Claims first made during an Extended Reporting Period, if applicable, no later than the end of the Extended Reporting Period.

B. Notice of a Privacy Event or Network Security Event

As a condition precedent to coverage under this Policy for Breach Costs, the Insured shall provide written notice to the Insurer of the Privacy Event or Network Security Event giving rise to such Breach Costs as soon as practicable after such Privacy Event or Network Security Event is Discovered.

C. Notice of an Interruption of Service

As a condition precedent to coverage for Direct Business Income Loss or Contingent Business Income Loss and Extra Expenses, the Insured shall provide written notice to the Insurer of the Interruption of Service giving rise to such Direct Business Income Loss or Contingent Business Income Loss and Extra Expense, or the Network Security Event or System Failure Event giving rise to such Interruption of Service, as soon as practicable after such Interruption of Service, Network Security Event, or System Failure Event is Discovered.

D. Notice of a Digital Asset Loss Event

As a condition precedent to coverage for Digital Asset Replacement Expenses, the Insured shall provide written notice to the Insurer of the Digital Asset Loss Event giving rise to such Digital Asset Replacement Expenses as soon as practicable after such Digital Asset Loss Event is Discovered.

E. Notice of a Cyber Extortion Threat

As a condition precedent to coverage for Loss on account of a Cyber Extortion Threat, the Insured shall provide written notice to the Insurer of such Cyber Extortion Threat as soon as practicable after such Cyber Extortion Threat is Discovered.

F. Notice of a Circumstance or Wrongful Act

If during the Policy Period an Insured first becomes aware of a fact, circumstance, or Wrongful Act that may reasonably give rise to a Claim that would be covered under this Policy, and the Insured provides written notice of such fact, circumstance, or Wrongful Act to the Insurer during the Policy Period, then any Claim that may subsequently be made against an Insured arising out of such fact, circumstance, or Wrongful Act shall be deemed to have been first made during the Policy Period.

As a condition precedent to exercising its rights hereunder, the Insured shall include within any such notice a description of the fact, circumstance, or Wrongful Act that is the subject of the notice, the nature or extent of the injury or potential damages, the names of the potential claimants, the manner in which the Insured first became aware of such fact, circumstance, or Wrongful Act, and give the Insurer any such additional information and cooperation as it may reasonably request. Notice to the Insurer of a Cyber Event as described in Subsections A. through E. above shall constitute notice to the Insurer of a circumstance that could give rise to a Claim as set forth in this Subsection.

G. Breach Assist Hotline

If during the Policy Period a Cyber Event or suspected Cyber Event is Discovered by an Insured, then the Insured is strongly encouraged to call the Breach Assist Hotline set forth in the Declarations and the Notice attached to this Policy for immediate assistance. If the Insured provides notice to the Insurer through the Breach Assist Hotline of an actual or suspected Cyber Event then such notice shall be deemed notice of a fact, circumstance, or Wrongful Act that could give rise to a Claim as set forth in Subsection F. above.

If the Insured intends to make Extortion Payments in connection with a Cyber Extortion Threat, then the Insured, through the Breach Assist Hotline, can access specialized third-party technical resources to assist in minimizing any potential further compromise of the Insured's Computer System.

H. Proof of Loss for Cyber Events

With respect to Loss on account of a Cyber Event for which the Insured seeks payment under Insuring Agreements E., F., G., H., and I., the Insured shall provide the Insurer with a proof of loss with the full particulars of the calculation of any such Loss within one hundred eighty (180) days after such Cyber Event is Discovered. Such proof of loss shall include documents and other supporting evidence, including, without limitation, reports, books of accounts, bills, invoices, and any other documentation of payment of such Loss by an Insured. The Insurer shall have the right to audit such proof of loss and inspect the records of the Insured.

I. Address for Notices of Claims, Circumstances, and Cyber Events

Notices of Claims, Cyber Events, and circumstances or Wrongful Acts that could give rise to a Claim, and proofs of loss shall be provided to the Insurer at the applicable address set forth in the Declarations, except as set forth in Subsection F. above, in which case notice of a Cyber Event or suspected Cyber Event may also be provided through the Breach Assist Hotline.

VIII. CHANGES IN EXPOSURE

A. Change in Control of the Named Insured

If during the Policy Period:

1. the Named Insured merges or consolidates with another organization such that the Named Insured is not the surviving entity; or

2. another organization, person, or group of organizations or persons acting in concert, acquires:

   a. Management Control of the Named Insured; or

   b. all or substantially all of the assets of the Named Insured;

then coverage under this Policy will continue until termination of the Policy Period, but only with respect to Wrongful Acts or Cyber Events taking place before such merger, consolidation, or acquisition. This Policy may not be cancelled after the effective time of such merger, consolidation, or acquisition, and the entire premium for this Policy shall be deemed earned as of such time.

B. New Subsidiaries

If during the Policy Period the Company obtains Management Control of an organization, or acquires an organization by merger or consolidation, then such organization shall be deemed a Subsidiary and coverage under this Policy shall automatically apply to such new Subsidiary and its Insured Persons.

Notwithstanding the foregoing, if the total annual revenues of such organization exceed twenty percent (20%) of the total consolidated annual revenues of the Named Insured and the Subsidiaries for the twelve (12) months immediately preceding the inception of the Policy Period, then coverage for such organization and its Insured Persons shall not extend beyond sixty (60) days following creation or acquisition of such organization, unless the Named Insured provides the Insurer with written notice thereof, provides any additional information, agrees to any additional terms and conditions, and pays any additional premium reasonably required by the Insurer, and the Insurer has agreed in writing to insure such organization.

C. Former Subsidiaries

If before or during the Policy Period an organization ceases to be a Subsidiary, then coverage under this Policy for such former Subsidiary and its Insured Persons shall continue until termination of the Policy Period, but only with respect to Wrongful Acts or Cyber Events that take place before the time such organization ceased to be a Subsidiary.

D. In all events this Policy shall not provide coverage for any Subsidiary, or its Insured Persons in their

capacity as such, for Wrongful Acts or Cyber Events taking place before such organization qualifies as a Subsidiary or after such Subsidiary ceases to be a Subsidiary.

IX. REPRESENTATIONS AND SEVERABILITY OF THE APPLICATION

A. Representations

The Insureds represent and acknowledge that the statements, representations, and information contained in the Application are true and complete, and are deemed to be incorporated into and a part of this Policy as if physically attached hereto. This Policy has been issued in reliance on the truth and completeness of such statements, representations, and information.

B. Severability of the Application

In the event the Application contains any untrue or incomplete statement or any omission, and such statement or omission either was made with the intent to deceive or materially affected either the acceptance of the risk or the hazard assumed by the Insurer, then this Policy shall not provide coverage for any Claim or Cyber Event arising from the facts that were untrue or incomplete with respect to any Insured Person who had knowledge of the true facts, or any Company and its Subsidiaries if a Control Group Member of such Company had knowledge of the true facts, whether or not such Insured Person or Control Group Member knew the Application contained such untrue or incomplete statement or omission.

The Application shall be construed as a separate Application for coverage by each of the Insured Persons. For purposes of this Subsection, the knowledge of a Company or an Insured Person shall not be imputed to any other Insured Person.

C. Non-Rescindable Policy

The Insurer shall not have the right to void or rescind, in whole or in part, the coverage provided under this Policy.

X. POLICY TERMINATION

A. Cancellation

1. The Named Insured may cancel this Policy during the Policy Period by giving prior written notice to the Insurer stating when such cancellation shall take effect.

2. The Insurer may cancel this Policy:

   a. for nonpayment of premium, by providing notice of cancellation to the Named Insured at least ten (10) days before the effective time of cancellation; or

   b. for any reason permitted under applicable law other than nonpayment of premium, by providing notice of cancellation to the Named Insured at least ninety (90) days before the effective time of cancellation.

Notice of cancellation shall state the reason for cancellation and the effective date of cancellation.

3. In the event of cancellation by the Insurer or the Named Insured, the Insurer shall refund any unearned premium computed on a pro rata basis. The return or tender of a return premium is not a condition precedent to the cancellation becoming effective at the time specified in the cancellation notice.

B. Nonrenewal

If the Insurer elects not to renew this Policy, then the Insurer shall provide notice of nonrenewal to the Named Insured at least sixty (60) days before the expiration of the Policy Period. Such notice shall state the reason for nonrenewal. An offer by the Insurer of renewal terms, conditions, limits, or premiums different from those in effect prior to renewal shall not constitute a nonrenewal.

C. Notice of Termination

The Insurer shall mail or deliver notice of cancellation or nonrenewal in writing to the Named Insured and to the Named Insured's authorized agent or broker of record, if any. Proof of mailing will be sufficient proof of notice. Proof of delivery of the notice shall be treated the same as mailing.

XI. GENERAL CONDITIONS

A. Alteration and Assignment

No change or modification of the terms or any rights under this Policy, or any assignment of interest under this Policy, shall be effective except when made by written endorsement to this Policy issued by the Insurer.

B. Authorization

By acceptance of this Policy, the Insureds agree that the Named Insured shall act on behalf of all Insureds with respect to giving and receiving notices under this Policy, paying premiums, receiving any return premiums that may become due under this Policy, receiving and accepting any endorsements, cancellation, nonrenewal, or the negotiation of renewal of this Policy, agreeing to any changes to this Policy, and purchasing an optional Extended Reporting Period.

C. Bankruptcy

Bankruptcy or insolvency of any Insured or of the estate of any Insured shall neither relieve the Insurer of any of its obligations hereunder nor deprive the Insurer of its rights or defenses under this Policy.

D. Calculation of Business Interruption Loss

For purposes of determining Direct Business Income Loss and Contingent Business Income Loss, net profit or loss and expenses will be calculated on an hourly basis. In determining the amount of net profit or loss, the Insurer will give due consideration to the net profit or loss of the Insured before the Interruption of Service occurred and the probable net profit or loss of the Insured had no Interruption of Service occurred.

However, such net profit or loss calculations shall not include net income that would likely have been earned as a result of an increase in the volume of the Insured's business due to favorable business conditions caused by the impact of any event similar to a Network Security Event suffered by other

businesses. The Insured will provide the Insurer with access to all relevant sources of information for purposes of determining Direct Business Income Loss and Contingent Business Income Loss, including, without limitation, the Insured's financial records, tax returns, accounting procedures, bills, invoices and other vouchers, and deeds, liens, and contracts.

E. Form of Notices

Except as otherwise provided in this Policy, all notices under this Policy shall be in writing and delivered as follows:

1. notice to the Insureds shall be given to the Named Insured and sent by prepaid express courier or certified mail to the address set forth in the Declarations; and

2. notice to the Insurer shall be sent by prepaid express courier, certified mail, or e-mail, to the applicable address set forth in the Declarations.

Notice given as described above shall be deemed to be received and effective upon actual receipt by the addressee or one day following the date such notice is sent, whichever is earlier, subject to proof of transmittal.

F. Headings

The headings and subheadings in this Policy are solely for convenience and do not form part of the terms and conditions of coverage under this Policy.

G. No Action Against the Insurer

No action may be brought against the Insurer under this Policy unless, as a condition precedent to such action, the Insureds have complied fully with the terms of this Policy. Neither a claimant nor the Insureds or their legal representatives shall have any right under this Policy to join the Insurer as a party to any action against the Insureds to establish the Insureds' liability.

H. Other Insurance

If any Loss is insured under any other valid and collectible policy of insurance, then this Policy shall apply as excess over any such policy, including any deductible or retention of such policy, whether such other insurance is stated to be primary, contributory, excess, contingent, or otherwise, unless such other insurance is written only as specific excess insurance over the Limits of Liability provided in this Policy by reference to its policy number.

I. Subrogation

In the event of any payment under this Policy, the Insurer shall be subrogated to the extent of such payment to all of the Insureds' rights of recovery. The Insureds shall execute all papers required, and shall do everything reasonably necessary, to secure and preserve such rights and to enable the Insurer effectively to bring suit in the name of the Insureds.

If the Insurer recovers Loss paid under this Policy, then the Insurer shall reinstate the applicable Limits of Liability to the extent of any recovery, less any costs incurred by the Insurer in recovering such Loss. The Insurer shall have no duty to seek a recovery of Loss paid under this Policy.

J. Territory and Valuation

Coverage under this Policy shall apply anywhere in the world, to the extent legally permitted.

All premiums, limits, Retentions, Loss, and other monetary amounts of this Policy are expressed and payable in the currency of the United States of America. If a judgment is rendered, settlement is denominated, or another element of Loss under this Policy is payable in a currency other than United States of America dollars, then payment under this Policy shall be made in United States of America dollars at the rate of exchange published in The Wall Street Journal on the date the final judgment is reached, the amount of the settlement is agreed upon, or the element of Loss is due, respectively.

SOMPO INTERNATIONAL

Endurance Assurance Corporation
1221 Avenue Of the Americas
New York, NY 10020

IN WITNESS WHEREOF, the Insurer has caused this Policy to be signed by its President and Senior Vice President and countersigned where required by law on the Declarations page by its duly authorized representative.

Senior Vice President

President

POLICYHOLDER NOTICE

U. S. TREASURY DEPARTMENT'S OFFICE OF FOREIGN ASSETS CONTROL (OFAC)

No coverage is provided by this Policyholder Notice nor can it be construed to replace any provisions of your policy. You should read your policy and review your Declarations page for complete information on the coverages you are provided.

This Notice provides information concerning possible impact on your insurance coverage due to directives issued by OFAC. Please read this Notice carefully.

The Office of Foreign Assets Control (OFAC) administers and enforces sanctions policy, based on Presidential declarations of "national emergency". OFAC has identified and listed numerous:

- Foreign agents;
- Front organizations;
- Terrorists;
- Terrorist organizations; and
- Narcotics traffickers;

as "Specially Designated Nationals and Blocked Persons". This list can be located on the United States Treasury's website - http//www.treas.gov/ofac.

In accordance with OFAC regulations, if it is determined that you or any other insured, or any person or entity claiming the benefits of this insurance has violated U.S. sanctions law or is a Specially Designated National and Blocked Person, as identified by OFAC, this insurance will be considered a blocked or frozen contract and all provisions of this insurance are immediately subject to OFAC. When an insurance policy is considered to be such a blocked or frozen contract, no payments nor premium refunds may be made without authorization from OFAC. Other limitations on the premiums and payments also apply.

ENDORSEMENT

Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	September 11, 2023 12:01 AM Standard Time at the address of the **Named Insured** as shown in the Declarations.	Endorsement Number:	9

INCREASE EACH CLAIM AND INSURING AGREEMENT LIMIT OF LIABILITY - SPECIFIC LIABILITY INSURING AGREEMENT ENDORSEMENT

It is agreed that:

In consideration of an additional premium of [redacted]

I. The Each Claim Limit and the Insuring Agreement Aggregate Limit with respect to B., C., and D. set forth in Item 3. of the Declarations are replaced with the following:

A. Each Claim Limit:

1. $10,000,000 with respect to each **Claim** first made on or after 09/11/2023; and

2. $5,000,000 with respect to each **Claim** first made before 09/11/2023.

B. Insuring Agreement Aggregate Limit:

1. $10,000,000 with respect to **Claims** first made on or after 09/11/2023; and

2. $5,000,000 with respect to **Claims** first made before 09/11/2023;

provided that the most that the Insurer shall pay for all **Claims** under the applicable Insuring Agreement combined, is the Limit set forth in 1. above.

II. The **Retroactive Date** applicable to B., C., and D. set forth in Item 3. of the Declarations is replaced with the following:

Retroactive Date:

A. 08/27/2014 - Technology Services and Media Liability; Full Prior Acts - Privacy and Network Security Liability, with respect to the first $5,000,000 of the Each Claim Limit;

B. 09/11/2023, with respect to the limit of liability of $5,000,000 excess of the first $5,000,000 of the Each Claim Limit;

C. 08/27/2014 - Technology Services and Media Liability; Full Prior Acts - Privacy and Network Security Liability, with respect to the first $5,000,000 of the Insuring Agreement Aggregate Limit; and

D. 09/11/2023, with respect to the limit of liability of $5,000,000 excess of the first $5,000,000 of the Insuring Agreement Aggregate Limit.

III. Solely with respect to B., C., and D., the Continuity Date set forth in Item 7. of the Declarations is replaced with the following:

Item 7. Continuity Date:

A. August 27, 2023, with respect to the first $5,000,000 of the Each Claim Limit;

B. August 27, 2023, with respect to the limit of liability of $5,000,000 excess of the first $5,000,000 of the Each Claim Limit;

C. August 27, 2023, with respect to the first $5,000,000 of the Insuring Agreement Aggregate Limit; and

D. August 27, 2023, with respect to the limit of liability of $5,000,000 excess of the first $5,000,000 of the Insuring Agreement Aggregate Limit.

Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ENDORSEMENT

Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	September 11, 2023 12:01 AM Standard Time at the address of the **Named Insured** as shown in the Declarations.	Endorsement Number:	10

INCREASE EACH CYBER EVENT AND INSURING AGREEMENT LIMIT OF LIABILITY - SPECIFIC FIRST PARTY INSURING AGREEMENT ENDORSEMENT

It is agreed that:

In consideration of an additional premium of included:

I. The Each Cyber Event Limit and the Insuring Agreement Aggregate Limit with respect to E., F., G., H. and I. set forth in Item 3. of the Declarations are replaced with the following:

A. Each Cyber Event Limit:

1. $10,000,000 with respect to each **Cyber Event** that is first **Discovered**, first occurs, or is received, as applicable, on or after 09/11/2023; and

2. $5,000,000 with respect to each **Cyber Event** that is first **Discovered**, first occurs, or is received, as applicable, on or after 09/11/2023.

B. Insuring Agreement Aggregate Limit:

1. $10,000,000 with respect to **Cyber Events** that are first **Discovered**, first occur, or are received, as applicable, on or after 09/11/2023; and

2. $5,000,000 with respect to **Cyber Events** that are first **Discovered**, first occur, or are received, as applicable, before 09/11/2023;

provided that the most that the Insurer shall pay for all **Cyber Events** under the applicable Insuring Agreement combined, is the Limit set forth in 1. above.

II. Solely with respect to E., F., G., H. and I., the Continuity Date set forth in Item 7. of the Declarations is replaced with the following:

Item 7. Continuity Date:

A. August 27, 2023, with respect to the first $5,000,000 of the Each Cyber Event Limit; and

B. August 27, 2023, with respect to the limit of liability of $5,000,000 excess of the first $5,000,000 of the Each Cyber Event Limit.

C. August 27, 2023, with respect to the first $5,000,000 of the Insuring Agreement Aggregate Limit; and

D. August 27, 2023, with respect to the limit of liability of $5,000,000 excess of the first $5,000,000 of the Insuring Agreement Aggregate Limit.

Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ENDORSEMENT

Named Insured:	Carahsoft Technology Corporation	Policy Number:	NRO30043701400
Endorsement Effective Date:	September 11, 2023 12:01 AM Standard Time at the address of the **Named Insured** as shown in the Declarations.	Endorsement Number:	11

INCREASE MAXIMUM AGGREGATE LIMIT OF LIABILITY ENDORSEMENT

It is agreed that:

In consideration of an additional premium of included:

I. Item 6. Maximum Aggregate Limit of Liability of the Declarations is replaced with the following:

Item 6. Maximum Aggregate Limit of Liability:

A. $10,000,000 with respect to **Claims** first made, or **Cyber Events** that are first **Discovered**, first occur, or are received, as applicable, on or after September 11, 2023; and

B. $5,000,000 with respect to **Claims** first made, or **Cyber Events** that are first **Discovered**, first occur, or are received, as applicable, before September 11, 2023;

provided that the most that the Insurer shall pay for all **Claims** and **Cyber Events** combined under this Policy, is the Limit of Liability set forth in A. above.

II. The **Retroactive Date** set forth in Item 3. of the Declarations with respect to each Insuring Agreement is amended by the addition of the following:

Notwithstanding any **Retroactive Date** set forth in this Item 3., 09/11/2023 shall be the **Retroactive Date** with respect to the limit of liability of $5,000,000 excess of the first $5,000,000 of the Maximum Aggregate Limit of Liability.

III. Item 7. Continuity Date of the Declarations is replaced with the following:

Item 7. Continuity Date:

A. August 27, 2023, with respect to the first $5,000,000 of the Maximum Aggregate Limit of Liability; and

B. August 27, 2023, with respect to the limit of liability of $5,000,000 excess of the first $5,000,000 of the Maximum Aggregate Limit of Liability.

Authorized Representative

This endorsement does not change any other provision of the Policy. The title and any headings in this endorsement are solely for convenience and do not affect its meaning.

ACORD

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
08/15/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATIONIS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
AUTOMATIC DATA PROCESSING INS AGCY 76250717 71 HANOVER ROAD FLORHAM PARK NJ 07932	PHONE (A/C, No, Ext): (800) 524-7024	FAX (A/C, No):
	E-MAIL ADDRESS:	
	INSURER(S) AFFORDING COVERAGE	NAIC#
	INSURER A : Hartford Fire and Its P&C Affiliates	00914
INSURED	INSURER B :	
CARAHSOFT TECHNOLOGY CORP 11493 SUNSET HILLS RD STE 100 RESTON VA 20190-5230	INSURER C :	
	INSURER D :	
	INSURER E :	
	INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED.NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/Y YYY)	LIMITS	
	COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	
	CLAIMS-MADE / OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	
							MED EXP (Any one person)	
							PERSONAL & ADV INJURY	
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	
	POLICY / PRO-JECT / LOC						PRODUCTS - COMP/OP AGG	
	OTHER:							
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	
	ANY AUTO						BODILY INJURY (Per person)	
	ALL OWNED AUTOS / SCHEDULED AUTOS						BODILY INJURY (Per accident)	
	HIRED AUTOS / NON-OWNED AUTOS						PROPERTY DAMAGE (Per accident)	
	UMBRELLA LIAB / **EXCESS LIAB** — OCCUR / CLAIMS-MADE						EACH OCCURRENCE	
							AGGREGATE	
	DED / RETENTION $							
A	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY**						X PER STATUTE / OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? Y/N	N/ A		76 WEG ZJ6798	04/19/2023	04/19/2024	E.L. EACH ACCIDENT	$1,000,000
	(Mandatory in NH)						E.L. DISEASE -EA EMPLOYEE	$1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - POLICY LIMIT	$1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES **(ACORD 101, Additional Remarks Schedule, may be attached if more space is required)**

Those usual to the Insured's Operations. Reference: Contract#6508243.

CERTIFICATE HOLDER

Purchasing Agent
Metropolitan Government of Nashville
and Davidson County
Metro Courthouse
Nashville TN 37201

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Susan L. Castaneda

METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY
DEPARTMENT OF FINANCE – PROCUREMENT
SOLE SOURCE JUSTIFICATION FORM

DEPARTMENT of FINANCE
DIVISION OF PURCHASES

SS #: SS2022034

Date Received: Dec. 10, 2021

Send an email to PRG@nashville.gov and attach completed sole source form and supporting documentation.

Proposed supplier MUST be Registered in iProcurement

Date: 11/23/2021 Requesting Department/Agency/Commission: ITS Department

Requesting Official: Dawn Clark Telephone #: 615-862-6033 This is for a multi-year contract.

Product/Service Description: This is for Acquia hosting and security services for Nashville.gov as well as Salesforce licensing and support for HubNashville, MAC Hope, Metro Clerk's PRR, Finance PRR and HR Benefits CRM system and related products including TIBCO, Nintex, FormAssembly, OwnBackup, File Storage and Community Logins.

Total Purchase *(Enter the value for the entire contract life)* Price: $25,000,000

BU Number: 14521017 Fund #: 51137 Object Account: 505252 Any Other Accounting Info: _____

Proposed Supplier: Carahsoft Proposed Supplier Contact: James Franklin

Supplier Address: 11493 Sunset Hills Road City: Reston ST: VA Zip: 20190

Supplier Telephone #: 571.662.3454 Supplier Email: James.Franklin@Carahsoft.com

Metro Code: 4.12.060 *Sole Source Procurement*.
A contract may be awarded for a supply, service or construction item without competition when, under regulations promulgated by the standards board, the purchasing agent determines in writing that there is only one source for the required supply, service or construction item. The standards board may, by regulation, establish specific categories of supplies, services, or construction items as sole source items. (Ord. 92-210 § 1 (3-205), 1992)

R4.12.060.02 Conditions for Use of Sole Source Procurement.
Other, see explanation below

If Other, Explain Request: This is for a new consolidated Carahsoft sole source 10 year contract for Acquia hosting and security services for Nashville.gov as well as Salesforce licensing and support for HubNashville, MAC Hope, Metro Clerk's PRR, Finance PRR and HR Benefits CRM system and related products including TIBCO, Nintex, FormAssembly, OwnBackup, File Storage and Community Logins. HubNashville and the related systems developed and implemented within the Salesforce system have grown tremendously over the last several years and this is a critical series of modules/systems within Salesforce that are obtained through Carahsoft. Additionally, Nashville.gov went live being cloud hosted and secured through a WAF in Acquia which is also procured through Carahsoft. We are looking to leverage and obtain volume discounts on these critically proprietary implementations procured through Carahsoft.

Signatures will be gotten by Procurement in DocuSign

Department Requester's Initials: DC

Requesting Department Director's Signature of Approval: _____

Date: 12/10/2021 | 1:18 PM CST

SS #: SS2022034

Date Received: Dec. 10, 2021

To be completed by the Procurement Division

☐ **Vetting & Research Needed; Date Requested by Purchasing Agent**_____

☒ **Sole Source is Approved for:**_____

☐ **Sole Source is Denied (See determination summary for denial reason)**

PURCHASING AGENT: Michelle R. Hernandez Lane Date: 12/21/2021 | 11:43 P

Cantlon, Judy (Finance - Contract Compliance)

From: Clark, Dawn (ITS)
Sent: Friday, December 10, 2021 8:15 AM
To: Finance – Procurement Resource Group
Cc: Lane, Michelle (Finance - Procurement); Ferguson, Scott (Finance)
Subject: FW: Sole Source Request for Carahsoft
Attachments: Carahsoft Sole Source Contract 2021.xlsx; Sole Source Form for Carahsoft .docx

Importance: High

Just wanted to be sure this was in the queue to begin working on this new contract either from the State Contract (if able to negotiate as Michelle and I discussed) or if no changes can be made for that procurement route then a new sole source contract for 10 years.

Dawn Clark
Assistant Director
Business Applications Solutions and Support
Metropolitan Government of Nashville and Davidson County
Information Technology Services
Office: 615-862-6033
Fax: 615-862-6295

From: Clark, Dawn (ITS)
Sent: Tuesday, November 23, 2021 12:33 PM
To: Finance – Procurement Resource Group <PRG@nashville.gov>
Cc: Lane, Michelle (Finance - Procurement) <Michelle.Lane@nashville.gov>
Subject: Sole Source Request for Carahsoft
Importance: High

Attached is the sole source form for a new consolidated Carahsoft 10-year contract. Michelle and I discussed this a few weeks ago so just sending it through PRG to start this process. We also discussed potentially procuring this off the State contract if we had the ability to negotiate pricing and terms, but I wasn't sure what the answer was on that. Certainly, if that can be done and a sole source is not necessary for this new contract, then I'm ok with whatever the best procurement process is for this.

Just so you can get context on the amount and type of licenses, support and services included on this, I prepared a spreadsheet projecting all the known items and volumes out for 10 years with their current annual uplift of 7% (hoping with volume discount that will go down). Obviously, we don't know how much expansion/growth we will add over a 10-year period so I increased the maximum contract value to account for that.

Dawn Clark
Assistant Director
Business Applications Solutions and Support

DocuSign

Certificate Of Completion

Envelope Id: 1C7CFFD0C7BD4D739156E043631CBBF4 Status: Sent

Subject: URGENT! Metro Contract 6508243 w/ Carahsoft Technology Corporation (Information Technology Services)

Source Envelope:

Document Pages: 223 Signatures: 5 Envelope Originator:
Certificate Pages: 18 Initials: 0 Procurement Resource Group
AutoNav: Enabled 730 2nd Ave. South 1st Floor
EnvelopeId Stamping: Enabled Nashville, TN 37219
Time Zone: (UTC-06:00) Central Time (US & Canada) prg@nashville.gov
IP Address: 170.190.198.190

Record Tracking

Status: Original Holder: Procurement Resource Group Location: DocuSign
10/18/2023 10:56:03 AM prg@nashville.gov
Security Appliance Status: Connected Pool: StateLocal
Storage Appliance Status: Connected Pool: Metropolitan Government of Nashville and Davidson County Location: DocuSign

Signer Events	Signature	Timestamp
Michelle A. Hernandez Lane michelle.lane@nashville.gov Chief Procurement Officer/Purchasing Agent Metro Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.190	Sent: 10/18/2023 11:40:25 AM Viewed: 10/18/2023 4:27:04 PM Signed: 10/18/2023 4:27:50 PM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Kevin Crumbo/mjw MaryJo.Wiggins@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 160.129.251.199 Signed using mobile	Sent: 10/18/2023 4:27:57 PM Resent: 10/19/2023 8:32:12 AM Viewed: 10/19/2023 11:18:37 AM Signed: 10/19/2023 11:19:47 AM
Electronic Record and Signature Disclosure: Accepted: 10/19/2023 11:18:37 AM ID: 6469b48f-275e-4355-9d9b-62b1f140927e		
Tara Ladd tara.ladd@nashville.gov Assistant Metropolitan Attorney Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.144	Sent: 10/19/2023 11:19:52 AM Viewed: 10/19/2023 1:17:32 PM Signed: 10/19/2023 1:17:42 PM
Electronic Record and Signature Disclosure: Accepted: 10/19/2023 1:17:32 PM ID: 76ac45be-c22f-41a8-b809-82d535747ac0		
Procurement Resource Group prg@nashville.gov Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None)		Sent: 10/19/2023 1:17:56 PM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Terri L. Ray Terri.Ray@nashville.gov Finance Manager Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 10/18/2023 11:40:22 AM
Gary Clay Gary.Clay@nashville.gov Asst. Purchasing Agent Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 10/18/2023 11:40:22 AM Viewed: 10/18/2023 11:42:31 AM
Gregg Nicholson Gregg.Nicholson@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/18/2023 4:07:27 PM ID: c50c57d9-87ed-4769-a413-ce3530b6b7da	COPIED	Sent: 10/18/2023 11:40:23 AM Viewed: 10/18/2023 1:51:52 PM
Elizabeth Jefferson elizabeth.jefferson@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/19/2023 8:14:42 AM ID: aba42ae2-b32a-4d9b-9901-3dfc7747bf89	COPIED	Sent: 10/18/2023 11:40:24 AM Viewed: 10/18/2023 3:13:16 PM
Colby Bender colby.bender@carahsoft.com Contracts Team Lead Carahsoft Technology Corp. Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/7/2023 6:26:26 AM ID: 1404b30f-23c6-4d28-b285-9b7b14b766ea	COPIED	Sent: 10/18/2023 11:40:24 AM
Keith Durbin keith.durbin@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/11/2023 6:44:46 AM ID: a44c57e9-2a66-416e-b779-4e01327b7797	COPIED	Sent: 10/18/2023 4:27:56 PM Viewed: 10/19/2023 6:13:37 AM

Carbon Copy Events	Status	Timestamp
Balogun Cobb balogun.cobb@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/19/2023 9:04:06 AM ID: 47927e04-bbc1-4e48-829d-fc4f4a5c7842	COPIED	Sent: 10/19/2023 11:19:51 AM Viewed: 10/19/2023 11:49:09 AM
Sally Palmer sally.palmer@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/19/2023 8:31:41 AM ID: 564644b2-e8bd-4939-98fb-03e95f1255e2	COPIED	Sent: 10/19/2023 1:17:49 PM Viewed: 10/19/2023 1:18:51 PM
Tara Ladd tara.ladd@nashville.gov Assistant Metropolitan Attorney Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/19/2023 1:17:32 PM ID: 76ac45be-c22f-41a8-b809-82d535747ac0	COPIED	Sent: 10/19/2023 1:17:52 PM
Jeremy Frye jeremy.frye@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/4/2023 5:51:11 AM ID: e1f4a6a3-5818-48f1-922d-10504b0ccaf5		
Dawn Clark Dawn.Clark@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 9/15/2023 2:22:59 PM ID: 7ac1a22e-e062-4504-9444-46e1a64addcf		
Amber Gardner Amber.Gardner@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 9/5/2023 8:07:23 AM ID: e289baef-bb37-4563-b714-9962aed0c75a		
Kristina Smith contracts@carasoft.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Austin Kyle publicrecords@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/19/2023 12:35:06 PM ID: 74f07485-de40-4232-b0ce-8506072c2a40		

Carbon Copy Events	Status	Timestamp
Zak Kelley Zak.Kelley@Nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Leia Bolick leia.bolick@carahsoft.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Ed Buckles ed.buckles@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 6/9/2023 7:06:46 AM ID: b75d5752-cae7-4bab-92ca-69c70bbddf9f		
Michell Bosch Michell.Bosch@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/17/2023 3:41:16 PM ID: 545c2f9e-4478-48bf-bf32-e4eb1a953bc4		
Sharon Sepik Sharon.Sepik@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/17/2023 4:19:04 PM ID: 4f4c9cd8-f8de-4f5c-a55f-400b0ae9257e		
Randall Williams Randall.Williams@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 9/1/2022 7:23:06 AM ID: 53d0279b-09f8-4338-8210-c0db3d207559		
John Singleton John.Singleton@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 8/23/2023 6:58:19 PM ID: 84b02ef0-0d9b-4a9f-9597-3ba0b8a990ac		

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	10/18/2023 11:40:22 AM
Envelope Updated	Security Checked	10/19/2023 8:32:11 AM
Envelope Updated	Security Checked	10/19/2023 8:32:12 AM

Envelope Summary Events	Status	Timestamps
Envelope Updated	Security Checked	10/19/2023 8:32:12 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure