METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY
DEPARTMENT OF FINANCE – PROCUREMENT COOPERATIVE PURCHASING REQUEST FORM

CPR #: C2022004

Date Received: Aug. 5, 2021

Send an email to PRG@nashville.gov and attach completed form with supporting documentation.

Date Submitted: Originating Agency/Cooperative Entity: State of Tennessee

Vendor Name: Enterprise Rent A Car

Requesting Department: General Services - Fleet

Requesting Departmental Contact (Name & Number): Chuck Yancey 862-5096

Good(s) or Service(s) to be Procured: Vehicle Rentals

REQUESTOR SHALL COMPLETE STEPS 1 and 2 AND PROVIDE THE REQUIRED DOCUMENTATION:

STEP:	ATTACH COPIES:	CONFIRM THE FOLLOWING:
Step 1	☒ Executed Contract Contract Number SWC 205	☒ The contract contains a cooperative purchase provision allowing use by other government agencies. ☒ Valid from 5-20-2020 through 5-19-2023 ☒ I have reviewed the terms and conditions and take no exception.
Step 2	☒ Formal Solicitation (ITB or RFP)	☒ Solicitation was advertised, open and unrestricted
Step 3		☐ Consideration has been given to whether this purchase is in the best interest of the Metropolitan Government including the pricing terms of the contract.* ***Provide narrative details documenting the above confirmation.*** _____

Procurement will route in DocuSign for signatures

Department Requester: DocuSigned by: Charles Yancey DCC112E34819479...

Velvet Hunter

Signature of Requesting Department Head

8/6/2021 | 9:15 AM CDT

Date

CONTRACT

(fee-for-goods or services contract with an individual, business, non-profit, or governmental entity of another state)

Begin Date	End Date	Agency Tracking #	Edison Record ID
May 20, 2020	May 19, 2023		

Contractor Legal Entity Name	Edison Vendor ID
EAN Services, LLC	149982

Goods or Services Caption (one line only)

Vehicle Rental

Contractor	CFDA #
☒ Contractor	

Funding —

FY	State	Federal	Interdepartmental	Other	TOTAL Contract Amount
TOTAL:					

Contractor Ownership Characteristics:

☐ Minority Business Enterprise (MBE):

☐ African American ☐ Asian American ☐ Hispanic American ☐ Native American

☐ Woman Business Enterprise (WBE)

☐ Tennessee Service Disabled Veteran Enterprise (SDVBE)

☐ Disabled Owned Business (DSBE)

☐ Tennessee Small Business Enterprise (SBE): $10,000,000.00 averaged over a three (3) year period or employs no more than ninety-nine (99) employees.

☐ Government ☐ Non-Minority/Disadvantaged ☐ Other:

Selection Method & Process Summary (mark the correct response to confirm the associated summary)

☒ Competitive Selection	RFP 32110-19400 was issued.
☐ Other	Describe the selection process used and submit a Special Contract Request

Budget Officer Confirmation: There is a balance in the appropriation from which obligations hereunder are required to be paid that is not already encumbered to pay other obligations.

Speed Chart (optional)	Account Code (optional)

TN Department of General Services

SWC #205 Vehicle Rental
Contract Information and Usage Instructions

Contract Period: This is a five-year contract term running from May 20, 2020 to May 19, 2025 with the final two years each being an optional one-year renewal. The contract was procured through an RFP as Event #32110-19400.

Summary: this contract provides state agencies and local users the ability to rent passenger and commercial vehicles:

- Passenger Vehicles:
  - Compact Sedan
  - Intermediate/Mid-size sedan
  - Full-size sedan
  - Small/Mid-size SUV
  - Large SUV
  - Minivan
  - *12/15 Passenger Van (see requirements)
- Commercial Vehicles:
  - ½ Ton Pick-up Truck (tow-capable)
  - ¾ Ton Pick-up Truck (tow-capable)
  - 16' Box Truck with ramp or liftgate
  - 24'/26' Box Truck with liftgate
  - Cargo Van
  - 1 ton Pick-up truck (tow-capable)

Agencies can rent vehicles through the traditional Enterprise/National branches located throughout the United States and at all major airports, if acquiring a vehicle in Nashville, TN.

Insurance in the form of a Full Damage Waiver (DW), also known as a Loss Damage Waiver (LDW) or Collision Damage Waiver (CDW), is included in all rentals for *business-use*. The Contract vehicle rates include this insurance; thus, no additional information is required of the renter at the time of vehicle pick-up. Refer to Contract Section E.6 Insurance.

*Please note that Passenger Vans have an age restriction. No one under the age of 25 may rent these vehicles due to safety reasons and the high rate of rollover incidents.

Contract Administrator:
Laitin Beecham - Category Specialist
Central Procurement Office (615) 291-5794
Laitin.Beecham@tn.gov

VENDOR CONTACT INFORMATION:

EAN Services, LLC
Edison Contract Number: 65939
Vendor Number: 149982

Primary Contact: **Rasheen Hartwell**
Sales Director
615-309-9692 direct
Rasheen.C.Hartwell@ehi.com
284 Mallory Station Rd. Franklin, TN 37067

Secondary Contact: **Gerald Sims**
Business Rental Sales Support
615-371-9524 direct
Gerald.D.Sims@ehi.com
284 Mallory Station Rd. Franklin, TN 37067

Emergency Call Procedures:

If you are involved in an accident, theft, or incur any other damage to the vehicle during the rental, please follow the instructions on the guide inside your vehicle and report the incident to Enterprise immediately.

Usage Instructions:

Before making a vehicle reservation, you should be aware of your agency's policy regarding travel and the use of rental vehicles. You may also refer to the State's policy on travel for business (Department of Finance & Administration Policy 8 – Comprehensive Travel Regulations).

All reservations will be made on the State of Tennessee Enterprise site. State employees can access this site through VAM's website on the Intranet: https://www.teamtn.gov/vam/vehicle-rentals/enterprise.html

Local Government and other Authorized Users should contact the two Enterprise contacts (above) to utilize the contract.

For Personal Use: Employees should use the account code (XZ56TNP) in the Corporate Account Number or Promotion Code when starting a reservation.

HOW TO BOOK

LOCAL • AIRPORTS

ENTERPRISE RENT-A-CAR

For **official approved state business**, select **OFFICIAL STATE BUSINESS DIRECT BILL ONLY**

a) Select your Department
b) Enter city or airport in "Pickup Location"
c) Enter "Pickup" and "Return" dates and times
d) Optional: Enter "Last Name" and "Emerald Club Number"
    i) To obtain your membership information, contact the Enterprise representative listed above
    ii) If you have forgotten your membership information, click on the blue link "Forgot your info?" and follow the instructions
e) Click green "Start Reservation" button
f) Select your vehicle from the provided list of available vehicles
    i) Refer to Attachment A SWC 205 Vehicle Rental Pricing for the list of available vehicles under this Contract
    ii) Click green "Select" button under the selected vehicle
g) Unless instructed by your Agency, do not select any "Optional Items" that appear on the next screen. Click the green "Continue" button.
    i) Sales Tax will appear while making a reservation but will not be applied to any rentals that originate in Tennessee (rentals originating outside of Tennessee will have tax applied)
h) Review the reservation information on the next screen
    i) Provide your contact information in "Driver Information"
    ii) Provide your employment information in "Manager/Supervisor Authorizing Travel" and "Speed Chart" (if you do not know your speed chart number, contact your department's fiscal office)
    iii) NOTE: Your supervisor will receive confirmation of your reservation
    iv) Optional: Provide your flight information under "Frequent Traveler"
i) Click the green "Reserve" button
j) The next screen will display the reservation information
    i) Make note of your rental confirmation number
    ii) You can print this page or refer to the confirmation email

Verify, Review and Evaluate Information Systems Continuity (12.1.3)

All State agencies and vendors or contractors who operate on behalf of the State should verify the established and implemented information systems continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Redundancies (12.2)

Objective: To ensure availability of information processing facilities.

Availability of Information Processing Facilities (12.2.1)

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

MINIMUM COMPLIANCE REQUIREMENTS

Verify, Review and Evaluate Information Systems Continuity (12.1.3)

- BIAs should be performed within every 365 days.
- A sample of critical applications should be tested within every 365 days as part of a scheduled disaster recovery exercise, as a tabletop or prior to go live exercise.

CONTRACT
BETWEEN THE STATE OF TENNESSEE,
DEPARTMENT OF GENERAL SERVICES
AND
EAN Services, LLC

This Contract, by and between the State of Tennessee, Department of General Services ("State") and EAN Services, LLC ("Contractor"), is for the provision of Short –Term and Long-Term Vehicle Rental Services, as further defined in the "SCOPE." State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is a Limited Liability Company.
Contractor Place of Incorporation or Organization: Delaware
Contractor Edison Registration ID # 149982

A. SCOPE:

A.1. State understands that Contractor intends to, and shall have the right to, delegate the performance of certain of its obligations and duties under this Contract (including, without limitation, all obligations and duties relating to the rental of vehicles) to one or more affiliates of Contractor (each, an "Affiliate" and collectively, the "Affiliates") and to make available to State a network of independently owned franchisees and licensees (collectively "Franchisees") operating Enterprise Rent-A-Car and National Car Rental brand vehicle rental locations from which State may rent vehicles at the rates provided herein in locations where Contractor itself does not operate. This Contract shall only apply to and cover vehicle rentals to Authorized Users from car rental facilities located in Contractor's North America locations set forth in Attachment B and which are operated the "Enterprise" and "National" brand names, including truck rentals operated by Enterprise Truck Rental. This Contract shall not apply to rentals in any other jurisdictions, to rentals by another brand not identified under the particular Schedule, to any rentals under the "Alamo Rent A Car" brand. Unless as may otherwise be specifically stated in this Contract, this Contract shall not apply to any program or rentals by Contractor or an Affiliate to an Eligible Renter under EnterpriseCarClub, Rideshare by Enterprise or Enterprise Vanpool or such other similar brand names or programs providing similar services as are provided under such brands. Franchisees are not parties to this Agreement, but Contractor shall ensure that each Franchisee will make vehicles available to eligible renters as described herein, and that Franchisees will honor the applicable rates (as well as Damage Waiver and Liability Protection to the extent included in the rate) as set forth in this Contract and the applicable Schedule(s) for each location where the respective Franchisees operate.

A.2. The Contractor shall provide all goods or services and deliverables as required, described, and detailed below and shall meet all service and delivery timelines as specified by this Contract.

A.3. Definitions. For purposes of this Contract, definitions shall be as follows and as set forth in the Contract:

Long-Term Vehicle Rental	Vehicle rented at least 30 days but no more than 6 months. Only available under Group 1 and Group 2 Vehicle Rental portion of the Contract.
Short-Term Vehicle Rental	Vehicle rented 29 days or less.
Authorized User	See section E.10.

A.4. Vehicle Groups.

a. Group 1 Vehicle Rental, Passenger Vehicles – this program will include only passenger vehicle rentals with unlimited miles available for daily, weekly, or monthly rental either through the Contractor's physical locations, airports, or pick-up.

(1) Weekly rates shall be based on 5.5 calendar days.
(2) Monthly rates shall be based on 23.9 calendar days.

b. Group 2 Vehicle Rental, Commercial Vehicles – this program will include only commercial vehicle rentals with unlimited miles available for daily, weekly, or monthly rental either through the Contractor's physical locations, airports, or pick-up.

(1) Weekly rates shall be based on 5.5 calendar days.
(2) Monthly rates shall be based on 23.9 calendar days.

c. Group 3 State Lot – The Contractor must provide vehicles in a State lot located in Nashville, TN.

(1) The State lot will be for State Employee use only, and public access to this lot will not be allowed.
(2) The State will only pay for the lot vehicles as they are used; for example, if a vehicle sits on the lot for 5 days but is only used for 2 days during that timeframe, the State will only pay for the 2 days of use.
(3) The State will provide Fuel Cards in State lot vehicles.
(4) A maximum of thirty-five (35) spaces will be made available in the State lot for use by the Contractor. These spaces will be provided at no cost to the Contractor.
(5) Contractor will furnish the State with sufficient quantities of forms, brochures and materials as Contractor may from time to time, in consultation with the State, determine to be necessary or appropriate for the adequate promotion of the State Lot.
(6) Contractor will provide to the State the instructions and procedures to be followed by the State in the rental of Vehicles as part of the Enterprise CarShare Program.
(7) Contractor will from time to time provide instruction and training to the State on how to register for the program, and reserve, use and process rentals under the program.
(8) Contractor will perform all regular and necessary inspections, maintenance and upkeep (including periodic exterior and interior cleaning) of the Group 3 State Lot vehicles and arrange for the maintenance or repair of any damaged vehicle(s).

A.5. Vehicle Specifications

The State requires that the following vehicles be made available within and outside the State of Tennessee to Authorized Users:

a. Passenger Vehicle Classes - Any type of vehicle used for carrying or transporting passengers
(1) Compact Sedan
(2) Intermediate/Mid-Size Sedan
(3) Full-Size Sedan
(4) Small/Mid-Size Sport Utility Vehicle
(5) Large Sport Utility Vehicle
(6) Minivan
(7) Passenger Van (15 passengers)

b. Commercial Vehicles Classes - Any type of vehicle used for carrying or transporting goods
(1) Pick-Up Truck – ½ ton
(2) Pick-Up Truck – ¾ ton
(3) Box Truck – 16 feet with Ramp
(4) Box Truck – 16 feet with Lift Gate
(5) Box Truck – 24 feet with Lift Gate
(6) Cargo Van

i. The Pick-Up Truck – ½ ton and the Pick-Up Truck – ¾ ton in the Commercial Vehicle Classes must come with a towing package.

c. No rentals of any vehicle class not listed in Contract Attachment B hereto (including, but not limited to, exotics, high line vehicles and commercial trucks not listed in Section A.5.b) shall be permitted under this Contract.

d. Group 3 State lot vehicles consist of those passenger vehicle classes listed in Section A.5.a.(1) – Section A.5.a.(6).

e. All Group 1 and Group 2 vehicles must have at least one quarter (1/4) tank of fuel upon pick-up by Authorized Users.

f. All vehicles must be equipped with at least the following features: Bluetooth sync, automatic transmission, power steering, power brakes, anti-lock brake systems, power windows, power door locks, air conditioning, AM/FM radio and all appropriate safety driver and passenger equipment, including but not limited to, air bags and all other manufacturer standard features/options included on the proposed model.

g. Vehicle Model Year

(1) Passenger vehicles must be either the current or previous model year in production (calculated from current calendar year).
(2) Commercial vehicles must be no older than five (5) years old (calculated from current calendar year).

h. All vehicles must be maintained according to the manufacturer maintenance schedule.

i. Upon pick-up by the Authorized User, the interior and exterior of the vehicle must be clean for Group 1 and Group 2 vehicles.

j. The Contractor will be responsible for organizing a maintenance and cleaning schedule for the vehicles in the State lot for Group 3. The maintenance and cleaning schedule must be shared with and approved by the State. The maintenance schedule shall consist of industry standard vehicle maintenance plans such as checking and replacing damaged windshields, oil changes, and tire rotations. State lot vehicles must be thoroughly cleaned at least once a month. The Contractor must establish a reporting system or provide a contact so that Authorized Users can report if a vehicle needs to be serviced or cleaned.

A.6. Users/Eligible Renters

a. The Contractor must provide vehicle rental services to all eligible and approved Authorized Users that hold a valid State-issued driver's license and are at least eighteen (18) years old, or at least twenty-five (25) years old for passenger vans, at the reservation start time, within and outside the State of Tennessee. For all eligible and approved drivers age eighteen (18) and over, the Contractor must not impose any additional fees. Eligible renters must meet any other qualifications in the jurisdiction in which the specific vehicle rental originates.

b. All eligible and approved Authorized Users that meet the license and age requirements detailed in Section A.6.a. can operate any vehicle rented by another eligible and approved Authorized User. There will not be a charge by the Contractor for these additional drivers.

c. The Contractor must provide, at no cost to the State, its preferred customer and/or reward program.

d. The Authorized User will be responsible for paying any and all traffic violations when the rental vehicle is in his or her possession. Contractor(s) must send notice of tickets to each Authorized User for payment by the rental driver. The State assumes no responsibility for the payment of any tickets received by the driver.

e. The Authorized User will be responsible for immediate reporting to the Contractor of any accident, property damage, or personal injury involving or associated with any vehicles or the theft of any vehicle.

A.7. Reservation and Pick-up/Return Policy

a. The Contractor must maintain rental facilities throughout the State of Tennessee and nationally to service Authorized Users outside the borders of the State. The Contractor must be able to provide service to all counties across the State. The Contractor must make available to the State a secure online reservation system that will be available for use 24 hours a day, 365 days a year (including weekends and holidays). The online reservation system must provide users a reservation confirmation and a summary of the vehicle reservation including date(s), location(s), vehicle class, and rental rates using the contracted rates.

b. Reservation Notification Process – the Contractor will create and implement upon State approval a process in which the State will be notified of reservations made by Authorized Users.

c. All Authorized Users must provide the proper documentation (e.g. State Employee ID, Driver's License, etc.) at the time of vehicle pick-up. The Contractor may turn away any Authorized User who is not able to provide this documentation. If this documentation is not provided and a rental is denied, the Authorized User will not be charged for the vehicle.

d. After-hours and weekend vehicle returns must be made available to all Authorized Users.

e. In the event an Authorized User has reserved a vehicle that has become over-sold, the Contractor must provide an upgraded vehicle that is mutually acceptable to the Authorized User and the Contractor. The Contractor will provide the mutually agreed upon upgraded vehicle at the same rate as the originally reserved vehicle.

f. The Contractor will provide a 59-minute grace period for rental returns.

g. The Contractor must provide secure on-site parking, or off-site with delivery and pick-up, options for user's personal vehicles at no additional charge during the entire rental period at off-airport locations (does not include airports and the State lot). If the Contractor does not offer on-site parking, the Contractor agrees to pick up State employees within a five (05) mile radius from the rental location for Group 1 and Group 2 rental types.

h. Reservations must be made at least four (4) hours in advance of reservation start time.

i. Eligible renters must use the Account Number(s) assigned by Contractor to State (XZ56801 for National and Enterprise brand business use rentals XZ56TNP when making the reservation for the rental. Except as otherwise stated herein, all rentals under this Contract shall be made through a booking channel or channels approved by Contractor or its designee in writing. Under no circumstances shall Contractor its Affiliates or Franchisees be responsible for paying any fees or charges to State or an Authorized User or any other third party in order to connect to such approved booking tool or for any channel to be used by State or an Authorized User. In the event an eligible renter does not use the applicable Account Number or approved booking channel as set forth herein for a rental, the terms and conditions of this Contract shall not apply to such rental. "Business use" means rentals under any Rental Contract which are paid, in whole or in part, by State or its affiliates for which the eligible renter is reimbursed, in whole or in part, by State or its affiliates.

A.8. Roadside Assistance and Emergency Response

The Contractor must provide 24-hour/365-day emergency roadside assistance on all vehicles available under this Contract. Upon vehicle pick-up, the Contractor must provide the user with a verbal and written 24-hour local or toll-free number to be used for any emergencies requiring roadside assistance.

A.9. Implementation Plan

a. The Contractor is responsible for the transition between the State's current contract for Vehicle Rental and the new contract according to the timeline proposed. The Implementation Plan is the transition process where the selected Contractor will provide instruction, service, support and maintenance to ensure proper utilization and functioning of the new Contractor system. The Contractor will be responsible for reporting progress on the Implementation Plan every two (2) weeks until the agreed upon go-live date is reached.

b. The Contractor Implementation Plan submitted in response to RFP #32110-19400 will be inserted as Attachment C.

A.10. Fuel

a. Vehicle Groups 1 and 2: If an Authorized User fails to fill the gas tank up to the same level that was present at rental pick up, the Contractor may charge in accordance with Section C.11.h. to return the gas tank to the level present at rental pickup.

b. Vehicle Group 3: The State is responsible for fueling vehicles in Vehicle Group 3.

A.11. Long Term Vehicle Rental

a. The Contractor must allow for long term vehicle rentals at the payment rates provided in Section C. Long- term vehicle rentals will last at least one (1) month but no longer than six (6) months.

b. For rentals lasting longer than thirty (30) days, Authorized Users shall contact the rental location every thirty (30) days to report the miles that have been driven. The State shall inform Authorized Users of their mileage reporting responsibility.

A.12. Reporting

a. Statewide Contract Reports: All reports shall be submitted electronically in Microsoft Excel format. Reports shall include the ability to sort or summarize data in accordance with the Contract Administrator's specifications. All reports shall be provided at no additional cost to the State.

b. Quarterly Reports: Contractor will submit quarterly reports to the Contract Administrator no later than ten (10) days after the end of the State's quarter (e.g. a fiscal year quarter 2 report for October - December is due no later than January 10th). At the Contract Administrator's sole discretion, the State may extend the time allowed to complete quarterly reports. Quarterly reports shall provide statistical data on all transactions under this Contract by Authorized Users. At minimum, the quarterly report's statistical data shall be detailed and broken down by line item to include:

i. Rental Reservation Start Date and Time
ii. Rental Reservation End Date and Time
iii. Rental Actual Start Date and Time
iv. Rental Actual End Date and Time
v. Rental Pick-Up Location
vi. Rental Drop-Off Location
vii. Vehicle Reserved
viii. Vehicle Driven

ix. Reserving User's Name
x. Reserving User's Agency and Location
xi. Vehicle Rental Rate
xii. Fees Charged
xiii. Explanation of Fees
xiv. Total Invoice Amount
xv. Total Miles Driven

c. Custom Reports: When requested by the State, the Contractor shall submit custom reports to the Contract Administrator within thirty (30) days of the request.

d. Reports shall be provided in electronic format. All electronic reports must be submitted in Microsoft Excel format. Reports must include the ability to sort/summarize by account, item number, Category, Equipment Category. Contractor agrees to provide all data requested in a flat file format as designated by the State Contract Administrator.

A.13. Green Vehicles.

The State is committed to providing state employees with energy-efficient and alternative fuel motor vehicles. At least twenty-five percent (25%) of vehicles procured by the State (including rentals) in designated nonattainment areas shall be energy-efficient and/or alternative fuel motor vehicles. The Contractor must work with the State to provide these types of vehicles, for example compact fuel-efficient vehicles with a mileage rating of at least twenty-five (25) miles per gallon.

A. 14. Leisure.

a. Authorized Users shall have the ability to rent Group 1 and Group 2 vehicles at the rates set forth in Contract Attachment B for leisure (non-business) use. Group 3 vehicles shall not be available for leisure rentals. For rentals to Authorized Users for leisure use, the Authorized User shall be responsible for damage to or loss of the vehicle in accordance with the terms and conditions of the applicable Rental Contract. For leisure use rentals, Authorized Users can elect to purchase optional damage waiver.

b. For rentals to Authorized Users for leisure use, the Authorized User shall be responsible pursuant to the terms and conditions of the applicable Rental Contract for all third-party claims for property damage, bodily injury or death resulting from the use or operation of any vehicle. Authorized Users can elect to purchase optional supplemental liability protection. Liability protection is not included in the leisure use rates provided in Contract Attachment B. Liability protection for third party claims, if purchased, will be upon the terms and subject to the limitations set forth in the applicable Rental Contract and insurance policy.

A.15. Rental Agreement.

For each vehicle rented under this Contract, the eligible renter must execute the then-standard rental agreement of the applicable Contractor Affiliate or Franchisee at the rental facility at which the vehicle rental occurs (or, for National brand rentals only, the National Emerald Club Agreement) (each, regardless of brand, a "Rental Contract"). In the event of a direct conflict between the terms of this Contract and the terms of any Rental Contract, the terms of this Contract will govern.

A.16. Warranty.

Contractor represents and warrants that the term of the warranty ("Warranty Period") shall be the greater of the Term of this Contract or any other warranty generally offered by Contractor, its suppliers, or manufacturers to customers of its goods or services. The goods or services provided under this Contract shall conform to the terms and conditions of this Contract throughout the Warranty Period. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge.

Contractor represents and warrants that the State is authorized to possess and use all equipment, materials, software, and deliverables provided under this Contract.

Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Contractor's industry.

If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services. Any exercise of the State's rights under this Section shall not prejudice the State's rights to seek any other remedies available under this Contract or applicable law.

A.17. Inspection and Acceptance. The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

A.18. Rentals originating in the United States shall not be driven to Mexico or Canada.

B. TERM OF CONTRACT:

B.1 This Contract shall be effective on May 20, 2020 ("Effective Date") and extend for a period of thirty-six (36) months after the Effective Date ("Term"). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

B.2. Renewal Options. This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to two (2) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.

B.3. Term Extension. The State may extend the Term an additional period of time, not to exceed one hundred-eighty (180) days beyond the expiration date of this Contract, under the same terms and conditions, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.

C. PAYMENT TERMS AND CONDITIONS:

C.1. Estimated Liability. The total purchases of any goods or services under the Contract are not known. The State estimates the purchases during the Term shall be eight million dollars ($8,000,000.00) ("Estimated Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.

C.2. Price Changes. Prices listed in awarded published catalog, price lists or price schedule shall remain firm for three hundred sixty-five (365) days ("Firm Price Period").

a. Price Decreases. After the Firm Price Period, prices shall be equitably adjusted to reflect a decrease in Contractor's costs.

b. Price Increases. After the Firm Price Period, Contractor may request price increases. The request shall: include copies of the new price lists or catalog that reflect a change in the Contractor's cost; not constitute an increase in profit; and apply to all of the Contractor's customers.

c. Approval of Price Changes. The State may at its sole option: (1) grant the Contractor's request; (2) cancel the Contract and award it to the next apparent best evaluated Respondent; (3) cancel the Contract and reissue the solicitation; or (4) deny the Contractor's request. If approved, any price changes of less than seven percent (7%) will become effective upon the State's approval in writing. Price changes exceeding seven percent (7%) shall require a Contract amendment. The Contractor shall honor all purchase orders dated prior to the approved price change. Upon request from the State, the Contractor shall furnish the approved catalog, price schedule or price list as applicable to the State at no charge.

C.3. Payment Methodology. The Contractor shall be compensated based on the payment rates for goods or services contained in Contract Attachment B and as authorized by the State. The Contractor's compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.

C.4. Travel Compensation. The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.

C.5. Invoice Requirements. The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3., above. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than thirty (30) days after goods or services have been provided to the following address:

State Agency Billing Address as defined on the Purchase Order

a. Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):

(1) Invoice number (assigned by the Contractor);
(2) Invoice date;
(3) Contract number (assigned by the State);
(4) Customer account name: State Agency & Division Name;
(5) Customer account number (assigned by the Contractor to the above-referenced Customer);
(6) Contractor name;
(7) Contractor Tennessee Edison registration ID number;
(8) Contractor contact for invoice questions (name, phone, or email);
(9) Contractor remittance address;
(10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
(11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
(12) Applicable payment methodology (as stipulated in Section C.3.) of each good or service invoiced;
(13) Amount due for each compensable unit of good or service; and
(14) Total amount due for the invoice period.

b. Contractor's invoices shall:

(1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;
(2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;

(3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and
(4) Include shipping or delivery charges only as authorized in this Contract.

c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.

C.6. Payment of Invoice. A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.

C.7. Invoice Reductions. The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.

C.8. Deductions. The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.

C.9. Prerequisite Documentation. The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation.

a. The Contractor shall complete, sign, and present to the State the "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by ACH; and

b. The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

C.10. Rebate.

Contractor shall pay to the State a rebate on all rentals by Authorized Users ("Rebated Rentals") from the Contractor under the terms of this Contract based on the rebate tier structure set below. The rebate will be determined quarterly from the Effective Date of the contract identified in Section B.1. and will be based on the total accumulative volume of spend for Rebated Rentals set forth in the rebate tier structure below for the duration of the Contract Term, including any renewals or extensions.

Spend Range			Percentage to State	
$ -	to	$ 1,000,000.00	provides	1.00%
$ 1,000,001.00	to	$ 1,500,000.00	provides	1.50%
$ 1,500,001.00	to	$ 2,000,000.00	provides	1.75%
$ 2,000,001.00	to	$ 2,500,000.00	provides	2.00%
$ 2,500,001.00	to	$ 3,000,000.00	provides	2.25%
$ 3,000,001.00	to	$ 3,500,000.00	provides	2.50%
$ 3,500,001.00	to	$ 4,000,000.00	provides	2.75%
$ 4,000,001.00	to	$ 5,500,000.00	provides	3.00%

$ 5,500,001.00	to	$ 7,000,000.00	provides	3.25%
$ 7,000,001.00	to		provides	3.50%

The rebate will be paid by the Contractor within forty-five (45) days after the end of each quarter as set forth below:

Calendar Quarter 1 (Jan 1-Mar 31)
Calendar Quarter 2 (Apr 1-June 30)
Calendar Quarter 3 (July 1-Sep 30)
Calendar Quarter 4 (Oct 1-Dec 31)

Contractor shall submit payments to:

Ron Plumb, Director of Financial Management
Department of General Services
22nd Floor, William R Snodgrass, Tennessee Tower
312 Rosa L. Parks Avenue
Nashville, TN 37243

C.11. Pricing and Fees

a. For Contractor rentals to Authorized Users for business use only, the rates in Contract Attachment B shall include full damage waiver.

b. For Contractor rentals to Authorized Users for business use only, the rates in Contract Attachment B shall include liability protection for accidents arising out of the operation or use of the rental vehicle with combined single limits of one million dollars ($1,000,0000) per occurrence. Unless required by law, liability protection excludes any protection afforded under: first party benefits; personal injury protection; medical payments; no-fault; and uninsured or underinsured motorist. Liability protection provides no coverage for physical damage to, or theft of, the rental vehicle. Insurer and policy terms shall not change without prior, written notice to the State. For leisure rentals to Authorized Users, the limits of liability described in this paragraph, C.11.b, do not apply. For leisure rentals to Authorized Users, liability protection for third party claims, if applicable, will be as specified in the applicable rental agreement with the Contractor.

c. For rentals under the National name brand only, the Contractor must provide lower pricing on a reserved vehicle should the user's reserved vehicle have a lower advertised rate than the State contract pricing at the time of pick-up.

d. The Contractor will not be allowed to charge the Authorized User a fee exceeding one (1) day of the rental rate in the situation there is a no-show or late cancellation of reservation. A late cancellation shall be defined as a cancellation made within fifty-nine (59) minutes. A no-show or late cancellation fee shall not be applicable to Group 3.

e. The rates provided in Contract Attachment B are not subject to blackout dates. Except for rentals in the New York City metropolitan area, the Contractor will not be allowed to impose surcharges during peak seasons.

f. The Contractor may charge an airport concession fee on vehicles rented only at airport locations. These fees are provided in Contract Attachment B. The Authorized User must not be charged an airport fee for vehicles rented at off-airport locations.

g. The Contractor may charge a daily city differential rate on rentals in the cities identified in Contract Attachment B.

h. In the event an Authorized User fails to fill the gas tank up to the same level that was present at rental pick up, the Contractor may charge the local per gallon pump price plus the per gallon fuel surcharge in Attachment B on the amount of fuel required to return the gas tank to the level present at rental pickup. The Contractor shall not charge a penalty fee for this action. Contractor shall report the local per gallon pump price to the State monthly.

j. In the event a user must reserve a vehicle for a one-way trip within the State of Tennessee, the Contractor may not charge additional fees or surcharges. For all one-way rentals not within the State of Tennessee that originate and terminate in different States, the Contractor will charge the one-way rates provided in Attachment B.

k. In the event a vehicle is returned late the Contractor will charge the contracted hourly rate for each hour past the originally specified return time that the vehicle is in use. The hourly rate will be charged until it reaches four (4) hours at which time the Contractor will charge a full daily rate until the vehicle return time.

D. MANDATORY TERMS AND CONDITIONS:

D.1. Required Approvals. The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.

D.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State:

Laitin Beecham, Category Specialist
Department of General Services
Central Procurement Office
3rd Floor, WRS Tennessee Tower
312 Rosa L. Parks Avenue
Nashville, TN 37243
Telephone # (615) 291-5794
Laitin.Beecham@tn.gov

The Contractor:

Don Young, Business Rental Sales Executive
EAN Services, LLC
284 Mallory Station Rd.
Franklin, TN 37067
Donald.e.young@ehi.com
Telephone # 615-309-1280

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

D.3. Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials. The State's exercise of a valid Renewal Option or Term Extension does not constitute an amendment so long as there are no other changes to the Contract's terms and conditions.

D.4. Subject to Funds Availability. The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount arising out of resulting from such termination.

D.5. Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.

D.6. Termination for Cause. If a Party ("Breaching Party") fails to properly perform its obligations under this Contract, or if a Party materially violates any terms of this Contract ("Breach Condition"), the other Party ("Non-breaching Party") may provide written notice to the Breaching Party specifying the Breach Condition. If within thirty (30) days of notice, the Breaching Party has not cured the Breach Condition, the Non-breaching Party may terminate the Contract. In the event the Non-breaching Party is the State, the State may withhold payments in excess of compensation for completed services or provided goods. The Breaching Party shall not be relieved of liability to the Non-breaching Party for damages sustained by virtue of any breach of this Contract, and the Non-breaching Party may seek other remedies allowed at law or in equity for breach of this Contract.

D.7. Assignment and Subcontracting. The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.

D.8. Conflicts of Interest. The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.

The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if

the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

D.9. Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

D.10. Equal Opportunity. The Contractor agrees as follows:

a. The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

(1) Employment, upgrading, demotion, or transfer, recruitment or recruitment advertising;
(2) Layoff or termination;
(3) Rates of pay or other forms of compensation; and
(4) Selection for training, including apprenticeship.

The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause.

b. The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive considerations for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

c. If the State approves any subcontract, the subcontract shall include paragraphs (a) and (b) above.

d. In addition, to the extent applicable the Contractor agrees to comply with 41 C.F. R. § 60-1.4, as that section is amended from time to time during the term.

D.11. Prohibition of Illegal Immigrants. The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.

a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment A, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.

b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal

immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.

c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.

d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.

e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.

D.12. Records. The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.

D.13. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.

D.14. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested.

D.15. Strict Performance. Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.

D.16. Independent Contractor. The Parties shall not act as employees, partners, joint ventures, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.

D.17. Patient Protection and Affordable Care Act. The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act, as amended ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless from any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.

D.18. Limitation of State's Liability. The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages

of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. Notwithstanding anything else herein, the State's total liability under this Contract (including without limitation any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Estimated Liability. This limitation of liability is cumulative and not per incident.

D.19. Limitation of Contractor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Estimated Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death.

D.20. Hold Harmless. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys' fees, court costs, expert witness fees, and other litigation expenses for the State to enforce the terms of this Contract.

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

D.21. HIPAA Compliance. The State and Contractor shall comply with their respective obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"), to the extent applicable to each Party's respective obligations under the Contract. The obligations set forth in this Section shall survive the termination of this Contract.

a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.

b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.

c. To the extent applicable the State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.

D.22. Reserved.

D.23. Tennessee Department of Revenue Registration. The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.

D.24. Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:

a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;

b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;

c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and

d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded, disqualified, or presently fall under any of the prohibitions of sections a-d.

D.25. Force Majeure. "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees for the affected obligations until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.

D.26. State and Federal Compliance. The Contractor shall comply with all State and federal laws and regulations applicable to Contractor in the Contractor's performance of this Contract.

D.27. Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee, without regard to its conflict or choice of law rules. The Tennessee

Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 408.

D.28. Entire Agreement. This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.

D.29. Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.

D.30. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.

D.31. Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:

a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;
b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes Attachments A through C;
c. any clarifications of or addenda to the Contractor's proposal seeking this Contract;
d. the State solicitation, as may be amended, requesting responses in competition for this Contract;
e. any technical specifications provided to proposers during the procurement process to award this Contract; and
f. the Contractor's response seeking this Contract.

D.32. Iran Divestment Act. The requirements of Tenn. Code Ann. § 12-12-101, *et seq*., addressing contracting with persons as defined at Tenn. Code Ann. §12-12-103(5) that engage in investment activities in Iran, shall be a material provision of this Contract. The Contractor certifies, under penalty of perjury, that to the best of its knowledge and belief that it is not on the list created pursuant to Tenn. Code Ann. § 12-12-106.

D.33. Insurance. Contractor shall maintain insurance coverage as specified in this Section. The State reserves the right to request additional insurance coverage, coverage amounts, and endorsements required under this Contract, such request shall not be unreasonably withheld. Contractor's failure to maintain or submit evidence of insurance coverage, as required, is a material breach of this Contract. If Contractor loses insurance coverage, fails to renew coverage, or for any reason becomes uninsured or self-insured during the Term, Contractor shall immediately notify the State. All insurance companies providing coverage must be: (a) authorized by the Tennessee Department of Commerce and Insurance ("TDCI"); and (b) rated A- / VII or better by A.M. Best. All coverage must be on a primary basis and noncontributory with any other insurance or self-insurance carried by the State. Contractor agrees to name the State as an additional insured where their interest may appear for liabilities arising in whole or in part by the conduct of the Contractor on any insurance policy with the exception of workers' compensation (employer liability). All policies must contain an endorsement for a waiver of subrogation in favor of the State. The deductible or SIR and any premiums are the Contractor's sole responsibility. The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements.

To achieve the required coverage amounts, a combination of an otherwise deficient specific policy and an umbrella policy with an aggregate meeting or exceeding the required coverage amounts is acceptable. For example: If the required policy limit under this Contract is for two million dollars ($2,000,000) in coverage, acceptable coverage would include a specific policy covering one million dollars ($1,000,000) combined with an umbrella policy for an additional one million dollars ($1,000,000). If the deficient underlying policy is for a coverage area without aggregate limits (generally Automobile Liability and Employers' Liability Accident), Contractor shall provide a copy of the umbrella insurance policy documents to ensure that no aggregate limit applies to the umbrella policy for that coverage area. In the event that an umbrella policy is being provided to achieve any required coverage amounts, the umbrella policy shall be accompanied by an endorsement at least as broad as the Insurance Services Office, Inc. (also known as "ISO") "Noncontributory—Other Insurance Condition" endorsement or shall be written on a policy form that addresses both the primary and noncontributory basis of the umbrella policy if the State is otherwise named as an additional insured.

Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified in this Section. The COI must be on a form approved by the TDCI (standard ACORD form preferred). The COI must list each insurer's National Association of Insurance Commissioners (NAIC) number and be signed by an authorized representative of the insurer or broker. The COI must list the State of Tennessee – CPO Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 as the certificate holder. Contractor shall provide the COI prior to the Effective Date. At any time, the State may require Contractor to provide a valid COI. The Parties agree that failure to provide evidence of insurance coverage as required is a material breach of this Contract. If Contractor self-insures, then a COI will not be required to prove coverage. Instead Contractor shall provide a certificate of self-insurance or a letter, on Contractor's letterhead, detailing its coverage, policy amounts, and proof of funds to reasonably cover such expenses.

The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

The insurance obligations under this Contract shall be: (1)—all the insurance coverage and policy limits carried by the Contractor; or (2)—the minimum insurance coverage requirements No representation is made that the minimum insurance requirements of the Contract are sufficient to cover the obligations of the Contractor arising under this Contract. The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.

a. Commercial General Liability ("CGL") Insurance

1) The Contractor shall maintain CGL, which shall be written on an ISO Form CG 00 01 occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises and operations products and completed operations, bodily injury, personal and advertising injury, and liability assumed under an insured contract

The Contractor shall maintain single limits not less than one million dollars ($1,000,000) per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this policy or location of occurrence or the general aggregate limit shall be twice the required occurrence limit.

b. Workers' Compensation and Employer Liability Insurance

1) For Contractors statutorily required to carry workers' compensation and employer liability insurance, the Contractor shall maintain:

    i. Statutory Workers' compensation and employer liability of one million dollars ($1,000,000) per accident for bodily injury by accident, one million dollars ($1,000,000) policy limit by disease, and one million dollars ($1,000,000) per employee for bodily injury by disease.

2) If the Contractor certifies that it is exempt from the requirements of Tenn. Code Ann. §§ 50-6-101 – 103, then the Contractor shall furnish written proof of such exemption for one or more of the following reasons:

    i. The Contractor employs fewer than five (5) employees;

    ii. The Contractor is a sole proprietor;

    iii. The Contractor is in the construction business or trades with no employees;

    iv. The Contractor is in the coal mining industry with no employees;

    v. The Contractor is a state or local government; or

    vi. The Contractor self-insures its workers' compensation and is in compliance with the TDCI rules and Tenn. Code Ann. § 50-6-405.

c. Automobile Liability Insurance

1) The Contractor shall maintain automobile liability insurance which shall cover liability arising out of any automobile (including owned, leased, hired, and non-owned automobiles).

2) The Contractor shall maintain bodily injury/property damage with a limit not less than one million dollars ($1,000,000) per occurrence or combined single limit.

3) Contractor may self-insure this coverage

D.34. Major Procurement Contract Sales and Use Tax. Pursuant to Tenn. Code Ann. § 4-39-102 and to the extent applicable, the Contractor and the Contractor's subcontractors shall remit sales and use taxes on the sales of goods or services that are made by the Contractor or the Contractor's subcontractors and that are subject to tax.

D.35. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law. Notwithstanding the foregoing, Contractor may collect, use and share renter information it receives in connection with vehicle rental transactions and reservations under this Contract as set forth in its privacy policy, the terms of which Authorized Users agree to prior to renting a vehicle ("Renter Information"). The obligations regarding Confidential Information are subject to the requirements of the Tennessee Public Records Act.

The obligations set forth in this Section shall survive the termination of this Contract.

E. SPECIAL TERMS AND CONDITIONS:

E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.

E.2. Additional lines, items, or options. At its sole discretion, the State may make written requests to the Contractor to add lines, items, or options that are needed and within the Scope but were not included in the original Contract. Such lines, items, or options will be added to the Contract through a Memorandum of Understanding ("MOU"), not an amendment.

a. After the Contractor receives a written request to add lines, items, or options, the Contractor shall have ten (10) business days to respond with a written proposal. The Contractor's written proposal shall include:
    (1) The effect, if any, of adding the lines, items, or options on the other goods or services required under the Contract;
    (2) Any pricing related to the new lines, items, or options;
    (3) The expected effective date for the availability of the new lines, items, or options; and
    (4) Any additional information requested by the State.
b. The State may negotiate the terms of the Contractor's proposal by requesting revisions to the proposal.
c. To indicate acceptance of a proposal, the State will sign it. The signed proposal shall constitute a MOU between the Parties, and the lines, items, or options shall be incorporated into the Contract as if set forth verbatim.

Only after a MOU has been executed shall the Contractor perform or deliver the new lines, items, or options.

E.3. Extraneous Terms and Conditions. Contractor shall fill all orders submitted by the State under this Contract. No purchase order, invoice, or other documents associated with any sales, orders, or supply of any good or service under this Contract shall contain any terms or conditions other than as set forth in the Contract. Any such extraneous terms and conditions shall be void, invalid and unenforceable against the State. Any refusal by Contractor to supply any goods or services under this Contract conditioned upon the State submitting to any extraneous terms and conditions shall be a material breach of the Contract and constitute an act of bad faith by Contractor.

E.4. State Furnished Property. The Contractor shall be responsible for the correct use, maintenance, and protection of all articles of nonexpendable, tangible personal property furnished by the State for the Contractor's use under this Contract. Upon termination of this Contract, all property furnished by the State shall be returned to the State in the same condition as when received, less ordinary wear and tear. Should the property be destroyed, lost, or stolen, the Contractor shall be responsible to the State for the fair market value of the property at the time of loss.

E.5. Prohibited Advertising or Marketing. The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.

E.6. Environmental Tobacco Smoke. Pursuant to the provisions of the federal "Pro-Children Act of 1994" and the Tennessee "Children's Act for Clean Indoor Air of 1995," the Contractor shall prohibit smoking of tobacco products within any indoor premises in which services are provided pursuant to this Contract to individuals under the age of eighteen (18) years. The Contractor shall post "no smoking" signs in appropriate, permanent sites within such premises. This prohibition shall be applicable during all hours, not just the hours in which children are present.

Violators of the prohibition may be subject to civil penalties and fines. This prohibition shall apply to and be made part of any subcontract related to this Contract.

E.8. Lobbying. The Contractor certifies, to the best of its knowledge and belief, that:

a. No federally appropriated funds have been paid or will be paid, by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of an agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

b. If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with any contract, grant, loan, or cooperative agreement, the Contractor shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying," in accordance with its instructions.

c. The Contractor shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into and is a prerequisite for making or entering into this transaction imposed by 31 U.S.C. § 1352.

E.9. State Insurance Program. The State of Tennessee self-insures its exposures in general liability, automobile liability, professional malpractice, and workers’ compensation.

a. The limits for general liability, professional malpractice, and automobile liability are three hundred thousand dollars ($300,000) per person and one million dollars ($1,000,000) per occurrence.
b. The limits of liability under workers’ compensation are those set forth in Tenn. Code Ann. § 50-6-101 et seq.

Copies of the statutes that authorize actions against the State of Tennessee, establish the State’s limit of liability, and authorize self-insurance through the Risk Management Fund, are set forth in Tenn. Code Ann. § 9-8-101 et seq.

Persons wishing to file a claim for damages against the State of Tennessee arising from an act or omission of the State or its employees should file a claim with the State Treasury Department, Division of Risk Management and Claims Administration, 15th Floor, Andrew Jackson State Office Building, 502 Deaderick Street, Nashville, Tennessee 37243-0202. A copy of the State of Tennessee’s Certificate of Self-Insurance may be obtained at http://treasury.tn.gov/risk/PDFs/Certificate_of_Self_Insurance.pdf or is available upon request.

E.10. Statewide Contract. This Contract establishes a source or sources of supply for all Tennessee State Agencies. “Tennessee State Agency” refers to the various departments, institutions, boards, commissions, and agencies of the executive branch of government of the State of Tennessee with exceptions as addressed in Tenn. Comp. R. & Regs. 0690-03-01-.01. The Contractor shall provide all goods or services and deliverables as required by this Contract to all Tennessee State Agencies. The Contractor shall make this Contract available to the following

entities who are authorized to and who may purchase off of this Statewide Contract ("Authorized Users"):

a. all Tennessee State governmental entities (this includes the legislative branch; judicial branch; and, commissions and boards of the State outside of the executive branch of government);
b. Tennessee local governmental agencies;
c. members of the University of Tennessee or Tennessee Board of Regents systems;
d. any private nonprofit institution of higher education chartered in Tennessee; and,
e. any corporation which is exempted from taxation under 26 U.S.C. Section 501(c) (3), as amended, and which contracts with the Department of Mental Health and Substance Abuse to provide services to the public (Tenn. Code Ann. § 33-2-1001).

These Authorized Users may utilize this Contract by purchasing directly from the Contractor according to their own procurement policies and procedures. The State is not responsible or liable for the transactions between the Contractor and Authorized Users.

E.11. Survival. The terms, provisions, representations, and warranties contained in this Contract which by their sense and context are intended to survive the performance and termination of this Contract, shall so survive the completion of performance and termination of this Contract

E.12. Contractor Hosted Services Confidential Data, Audit, and Other Requirements

a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:

(1) The Contractor shall ensure that all Confidential State Data (other than except as noted below, Renter Information) is housed in the continental United States, inclusive of backup data. Notwithstanding the foregoing all driver's license data will be maintained in the continental United States.

(2) The Contractor shall encrypt Confidential State Data. Encryption in storage is full disk encryption using 256-bit AES-XTS encryption algorithm. TLS 1.2 is utilized on transporting confidential data. If these technologies are deprecated, current technologies will be used.

(3) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. At the State's request, the Contractor shall review a summary of the Penetration Tests and Vulnerability Assessments on the Processing Environment.

(4) Contractor shall be certified to host Payment Card Industry ("PCI") data in accordance with the current version of PCI DSS ("Data Security Standard"), maintained by the PCI Security Standards Council. The Contractor shall provide upon request of the State with the Contractor's and Subcontractor's annual Attestation of Compliance report within 30 days from when an independent firm provides the report to the Contractor or Subcontractor. No additional funding

shall be allocated for these certifications, authorizations, or audits as these are included in the Estimated Liability of this Contract.

(5) Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State

(6) In Alignment with Contractor's internal storage policies, after termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88.

b. Minimum Requirements

(1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the agreed upon State's Enterprise Information Security Policy. This policy can be found as Attachment D.

(2) The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

(3) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

c. Comptroller Audit Requirements

Upon reasonable notice and at any reasonable time, but not more than once per year, the Contractor agrees to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform reasonable information technology control audits of the Contractor. Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Contractor personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Contractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Contractor's compliance with the State's Enterprise Information Security Policies in Attachment D and all applicable requirements, laws, regulations or policies. The audit shall also include review of the Contractor's alignment of internal controls with the International Standards Organization "ISO" 27001 standards and National Institute of Standards and Technology (NIST) security standards.

The audit may include interviews with technical and management personnel, and review of paper or electronic documentation.

For any audit issues identified, the Contractor will correct the issues in accordance with its own internal security policies, the State's security policies found in Attachment D, ISO 27001 standards, and NIST security standards. In addition, upon request from the State or the Comptroller of the Treasury, the Contractor must provide the State or the Comptroller of the Treasury assurance that the issues were corrected.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

E.13. Personally Identifiable Information. While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only in accordance with this Contract, GLBA, Contractor's privacy policy and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify or ensure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after a breach of PII has been confirmed by the Contractor's Security. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor , at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of legally required notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law. The obligations set forth in this Section shall survive the termination of this Contract.

IN WITNESS WHEREOF,

EAN Services, LLC

DocuSigned by:
Meredith Perkins
922F4FA51048451...

5/20/2020

CONTRACTOR SIGNATURE **DATE**

Meredith Perkins Authorized Officer

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

DEPARTMENT OF GENERAL SERVICES, CENTRAL PROCUREMENT OFFICE:

MICHAEL F. PERRY, CHIEF PROCUREMENT OFFICER **DATE**

ATTACHMENT A

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	65939
CONTRACTOR LEGAL ENTITY NAME:	EAN Services, LLC
EDISON VENDOR IDENTIFICATION NUMBER:	149982

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

DocuSigned by:
Meredith Perkins
922F4FA51048451...

CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

Meredith Perkins Authorized Officer

PRINTED NAME AND TITLE OF SIGNATORY

5/15/2020

DATE OF ATTESTATION

Attachment B

Groups 1, 2, and 3 Vehicle Rental Rates and Permissible Fees and Surcharges
FOR ENTERPRISE AND NATIONAL LOCATIONS IN U.S. AND CANADA

Groups 1, 2, & 3 Vehicle Rental and State Lot					
Group 1 and 2: Vehicle Rental					
Group 1: Passenger Vehicles					
	Vehicle Class	**Hourly**	**Daily**	**Weekly**	**Monthly**
1	**Compact Sedan**	$8.37	$27.09	$162.35	$616.64
2	**Intermediate/Mid-Size Sedan**	$9.95	$29.86	$179.16	$716.64
3	**Full-Size Sedan**	$10.28	$30.85	$185.10	$740.40
4	**Small/Mid-Size Sport Utility Vehicle**	$15.57	$46.70	$280.20	$1,120.80
5	**Large Sport Utility Vehicle**	$24.07	$72.21	$433.26	$1,733.04
6	**Minivan**	$15.91	$47.73	$286.38	$1,145.52
7	**Passenger Van (15 or more passengers)**	$25.18	$75.54	$453.24	$1,812.96
Group 2: Commercial Vehicles					
-	**Vehicle Class**	**Hourly**	**Daily**	**Weekly**	**Monthly**
1	**Pick-up Truck - 1/2 Ton**	$ 12.65	$ 38.35	$ 230.00	$ 917.06
2	**Pick-up Truck - 3/4 Ton**	$ 16.79	$ 50.88	$ 231.00	$ 840.00
3	**Box Truck - 16 ft. with Ramp**	$ 24.73	$ 74.93	$ 329.62	$1,189.57
4	**Box Truck - 16 ft. with Lift Gate**	$ 24.73	$ 74.93	$ 329.62	$1,189.57
5	**Box Truck - 24 ft. with Lift Gate**	$ 26.43	$ 80.08	$ 457.68	$1,474.15
6	**Cargo Van**	$ 13.50	$ 40.91	$ 203.35	$ 794.79
Group 3: State Lot					
	Vehicle Class	**Hourly**	**Daily**	**Weekly**	
1	**Compact Sedan**	$5.67	$27.90	$155.28	
2	**Intermediate/Mid-Size Sedan**	$6.40	$29.86	$164.81	
3	**Full-Size Sedan**	$6.77	$30.84	$183.34	
4	**Small/Mid-Size Sport Utility Vehicle**	$11.13	$46.69	$268.67	
5	**Large Sport Utility Vehicle**	$17.11	$72.20	$366.29	
6	**Minivan**	$11.23	$47.73	$257.81	

Applicable Fees and Surcharges		
Fee/Surcharge	**Fee**	**Unit of Measure**
Vehicle Returned Below Fuel Level	$5.99	Gallon
One-Way Rental	N/A	Daily
One-Way Rental	$0.40	Mile
State Lot Only: Administrative Fee per Parking Ticket and Non-Moving/Moving Violation		Once
State Lot Only: Improperly Returned, Smoking, Pet Hair, Not Locked, or Failure to report damage/ accident/theft Fees	$200.00	Once
State Lot Only: Administrative Fee per Toll Charge		Once
State Lot Only: Administrative Fee per tow while vehicle is parked illegally***	$5.99	Once

City/State Surcharge Fees			
City/State Surcharge fees may be applied per day on vehicles rented in the below locations.			
City	**State**	**Fee**	**Unit of Measure**
Baltimore	Maryland	$-	
Chicago	Illinois	$5.00	Daily
Los Angeles	California	$-	
Philadelphia	Pennsylvania	$-	
Detroit	Michigan	$-	
New York	New York	$19.00	Daily
Manhattan	New York	$19.00	Daily
Dallas	Texas	$-	
Houston	Texas	$-	
JFK, LaGuardia	New York/New Jersey	$19.00	Daily
	Arkansas	$-	
Atlanta	Georgia	$-	
Davidson County Convention Center Fee	Tennessee	$-	

Airport Fees and Surcharges			
Airport Name	**Airport Code**	**State**	**Fee**
Birmingham International Airport	BHM	Alabama	$-
Dothan Regional Airport	DHM	Alabama	$-
Huntsville International Airport	HSV	Alabama	$-
Mobile	MOB	Alabama	$5.00
Montgomery	MGM	Alabama	$-
Anchorage International Airport	ANC	Alaska	$10.00

Fairbanks International Airport	FAI	Alaska	$5.00
Juneau International Airport	JNU	Alaska	$-
Flagstaff Pulliam Airport	FLG	Arizona	$-
Phoenix, *Phoenix Sky Harbor International Airport*	PHX	Arizona	$-
Tucson International Airport	TUS	Arizona	$-
Yuma International Airport	YUM	Arizona	$-
Fayetteville	FYV	Arkansas	$-
Little Rock National Airport	LIT	Arkansas	$5.00
Burbank	BUR	California	$5.00
Fresno	FAT	California	$-
Long Beach	LGB	California	$5.00
Los Angeles International Airport	LAX	California	$5.00
Oakland	OAK	California	$5.00
Ontario	ONT	California	$5.00
Palm Springs	PSP	California	$-
Sacramento	SMF	California	$5.00
San Diego	SAN	California	$5.00
San Francisco International Airport	SFO	California	$5.00
San Jose	SJC	California	$5.00
Santa Ana	SNA	California	$-
Aspen	ASE	Colorado	$10.00
Colorado Springs	COS	Colorado	$5.00
Denver International Airport	DEN	Colorado	$5.00
Grand Junction	GJT	Colorado	$-
Pueblo	PUB	Colorado	$-
Hartford	BDL	Connecticut	$5.00
Washington, *Dulles International Airport*	IAD	District of Columbia	$8.00
Washington National Airport	DCA	District of Columbia	$8.00
Daytona Beach	DAB	Florida	$-
Fort Lauderdale-Hollywood International Airport	FLL	Florida	$-
Fort Meyers	RSW	Florida	$10.00
Jacksonville	JAX	Florida	$-
Miami International Airport	MIA	Florida	$5.00
Orlando	MCO	Florida	$-
Pensacola	PNS	Florida	$-
St. Petersburg	PIE	Florida	$-
Sarasota	SRQ	Florida	$-
Tampa	TPA	Florida	$-
West Palm Beach	PBI	Florida	$-
Panama City-Bay County International Airport	PFN	Florida	$-
Orlando Sanford International Airport	SFB	Florida	$-
Atlanta Hartsfield International Airport	ATL	Georgia	$5.00
Augusta	AGS	Georgia	$5.00

Savannah	SAV	Georgia	$-
Hilo	ITO	Hawaii	$-
Honolulu International Airport	HNL	Hawaii	$5.00
Kahului	OGG	Hawaii	$-
Kailua	KOA	Hawaii	$-
Lihue	LIH	Hawaii	$-
Boise	BOI	Idaho	$-
Idaho Falls Regional Airport	IDA	Idaho	$3.00
Chicago Midway Airport	MDW	Illinois	$8.00
Chicago, *O'Hare International Airport*	ORD	Illinois	$8.00
Moline	MLI	Illinois	$-
Peoria	PIA	Illinois	$5.00
Evansville	EVV	Indiana	$-
Fort Wayne	FWA	Indiana	$-
Indianapolis International Airport	IND	Indiana	$19.00
Lafayette	LAF	Indiana	$-
South Bend	SBN	Indiana	$-
Cedar Rapids	CID	Iowa	$-
Des Moines	DSM	Iowa	$-
Wichita	ICT	Kansas	$-
Lexington	LEX	Kentucky	$5.00
Louisville	SDF	Kentucky	$5.00
Baton Rouge	BTR	Louisiana	$-
New Orleans International Airport	MSY	Louisiana	$19.00
Shreveport	SHV	Louisiana	$-
Augusta	AUG	Maine	$-
Bangor	BGR	Maine	$5.00
Portland	PWM	Maine	$5.00
Baltimore	BWI	Maryland	$5.00
Boston, Logan International Airport	BOS	Massachusetts	$5.00
Hyannis	HYA	Massachusetts	$-
Nantucket	ACK	Massachusetts	$-
Worcester	ORH	Massachusetts	$-
Battlecreek	BTL	Michigan	$-
Detroit Metropolitan Airport	DTW	Michigan	$5.00
Detroit	DET	Michigan	$5.00
Flint	FNT	Michigan	$-
Grand Rapids	GRR	Michigan	$-
Kalamazoo-Battle Creek International Airport	AZO	Michigan	$5.00
Lansing	LAN	Michigan	$5.00
Saginaw	MBS	Michigan	$-
Duluth	DLH	Minnesota	$-
Minneapolis/St.Paul International Airport	MSP	Minnesota	$-

Rochester	RST	Minnesota	$-
Gulfport	GPT	Mississippi	$5.00
Jackson	JAN	Mississippi	$-
Kansas City	MCI	Missouri	$-
St Louis, Lambert International Airport	STL	Missouri	$3.00
Springfield	SGF	Missouri	$-
Billings	BIL	Montana	$5.00
Bozeman Yellowstone International Airport	BZN	Montana	$-
Lincoln	LNK	Nebraska	$10.00
Omaha	OMA	Nebraska	$-
Las Vegas, *Las Vegas McCarran International Airport*	LAS	Nevada	$-
Reno-Tahoe International Airport	RNO	Nevada	$-
Manchester	MHT	New Hampshire	$-
Atlantic City International Airport	ACY	New Jersey	$-
Newark International Airport	EWR	New Jersey	$-
Trenton	TTN	New Jersey	$-
Albuquerque International Airport	ABQ	New Mexico	$-
Alamogordo	ALM	New Mexico	$-
Albany International Airport	ALB	New York	$5.00
Buffalo	BUF	New York	$5.00
Islip	ISP	New York	$-
New York, *John F Kennedy International Airport*	JFK	New York	$19.00
New York, *La Guardia Airport*	LGA	New York	$19.00
Newburgh	SWF	New York	$-
Rochester	ROC	New York	$5.00
Syracuse	SYR	New York	$5.00
Westchester	HPN	New York	$19.00
Asheville	AVL	North Carolina	$-
Charlotte/Douglas International Airport	CLT	North Carolina	$-
Fayetteville	FAY	North Carolina	$10.00
Greensboro	GSO	North Carolina	$-
Raleigh	RDU	North Carolina	$-
Winston-Salem	INT	North Carolina	$-
Bismark	BIS	North Dakota	$-
Fargo	FAR	North Dakota	$-
Grand Forks International Airport	GFK	North Dakota	$-
Akron	CAK	Ohio	$-
Cincinnati	CVG	Ohio	$-
Cleveland	CLE	Ohio	$-
Columbus	CMH	Ohio	$-
Dayton	DAY	Ohio	$-
Toledo	TOL	Ohio	$-
Oklahoma City	OKC	Oklahoma	$-

Tulsa	TUL	Oklahoma	$-
Eugene	EUG	Oregon	$-
Portland International Airport	PDX	Oregon	$-
Portland, Hillsboro Airport	HIO	Oregon	$-
Salem	SLE	Oregon	$-
Allentown	ABE	Pennsylvania	$5.00
Erie	ERI	Pennsylvania	$-
Harrisburg	MDT	Pennsylvania	$5.00
Philadelphia	PHL	Pennsylvania	$5.00
Pittsburgh	PIT	Pennsylvania	$-
Scranton	AVP	Pennsylvania	$-
Providence - T.F. Green Airport	PVD	Rhode Island	$-
Charleston	CHS	South Carolina	$-
Columbia	CAE	South Carolina	$-
Greenville	GSP	South Carolina	$-
Myrtle Beach	MYR	South Carolina	$-
Pierre	PIR	South Dakota	$-
Rapid City	RAP	South Dakota	$-
Sioux Falls	FSD	South Dakota	$-
Bristol	TRI	Tennessee	$-
Chattanooga	CHA	Tennessee	$-
Knoxville	TYS	Tennessee	$-
Memphis	MEM	Tennessee	$-
Nashville	BNA	Tennessee	$-
Upper Cumberland Regional Airport	SRB	Tennessee	$-
Amarillo	AMA	Texas	$5.00
Austin Bergstrom International Airport	AUS	Texas	$5.00
Corpus Christi	CRP	Texas	$5.00
Dallas Love Field Airport	DAL	Texas	$5.00
Dallas/Fort Worth International Airport	DFW	Texas	$5.00
El Paso	ELP	Texas	$5.00
Houston, William B Hobby Airport	HOU	Texas	$-
Houston, George Bush Intercontinental Airport	IAH	Texas	$-
Lubbock	LBB	Texas	$-
Midland	MAF	Texas	$5.00
San Antonio International Airport	SAT	Texas	$5.00
Tyler Pounds Regional Airport	TYR	Texas	$5.00
Salt Lake City	SLC	Utah	$-
Burlington	BTV	Vermont	$-
Montpelier	MPV	Vermont	$-
Rutland	RUT	Vermont	$-
Dulles	IAD	Virginia	$-
Newport News	PHF	Virginia	$-

Norfolk	ORF	Virginia	$10.00
Richmond	RIC	Virginia	$-
Roanoke	ROA	Virginia	$-
Virginia Tech Montgomery Executive Airport	BCB	Virginia	$-
Pasco, Pasco/Tri-Cities Airport	PSC	Washington	$-
Seattle, Tacoma International Airport	SEA	Washington	$-
Spokane International Airport	GEG	Washington	$-
Charleston	CRW	West Virginia	$-
Clarksburg	CKB	West Virginia	$-
Green Bay	GRB	Wisconsin	$-
Madison	MSN	Wisconsin	$-
Milwaukee	MKE	Wisconsin	$5.00
Central Wisconsin Airport	CWA	Wisconsin	$-
Casper	CPR	Wyoming	$-
Cheyenne	CYS	Wyoming	$-
Jackson Hole	JAC	Wyoming	$-
Rock Springs	RKS	Wyoming	$-

Attachment C

Implementation Plan

Implementation

The entire implementation process will be managed by your account management team, with support from internal departments, facilitating a smooth transition. We will provide all necessary implementation and marketing materials for distribution to your employees.

To monitor transition progress, we will use a timeline and strategy checklist to ensure thorough implementation. Our timeline on the following pages notes all pertinent action items, as well as the expected completion dates and any other relevant information.

Traditional Vehicle Rental, Passenger Vehicles

We will create a complimentary, instant enrollment link for your travelers to join our frequent renter program, Emerald Club. The customized link prepopulates certain fields for the member, such as the account number, insurance coverage, and other agreement provisions. The link can be embedded in our logo on the State's intranet and in emails.

The education of both the State of Tennessee travelers and travel agents is an important part of the implementation process. We will provide documents for the State intranet and emails that outline services and benefits available to your employees. Your account management team can conduct travel seminars to teach your renters about our services. Travel agency guides can be produced for the State's preferred agency.

In addition, the State of Tennessee's top 10 rental locations will be notified no less than 30 days before a new contract is launched to make any necessary adjustments in fleet or personnel.

Implementation Timeline

Week 1

- Receive letter of intent
- Confirm program start date
- Use pre-enrollment timeline calculator to identify key dates
- Implementation and Emerald Club conversion meetings:
  - Confirm program start date
  - Identify and contact State of Tennessee key personnel
  - Pinpoint locations that need pickup and delivery
  - Review long-term rental needs and personal mileage reimbursements
  - Establish dates for communication and announcement methods
  - Review Emerald Club enrollment methods:
    - Identify travelers qualified for status matching and executives eligible for invited tiers
  - Establish program training method and dates:
    - Loading of contract rates for Enterprise and National
    - Meeting to review process and progress of week

Week 2 – 3

- Receive traveler database
- The State announces program — Enterprise and National to receive endorsement
- Begin Emerald Club enrollment:
  - Continue Emerald Elite invited enrollments

- Obtain contact information for travel agency:
  - Schedule dates for training seminars and presentations
  - Create agent incentive to coincide with contract launch
- "Key Account" notice sent to the State's top rental locations; begin training with Enterprise and National managers and airport staff
- "Key Account" notice sent internally for training of reservation agents, customer service staff, etc.
- Discuss Customer Satisfaction Guarantee rollout:
  - Review sample questions for online survey and select dates
- Review and confirm risk management process
- Review long-term rentals and personal mileage reimbursements findings
- Confirm rate loading and test rates for accuracy
- Advise the State of Direct Billing accounts and procedures
- Creation of Travel Agency guides for seminars
- Meeting to review process and progress of week
- Obtain a top list of FBO locations (if applicable)

Week 3 – 4

- Email virtual Emerald Club membership information — National
- Conduct seminar with travel agency:
  - Roll out agent incentive
  - Loyalty report furnished for passenger profiles
  - Benefits of Enterprise in home-city locations
- Final confirmation of rates loaded
- Email Emerald Club Elite packets
- Implementation review with entire the State travel team
- Finalize contract and obtain signatures
- Weekly email reminder to travelers — Instant Enrollment
- Meeting to review process and progress of week

Week 5 – 6

- Program start date
- Online customer service surveys sent out (if requested)
- Weekly email reminder to travelers — Instant Enrollment

Post-Launch

- Implementation Evaluation Meeting after first three months
- Weekly email reminder to travelers — Instant Enrollment
- For the first 45 days, hold weekly or biweekly calls to review rental program progress
- Discuss quarterly reporting methods and formats

State Lot

At Enterprise, we believe it is important to make sure all of your employees are familiar with the new car-sharing program upon launch. That is why we are very thorough in our implementation process — customer satisfaction depends upon it.

When starting a new program, Enterprise CarShare can have vehicles in place and ready to rent soon after the execution of a signed contract. With our purchasing power, vehicle availability and selection is unlimited.

Implementation Meetings	Pre "Go Live"

• Discuss best practices and timeline to launch a successful program • Determine effective "Go Live" date • Identify communication process to employees • Set email announcement dates • Set employee "Learn &Enroll" meetings • Determine policy updates • Identify payment method • Identify vehicle types • Identify vehicle locations	• Initial announcement email sent • Announcement sent prior to "Go Live" if needed • Travel policy updates on intranet site/travel portal to reflect Enterprise CarShare usage guidelines • Customized Join Link is live • Conduct "Learn & Enroll" meetings – 80 percent enrollment goal • Reservation link is live for future reservations

Implementation Group 2

As stated previously, the entire implementation process will be managed by your account management team, with support from internal departments, facilitating a smooth transition. We will provide all necessary implementation and marketing materials for distribution to your employees.

To monitor transition progress, we will use a timeline and strategy checklist to ensure thorough implementation. Our timeline below and on the following pages notes all pertinent action items, as well as the expected completion dates and any other relevant information.

The education of both the State of Tennessee travelers and travel agents is an important part of the implementation process. We will provide documents for the State intranet and emails that outline services and benefits available to your employees. Your account management team can conduct travel seminars to teach your renters about our services. Travel agency guides can be produced for the State's preferred agency.

In addition, the State of Tennessee's top 10 rental locations will be notified no less than 30 days before a new contract is launched to make any necessary adjustments in fleet or personnel.

Implementation Timeline

Week 1

- Receive letter of intent
- Confirm program start date
- Use pre-enrollment timeline calculator to identify key dates
- Implementation meetings:
  - Confirm program start date
  - Identify and contact State of Tennessee key personnel
  - Pinpoint locations that need pickup and delivery
  - Review long-term rental needs and personal mileage reimbursements
  - Establish dates for communication and announcement methods
  - Establish program training method and dates:
    - Loading of contract rates for Enterprise
- Meeting to review process and progress of week

Week 2 – 3

- Receive traveler database
- The State announces program — Enterprise to receive endorsement
- Obtain contact information for travel agency:
  - Schedule dates for training seminars and presentations
  - Create agent incentive to coincide with contract launch
- "Key Account" notice sent to the State's top rental locations; begin training with Enterprise managers and airport staff
- "Key Account" notice sent internally for training of reservation agents, customer service staff, etc.
- Discuss Customer Satisfaction Guarantee rollout:
  - Review sample questions for online survey and select dates
- Review and confirm risk management process
- Review long-term rentals and personal mileage reimbursements findings
- Confirm rate loading and test rates for accuracy
- Advise the State of Direct Billing accounts and procedures
- Creation of Travel Agency guides for seminars
- Meeting to review process and progress of week
- Obtain a top list of FBO locations (if applicable)

Week 3 – 4

- Conduct seminar with travel agency:
  - Roll out agent incentive
  - Benefits of Enterprise in home-city locations
- Final confirmation of rates loaded
- Implementation review with entire the State travel team
- Finalize contract and obtain signatures
- Weekly email reminder to travelers — Instant Enrollment
- Meeting to review process and progress of week

Week 5 – 6

- Program start date
- Online customer service surveys sent out (if requested)

Post-Launch

- Implementation Evaluation Meeting after first three months
- For the first 45 days, hold weekly or biweekly calls to review rental program progress
- Discuss quarterly reporting methods and formats

Enterprise Information Security Policies – SWC 205 Attachment D

State of Tennessee
Department of Finance and Administration
Strategic Technology Solutions Information Security Program

Document Version 2.4 – January 29, 2020

Table of Contents

1. EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies of the State of Tennessee along with the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. Information security is a critical component that is required to enable and ensure the confidentiality, integrity and availability of data, network and processing resources required for the State of Tennessee to perform its business and operational practices. This policy document has been created to establish and uphold the minimum requirements that are necessary to protect Information Technology (IT) resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction or disclosure as set forth by the Information Systems Council (ISC) of the State of Tennessee.

The scope of this document is intended to cover any information asset owned, leased or controlled by, or operated on behalf of the State of Tennessee. The methodologies and practices of external entities that require access to the State of Tennessee's IT resources may be impacted and could be included in this scope. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches and mobile devices (computing platforms) owned by the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware or application software under the control of third parties that connect in any way to the State of Tennessee's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.

- All data, information, knowledge, documents, presentations, databases or other information resource stored on contractor computing platforms and/or transferred over contractor network infrastructure.

This document applies to all full- and part-time employees of the State of Tennessee, all third parties, outsourced employees or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data.

By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the State envisions maximum voluntary compliance. The policy development and implementation process includes an impact analysis, input from Agency information technology (IT)

professionals and approval by the Chief Information Security Officer (CISO) and Policy Review Committee within Strategic Technology Solutions (STS), Department of Finance and Administration.

All IT resources and any information system owned by the State of Tennessee should be protected from unauthorized disclosure, use, modification or destruction in a manner commensurate with their value, sensitivity and criticality to the business and operation of the State government and those they serve. Access to information technology assets will be granted using the principle of least privilege.

All approved policies will support the requirements established by the Information Systems Council of the State of Tennessee.

2. INTRODUCTION

The Information Security Challenge

IT solutions are driven by the demands of our daily business activities. The ability to procure efficient communication, IT resources and technologies that support business processes at a low cost is a foundational component of successful IT programs. Cloud technologies and offerings continue to grow, and this integration moves quickly to align itself with the "just in time" requirements of the business. Given the growth demands of the business along with the associated time sensitive integration strategies, we are presented with new risks at every turn. Organizations will frequently take risks in order to meet those time sensitive business requirements, sometimes bypassing existing processes to meet time demands of the customers whom they serve. As the State expands its use of cloud technologies, it is incumbent upon the State to ensure the State data that is hosted or processed in cloud environments or is transmitted across cloud infrastructure receives protection similar to what is provided by the STS managed data centers and infrastructure. This practice, also known as risk management, is a component of any successful business. Modern enterprises will implement risk management and/or information security programs to mitigate these risks.

The State of Tennessee has recognized the need to evaluate risk and has established information security programs. One of the main goals of any successful information security program is to protect the organization's revenues, resources, and reputation. This is accomplished through several means. Some examples are implementing risk management methodologies, security architectures, control frameworks and security policy.

Security policies are a foundational component of any successful security program. The Enterprise Information Security Policies for the State of Tennessee are based on the International Standards Organization (ISO) 27000 series standard framework. The policies are designed to comply with applicable statutes and regulations; however, if there is a conflict, applicable statutes and regulations will take precedence. The policies included in this document are to be considered the minimum requirements for providing a secure operational environment.

Scope (2.1)

The scope of this document is intended to cover any information asset owned, leased or controlled by the State of Tennessee and the methodologies and practices of external entities that require access to the State of Tennessee's IT resources. This document seeks to protect:

- All desktop computing systems, servers, data storage devices, communication systems, firewalls, routers, switches and mobile devices (computing platforms) controlled by or operated on behalf of the State of Tennessee where lawfully permitted.
- All computing platforms, operating system software, middleware or application software under the control of the State of Tennessee, or by third parties, operated on behalf of the State of Tennessee that connect in any way to the State's enterprise computing or telecommunications network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on the State of Tennessee's computing platforms and/or transferred by the State's enterprise network.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on contractor computing platforms and/or transferred over contractor network infrastructure.
- All data, information, knowledge, documents, presentations, databases or other information resource stored on contractor computing platforms and/or transferred over contractor network infrastructure.

All full- and part-time employees of the State of Tennessee, all third parties, outsourced employees, or vendors who work on state premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data should adhere to the policies and requirements set forth in this document.

Authority (2.2)

The ISC authorized the Department of Finance and Administration, Strategic Technology Solutions to establish and enforce enterprise policies and standards related to information security. These policies and standards include, but are not limited to, network and Internet access, any computing platform attached to the State's enterprise network and any wired or wireless technology attached to the State's enterprise network. STS is responsible and authorized by the ISC to perform audits on any device that attaches to the State of Tennessee's enterprise network.

References:

Tennessee Code Annotated, Section 4-3-5501, et seq., effective May 10, 1994 [Acts 1994, ch. 992, § 2; 1995, ch. 305, § 66] 1994

ISC Information Resource Policies, Policy 1.00 ISC Information Resource Policies, Policy 5.00 ISC Information Resource Policies, Policy 9.00 ISC Information Resource Policies, Policy 13.00

Exceptions (2.3)

All exceptions to any of the security policies will be reviewed, evaluated and processed by a member of the Chief Information Security Officer's staff.

Review (2.4)

Review of this document takes place within the STS Policy Review Committee sessions and will occur on an annual (within every three hundred and sixty-five (365) days) basis at a minimum. Document review can also be requested by sending a request to the Chief Information Security Officer.

The official policy document and supporting documentation will be published on the STS intranet site located at:

https://www.teamtn.gov/sts/policies-and-procedures.html

Document Format (2.5)

This document generally follows the International Standards Organization 27000 series standard framework for information technology security management. Each section starts with a high-level security control category followed by the control objective. Policy statements follow the objectives.

The MINIMUM COMPLIANCE REQUIREMENTS category contains the minimum requirements for compliance criteria that are global and apply to all systems or platforms across the entire enterprise.

X. Section Name

Control Category (x.x)
Objective Statement

Policy Name (x.x.x)

Policy Statement

Sub-Policy Name (x.x.x.x)
Sub-Policy Statement

MINIMUM COMPLIANCE REQUIREMENTS:

Policy Maintenance (2.6)

All policies will be maintained in accordance with the STS policy process documentation.

3. INFORMATION SECURITY POLICIES

Management Direction for Information Security (3.1)

Objective: To provide management direction and support for information security in accordance with agency business requirements and relevant state and federal statute and regulations for the State of Tennessee's computing environments.

Policies for Information Security (3.1.1)

STS Information Security Management will initiate, control and communicate an enterprise information security architecture that includes, but is not limited to, a policy framework, an organizational and communication framework and a security technology framework.

Agency Policies for Information Security (3.1.2)

Agencies should develop and communicate agency specific policy documents as required by agency or regulatory requirements provided the minimum requirements set forth in this document are met.

4. OPERATIONS SECURITY

Operational Procedures and Responsibilities (4.1)

Objective: To protect critical State information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction to ensure correct and proper operations.

Documented Operating Procedures (4.1.1)

All agencies of the State of Tennessee and vendors or outsourced employees acting on behalf of the State should identify, document and maintain standard security operating procedures and configurations for their respective operating environments and ensure the documentation is available to all users who need it.

Change Management (4.1.2)

Changes to information processing facilities and systems should be controlled and monitored for security compliance. Formal management responsibilities and procedures should exist to ensure satisfactory control of all changes to equipment, software, applications, configurations and/or procedures that affect the State of Tennessee's operational environment. All written documentation generated by the change control policies and procedures should be retained as evidence of compliance.

Change Control Procedures (4.1.2.1)

Change control procedures should include authorization, risk assessment, logging, auditability, and roll back procedures.

Capacity Management (4.1.3)

The use of IT resources should be monitored and tuned so that projections of future capacity requirements can be made.

Separation of Development, Testing and Operational Environments (4.1.4)

Development and testing environments should be segregated from production environments in order to reduce the risks of unauthorized access or changes to the production environment. Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and should not be used in development or test environments.

Protection from Malware (4.2)

Objective: Prevent the automated propagation of malicious code and contamination of environments attached to the enterprise network.

Malicious Software Control (4.2.1)

All computing platforms that are attached to the State's enterprise technology infrastructure or operated on behalf of the State should be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses, logic bombs and rootkits. Compromised systems should be removed from the operational environment. All computing platforms that are attached to the State's enterprise technology infrastructure will participate in the State's enterprise antivirus program if antivirus signatures are available for the computing platforms. STS Security Management reserves the right to seize any State compromised system for forensic analysis.

Backup (4.3)

Objective: To prevent loss of data and to ensure data availability.

Data Backup (4.3.1)

Backup copies of data, software and system images should be taken and tested regularly in accordance with established procedures. A copy of the backup data should be stored off-site according to applicable regulatory requirements and EHI policy. Results of restore tests should be furnished to data owners with recommendations for any remedial steps found. Data owners should approve any remedial plans and timelines for implementing those remediation steps within a reasonable period not to exceed three months. Following remediation, the restore testing should be repeated and results documented to ensure that those steps mitigated all identified issues.

Logging and Monitoring (4.4)

Objective: To record events and generate evidence.

Event Logging (4.4.1)

All systems should be configured to support security event logging, recording user activities, exceptions, faults and information security events. System administrators should monitor and report inappropriate access to the EHI CSIRT. Critical systems should be configured to support automated logging to a facility that protects the integrity of the logs. Logging levels and

monitored elements will be configured in accordance with federal and state statute and regulatory requirements.

Availability and Performance Monitoring (4.4.2)

Critical systems should be configured to support EHI approved automated monitoring of system availability and performance.

Protection of Log Information (4.4.3)

Logging facilities and log information should be protected against tampering and unauthorized access.

Administrator and Logs (4.4.4)

System administrator activities should be logged and the logs protected and regularly reviewed.

Clock Synchronization (4.4.5)

Approved State of Tennessee managed enterprise network time servers should be the only State devices permitted to synchronize with external time services. All State provided or managed systems will synchronize time with approved State of Tennessee managed enterprise network time servers. All non-State provided or managed systems storing, processing or transmitting State data should be synchronized to NTP.

Control of Operational Software (4.5)

Objective: To ensure the integrity of operational systems.

Installation of Software on Operational Systems (4.5.1)

Only software that has been licensed and approved as a State standard software product or that has been approved as an exception through the State's architecture standards approval process should be installed on devices covered by the software's license agreement.

Patch Management (4.5.1.1)

All applications and processing devices that are attached to the State's enterprise technology infrastructure will have critical security related application, operating system, and/or security related patches made available by the software or hardware vendor applied within 90 calendar days or sooner if an acceptable date can be agreed upon by all affected

parties. Emergency patches and updates will be applied as soon as possible following successful validation and testing.

Patch schedule:

- 14 days for critical patches addressing known exploits
- 30 days for high patches addressing known exploits
- 90 days for critical patches
- 90 days high patches

Software Maintenance (4.5.1.2)

Servers and workstation computing devices should have defined maintenance windows within every 90 days.

Appliances should have established review and maintenance cycles for software updates.

Software Development Code (4.5.1.3)

Software development code cannot be installed on production systems (i.e. non-compiled software programming code).

Review of Application and Operating System Changes (4.5.1.4)

Applications and operating systems should be reviewed and tested to ensure that there is no adverse impact on operations or security when a change has been performed on the operating system. (e.g. patch).

Technical and Vulnerability Management (4.6)

Objective: To prevent the exploitation of technical vulnerabilities.

Management of Technical Vulnerabilities (4.6.1)

Information about technical vulnerabilities on information systems and supporting infrastructure should be obtained in a timely fashion, evaluated for exposure and risk to the State and appropriate measures implemented to address the associated risk.

Restrictions on Software Installation (4.6.2)

Users should not install software that has not been approved by STS and their agency.

Information Systems Audit Considerations (4.7)

Objective: To minimize the impact of audit activities on operational systems.

Information Systems Audit Controls (4.7.1)

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed upon in advance to minimize disruptions to business processes.

5. ACCESS CONTROL

Business Requirements of Access Control (5.1)

Objective: To limit access to information and information processing facilities.

Access Control Policy (5.1.1)

All access rules and requirements to access the State of Tennessee's IT resources should be developed, documented, and maintained by their respective resource owners. Access to the State of Tennessee's IT resources will be granted consistent with the concept of least privilege. All information processing systems owned by or operated on behalf of the State of Tennessee should have an appropriate role-based access control system that ensures only legitimate users and/or systems have access to IT resources that they are explicitly authorized to use.

Access to Networks and Network Services (5.1.2)

All access and connectivity to the State of Tennessee's enterprise network or networks operated on behalf of the State should be granted consistent with the concept of least privilege. Users will only be provided with access to the network and network resources that they have been specifically authorized to use.

Remote Access (5.1.2.1)

All users who are accessing the State's internal network should access those resources through a State approved multifactor Virtual Private Network (VPN) solution. All users who access State data on networks operated on behalf of the State should use secure connection methods.

Information Security Roles and Responsibilities (5.1.3)

All information security responsibilities should be defined and assigned by the access granting authority.

Segregation of Duties (5.1.4)

Where appropriate, conflicting duties and areas of responsibility should be segregated and assigned to different individuals to reduce opportunities for unauthorized or unintentional modification or misuse of the State's assets.

User Access Management (5.2)

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

User Registration and De-Registration (5.2.1)

A formal user registration and de-registration process should be implemented to enable assignment of access rights and to adjust those rights as the user's role changes.

User Access Provisioning (5.2.2)

User access to IT resources should be authorized and provisioned according to the Agency's employee provisioning process.

User Account Naming (5.2.2.1)

All State user accounts will follow a State approved standardized naming convention.

Management of Privileged Access Rights (5.2.3)

Users should have the least privileges required to perform their roles as identified and approved by their management. The allocation and use of privileged access rights should be restricted and controlled.

Management of Secret Authentication of Information Users (5.2.4)

The allocation of secret authentication information should be controlled through a formal management process.

Review of User Access Rights (5.2.5)

A user's access rights should be reviewed, validated and updated for appropriate access by their section supervisor on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfers within and between agencies).

Removal or Adjustment of Access Rights (5.2.6)

All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement or change of agency by the close of business on the user's last working day or within 24 hours of notification of the user's death, determination of job abandonment or retroactive notification of resignation or retirement.

In the event the user is retiring and returning as a 120 Day Appointment within 45 days of the last working day, the user's account is exempt from the revocation requirement stated above.

Procedures for emergency removal of access rights should be in place.

User Responsibilities (5.3)

Objective: To make users accountable for safeguarding their authentication information.

Use of Secret Authentication Information (5.3.1)

Users should follow State policy in the use of secret authentication information.

System and Application Access Control (5.4)

Objective: To prevent unauthorized access to systems and applications.

Information Access Restriction (5.4.1)

Access to information and application system function should be restricted in accordance with the defined access control policy.

Secure Log-on Procedures (5.4.2)

Where required by the access control policy, access to systems and application should be controlled by a secure log-on procedure. At a minimum, user access to protected IT resources requires the utilization of User Identification (User ID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.

System Administrator Access (5.4.2.1)

All systems administrators or users with elevated privileges using administrative tools or protocols to access servers located in State managed data processing facilities or

facilities operated on behalf of the State must use a multifactor VPN solution to obtain access.

Logon Banner (5.4.2.2)

All systems and devices owned and operated by or on behalf of the State of Tennessee must display the State approved logon banner before the user is able to log in.

Service Account Use (5.4.2.3)

Service accounts should be unique to each application and/or system and should only be used to authenticate systems and/or applications to specific services.

System/Application Account Use (5.4.2.4)

System/application accounts are created upon installation of an application and may have a predetermined User ID. Privileged User access to system accounts must be approved and documented. A system/application account differs from a service account in that individuals may know the password to the system/application account. This account must be elevated to from a lesser account.

An example of this type of account is the default administrative account required by the application.

System Administrator Account Use (5.4.2.5)

System Administrator accounts have elevated privileges and should only be used when elevated privileges are required. Administrative accounts are used to administer operating systems and applications.

Password Management System (5.4.3)

Password management systems should be interactive and should ensure quality passwords.

Use of Privileged Utility Programs (5.4.4)

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Access Control to Program Source Code (5.4.5)

Access to program source code should be restricted to authorized users.

Default Configurations (5.4.6)

All applications and processing devices that are attached to the State's enterprise technology infrastructure should be deployed with modified configurations for, but not limited to, default accounts, and/or installation paths to minimize the use of default settings to gain unauthorized use, modification or destruction.

MINIMUM REQUIREMENTS:

Password Management (5.4.3)

- All user and system administrator passwords must contain a minimum of eight characters.
- All service account and system/application account passwords must contain a minimum of 15 characters.
- All passwords must include a character from each of the following three categories.
  - Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
  - Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
  - Base 10 digits (0 through 9)
  - Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/, including any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- Temporary or default passwords assigned by system administrators or dictated by the operating system must be changed immediately after initial login.
- Passwords must be changed every 90 days or less from the last change. Shared system administrator passwords must be changed when an individual who has access to the passwords leaves.
- All systems that support password history will be configured to remember a password history of 4 at a minimum.
- All passwords should be hashed and salted.

- User ID's will be revoked after five (5) consecutive attempts to login with an invalid password.

- All service account and system/application account passwords must be changed when an individual who has had access to the passwords is terminated or accepts a role where knowledge of those passwords is no longer required.

- Service and system/application accounts should be approved for use and documented in the area where the account is being used.

6. ASSET MANAGEMENT Responsibility for Assets (6.1)

Objective: To identify organizational assets and define appropriate protection responsibilities.

Inventory of Assets (6.1.1)

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be created and maintained in order to protect the assets in accordance with EHI's internal policy.

Ownership of Assets (6.1.2)

All information resource assets listed in the asset inventory should have an assigned owner or entity who will ensure the assets are protected in a manner consistent with their value, sensitivity and criticality to the business and operation of EHI and those it serves or as specified by any superseding state or federal statute or regulation**.**

Acceptable Use of Assets (6.1.3)

Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented, implemented and communicated to the employees and outsourced employees who have access to those assets.

Return of Assets (6.1.4)

All employees and outsourced employees must return all state assets in their possession upon termination of their employment or contract**.**

Asset Identification (6.1.5)

All state hardware assets will be named in accordance with the State approved standardized naming convention.

Data Classification (6.2)

Objective: To ensure the data used and managed by the State receives an appropriate level of protection commensurate with the value, importance and criticality of the data to the State.

Classification of Data (6.2.1)

Data assets owned and/or managed by the State of Tennessee should be classified according to the definition of "Personal Information" or "Confidential Records" as specified by applicable state and/or federal statute or regulations to indicate the need, priorities and degree of protection it will receive. At a minimum, data will be classified as Public or Confidential.

Labelling of Data (6.2.2)

An appropriate set of procedures for labeling data assets owned and/or managed by the State of Tennessee should be developed and implemented in accordance with the State's data classification scheme.

Handling and Use of Data (6.2.3)

Procedures for handling data assets should be developed and implemented in accordance with the data classification scheme adopted by the State.

Public Data Classification and Control (6.2.3.1)

Data classified as public should be protected from unauthorized modification or destruction.

Confidential Data Classification and Control (6.2.3.2)

Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and cannot be used in development or test environments or publicly disclosed. Controls should be applied to data in a manner consistent with its value, sensitivity and criticality to the business and operation of state government. Data classified as confidential must be encrypted at rest and during transmission in accordance with applicable state or federal statute or regulatory requirements.

Confidential Data on Personally Owned Devices (6.2.3.3)

Confidential data should not be stored on personally owned computing platforms or on personally owned mobile computing platforms unless managed by EHI's mobile device management solution or EHI's enterprise configuration manager.

Confidential Electronic Messages Classification and Control (6.2.3.4)

E-mail sent from the State's domain out through the public Internet must be encrypted if it contains confidential information in the body or attachment. Confidential information should not be placed into the subject line of the message.

Payment Card Information Classification and Control (6.2.3.5)

Payment card information must be considered confidential when an individual's first name or first initial and last name are present in combination with account number, credit or debit card number, required security code, access code, or password that would permit access to an individual's financial account.

https://www.pcisecuritystandards.org/pci_security/

The Payment Card Industry – Data Security Standards (PCI DSS) comprise a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector statutes and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional statutes, government regulations, or other legal requirements.

All payment card information stored and processed by the State, or transmitted over State networks must be in compliance with the PCI-DSS. Storage of the full Primary Account Number (PAN) on State systems is prohibited. Agencies that use payment card services should also comply with statewide accounting policies as documented by the Department of Finance and Administration, Division of Accounts.

All purchased (off the shelf) applications used to process payment card information must be compliant with the Payment Application Data Security Standard (PA-DSS).

Use of Confidential Data (6.2.3.6)

The use of confidential data will only be permitted in production systems. The use of confidential data is prohibited from training, test, and development systems.

To reduce the risk of accidental change or unauthorized access to operational software and business data, there should be a separation of duties based on development, test, and operational facilities. Confidential data should not be copied into test and development systems. Development and test environments should not be directly connected to production environments. Data and operational software test systems should emulate production systems as closely as possible.

Media Handling (6.3)

Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on media.

Management of Removable Media (6.3.1)

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

Repair of Removable Media (6.3.1.1)

Removable media should be sanitized prior to removing it from State facilities for maintenance or repair.

Disposal of Removable Media (6.3.2)

Removable media should be disposed of securely when no longer required, using approved State procedures.

Physical Transfer of Removable Media (6.3.3)

Removable media containing sensitive or confidential data must be protected against unauthorized access, misuse or corruption during transport.

Workstation Computing (6.4)

Objective: To prevent unauthorized disclosure, modification, removal or destruction of data stored on user assigned processing devices.

State Provided Workstation Computing Platforms (6.4.1)

Workstation computing platforms, including laptops should be physically protected against theft when left unattended. Workstation computing platforms should not store confidential data assets where it is not absolutely necessary to perform the specific job-related duties. Storage of confidential data assets on a workstation computing platform should have approval from the asset custodian for such storage. Confidential data assets which have been authorized to be stored on the local workstation should be encrypted while stored on the workstation computing platform.

Workstation Platform Reassignment (6.4.2)

All workstation computing platforms, including all external storage devices, should be sanitized prior to being re-issued or re-purposed to another employee or outsourced employee.

Workstation Platform Disposal (6.4.3)

Hard drives in workstation computing platforms, including all mobile storage devices and phones, should be sanitized using approved sanitization procedures or destroyed prior to transfer or surplus of processing device to non-State agencies.

Sanitization services provided by third parties must meet the State's media sanitization guidelines, and the provider should provide proof of sanitization.

Cloud Services (6.4.4)

Agencies and full- and part-time employees of the State of Tennessee and all third parties, outsourced employees, or vendors who are acting on behalf of the State who use cloud services for State business should seek STS guidance and approval for proposed cloud solutions prior to enabling cloud services.

Cloud Services Procurement (6.4.4.1)

Agencies that procure cloud services that host or process State data must include security language approved by the Department of General Services, Central Procurement Office. Agencies should use legally binding documents to procure those services.

https://www.teamtn.gov/cpo/resources.html

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas (7.1)

Objective: To prevent unauthorized physical access, damage and interference to the State's information and information processing facilities.

Physical Security Perimeter (7.1.1)

All enterprise data processing facilities that process or store data classified as critical or sensitive should have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All other processing facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.

Physical Entry Controls (7.1.2)

Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel.

Securing Offices, Rooms and Facilities (7.1.3)

Physical security for offices, rooms and facilities should be designed and applied commensurate with the classification and value of the data being handled or processed.

Protecting against External and Environmental Threats (7.1.4)

Physical protection against natural disaster, malicious attack or accidents should be considered and incorporated in facility design, construction and placement.

Working in Secure Areas (7.1.5)

Procedures for working in secure areas should be created and implemented.

Delivery and Loading Areas (7.1.6)

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities.

Equipment (7.2)

Objective: To prevent loss, damage, theft or compromise of assets or an interruption to State operations.

Equipment Siting and Protection (7.2.1)

Equipment should be located in secured areas or protected to reduce the risks from environment threats and hazards, and to reduce the opportunities for unauthorized access. Equipment located in areas where the State of Tennessee is unable to maintain a secure perimeter should be locked in a secured manner with access controlled by the State of Tennessee. Secured cabinets or facilities should support further segregation within the State of Tennessee's IT organization based on role and responsibility.

Supporting Utilities (7.2.2)

Infrastructure and related computing equipment should be protected from power failures and other disruptions by failures in supporting utilities.

Cabling Security (7.2.3)

Power and telecommunications cable carrying data or supporting information services should be protected from interception, interference or damage.

Equipment Maintenance (7.2.4)

Equipment should be correctly maintained to ensure its continued availability and integrity.

Removal of Assets (7.2.5)

All equipment, software or information that is a part of State operational systems or processes should not be taken off-site without the prior authorization from executive management or a designated representative and should be removed according to documented agency equipment transfer procedures.

Security of Equipment and Assets Off-Premises (7.2.6)

Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

Secure Disposal or Re-Use of Data Processing Equipment (7.2.7)

All data processing equipment including storage devices subject to transfer or reuse should be sanitized in accordance with the State of Tennessee's media reuse procedure or superseding state or federal requirements. Data processing equipment assets that are not subject to transfer or reuse should be destroyed in accordance with the State of Tennessee's media disposal procedures or in accordance with superseding state or federal requirements.

Unattended User Equipment (7.2.8)

Users should ensure that unattended data processing equipment has appropriate protection.

Session Time Outs (7.2.8.1)

All systems and devices owned and operated by or on behalf of the State of Tennessee should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

Clear Desk and Clear Screen Policy (7.2.9)

All data classified as confidential must be stored in a locked cabinet or room when unattended. All data processing equipment that provide access to Information Processing Systems will be configured so that a screen-saver, with password protection engaged, or other lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system will automatically be implemented if the system has been left unattended.

All computing platforms residing in non-secured facilities with attached displays should be oriented away from direct line of sight from unauthorized viewers.

MINIMUM COMPLIANCE REQUIREMENTS:

(7.2.8.1) Session Time Outs

Sessions will be configured to time out after 15 minutes of inactivity.

(7.2.9) Clear Screen Policy

Maximum inactivity interval for engaging screen-saver or other lockdown mechanism is 15 minutes.

8. NETWORK CONNECTIVITY SECURITY

Network Security Management (8.1)

Objective: To ensure the protection of the State's assets that are accessible by suppliers and vendors.

Network Controls (8.1.1)

Networks should be managed and controlled to protect information in systems and applications.

Security of Network Services (8.1.2)

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

Segregation in Networks (8.1.3)

All enterprise network architectures operated by, or on behalf of, the State of Tennessee should be designed to support, at a minimum, separate public, "demilitarized" and private security zones based on role, risk and sensitivity. Bridging between separate security zones is strictly prohibited. All access between separate security zones should be controlled by a security mechanism configured to deny all access by default unless explicitly authorized and approved by the EHI Security Management Team.

Information Transfer (8.2)

Objective: To maintain the security of information transferred within network infrastructures manage by on behalf of the State and with any external entity.

Information Transfer Policies and Procedures (8.2.1)

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Agreements on Data Transfer Policies (8.2.2)

Agreements should address the secure transfer of business information between the State and external parties.

Electronic Messaging (8.2.3)

Data involved in electronic messaging should be appropriately protected.

Internal Electronic Messages Control (8.2.3.1)

Email and instant messages internal to the State's domain containing confidential data should be encrypted during transmission. Confidential information should not be placed into the subject line of email or as any part of instant messages.

External Electronic Messages Control (8.2.3.2)

E-mail sent through the public Internet must be encrypted if it contains confidential information in the body or attachment of the email. Confidential information should not be placed into the subject line of the message.

Electronic Messaging Management (8.2.3.3)

All electronic messages created, sent or received in conjunction with the transaction of official business should use the State approved gateway(s) to communicate via the Internet.

Confidentiality or Non-Disclosure Agreements (8.2.4)

When exchanging or sharing information classified as "Sensitive" or "Confidential" with external parties that are not already bound by the contract confidentiality clause, a non-disclosure agreement should be established between the owner of the data and the external party.

Note: Agencies should work with agency legal counsel to ensure proper language is used.

9. MOBILE DEVICE SECURITY POLICY

Mobile Devices and Alternate Work Space (AWS) (9.1)

Objective: To extend the State's security posture to the mobile workforce.

Mobile Device Policy (9.1.1)

All mobile devices that connect to State of Tennessee managed data or infrastructure should be managed by the State's enterprise mobile device management solution or the State's enterprise configuration manager and should comply with appropriate mobile device usage policies as required by state or federal statute or regulation.

Alternate Work Space (9.1.2)

AWS workers should comply with the appropriate AWS policies as required by state or federal statute, regulation, or state or agency policy.

10. EXTERNAL PARTY SECURITY

Information Security for External Party Relationships (10.1)

Objective: To ensure the protection of the State's assets that are accessed, processed, communicated to, or managed by external parties, suppliers or vendors. This includes any external party who has access to physical data processing facilities, logical access to State data processing systems via local or remote access or access via another external party into the State's data processing facilities.

Information Security Policy for External Party Relationships (10.1.1)

Information and physical security requirements for mitigating the risks associated with supplier or vendor access to the State's assets should be agreed upon in writing with the external party. All external parties must agree in writing to comply with all applicable information security policies, confidentiality agreements, third party connectivity agreements, executive orders, standards, controls and regulations.

Identification of Risk (10.1.2)

Risk involving external parties should be identified and proper controls implemented prior to the granting of access to any State of Tennessee information, information technology asset or information process facility.

Addressing Security within External Party Agreements (10.1.3)

All relevant information security requirements should be established and agreed upon with each supplier or vendor that may access, process, store, communicate, or provide IT infrastructure components for the State's processing systems or infrastructure.

Reporting of Security Incidents (10.1.3.1)

External Party Agreements will require external parties to report known security incidents within twenty-four (24) hours that may impact the confidentiality, integrity or availability of State data.

Sub-Contractor Requirements (10.1.3.2)

Primary external parties should require their sub-contractors to abide by State of Tennessee policies and security requirements, as applicable.

Addressing Security for Access to Citizen Data (10.1.4)

Risk involving external party access to citizen data should be identified and proper controls implemented prior to the granting of access to any State of Tennessee citizen data. Appropriate controls should be agreed upon, documented in external party agreements and implemented prior to the granting of access to any citizen data.

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security Requirements of Information Systems (11.1)

Objective: To ensure that information security is an integral part of information systems throughout their life cycle. This includes application infrastructure, vendor applications, agency-developed, and user- developed applications and information systems which provide services over public networks or the State's internal network.

Security Requirements of Information Systems (11.1.1)

Security requirements should be identified and documented as part of the overall business case for new information systems and for enhancement to existing information systems and should be included early and continuously throughout the lifecycle of the application, including, but not limited to the conception, design, development, testing, implementation, maintenance and disposal phases.

Securing Application Services on Public Networks (11.1.2)

Information involved in application services passing over public networks should be protected from fraudulent activity and unauthorized disclosure or modification.

Protecting Application Services Transactions (11.1.3)

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Information Security in Project Management (11.1.4)

Information security should be addressed at project initiation and throughout the lifecycle of the project.

Security in Development and Support Processes (11.2)

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

Security Requirements of Information Systems (11.2.1)

Requirements, rules and guidelines for the development of software and systems should be established and applied to all systems development.

Security in Application Systems Development (11.2.1.1)

Input validation, authentication, and authorization should be included in the design, development and implementation of applications.

Input and Data Validation (11.2.1.2)

Applications should not pass raw input to other processes including, but not limited to, other applications, web services, application server and databases. Applications should use parameterized queries or stored procedures, not dynamic SQL statements.

Output Data Validation (11.2.1.3)

Applications should not echo input back to the user or disclose information about the underlying system through error messages.

Application Authorization (11.2.1.4)

Applications that provide access to information in databases or from network shares should perform user authentication.

Inter-process Message Authentication (11.2.1.5)

Inter-process message authentication should be used to verify that a message originated from a trusted source and that the message has not been altered during transmission.

Control of Internal Processing (11.2.1.6)

Security controls should be included to prevent corruption due to processing errors or deliberate acts.

Change Control Procedures (11.2.2)

Changes to systems or applications within the development lifecycle should be controlled by the use of formal change control procedures.

Technical Review of Applications after Operating Platform Changes (11.2.3)

When operating platforms or applications are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Restrictions or Changes to Software Packages (11.2.4)

Modifications to software packages should be limited to necessary changes, and all changes should be strictly controlled.

Secure System Engineering Principles (11.2.5)

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Secure Development Environment (11.2.6)

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development (11.2.7)

Outsourced system development should be monitored and supervised to ensure the State's policies and practices are followed and to ensure appropriate security controls are in place.

System Security Testing (11.2.8)

Testing of security functionality should be carried out during development. Applications should be tested periodically throughout their respective lifecycles, at each major version release and prior to assigning public IP addresses or being moved or promoted into the production environment.

System Acceptance Testing (11.2.9)

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

Test Data (11.3)

Objective: To ensure the protection of the data used for testing.

Protection of Test Data (11.3.1)

Test data should be selected carefully, protected and controlled. The use of production data for development and testing is prohibited.

12. BUSINESS CONTINUITY MANAGEMENT

Information Business Continuity (12.1)

Objective: To ensure the availability of critical systems and infrastructure and the continued ability to provide services in the event of a crisis or disaster.

Planning Information Systems Continuity (12.1.1)

All State agencies should determine their requirements for the continuity of information management systems in adverse situations, e.g. during a crisis or disaster.

Business Impact Analysis (12.1.1.1)

All State agencies should perform a Business Impact Analysis (BIA) to identify systems and infrastructure that are critical to State operations and services to citizens, other agencies and regulatory bodies.

Critical Applications (12.1.1.2)

Systems including Infrastructure components, applications and security systems identified as critical in the BIA will be recovered in accordance with the Business Impact Analysis and documented system recovery strategy.

Non-Critical Applications (12.1.1.3)

Infrastructure components and applications identified as non-critical in the BIA will be recovered on a best–effort basis. The components and applications listed as non-critical should have an explanation in the BIA justifying their low importance and demonstrating how the loss of their associated functionality will be acceptable during an event or how a manual workaround can be implemented.

Implementing Information Systems Continuity (12.1.2)

All State agencies should establish, document, implement, and maintain processes, procedures and controls in disaster recovery plans to ensure the required level of business continuity for all systems during an adverse situation.

13. INFORMATION SECURITY INCIDENT MANAGEMENT

Management of Information Security Incidents and Improvements (13.1)

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Responsibilities and Procedures (13.1.1)

The State of Tennessee will establish a Security Incident Response Team (SIRT). The SIRT will ensure that the State of Tennessee can efficiently and effectively communicate information security incidents to the proper stakeholders and respondents of the State. The SIRT members will be appointed based on their position and capabilities within the organization. Each agency should designate an information security "point of contact" (POC), in accordance with the Information Systems Council's "Information Resource Policies" requirements. This POC will act as the central communications figure regarding security incidents within the agency. The POC will have responsibility for incident escalations, actions and authority for the administrative oversight of security for the IT resources under the agency's control. The POC within each agency will participate as a member of the SIRT. The CISO of the State of Tennessee will appoint members from within STS to participate in the SIRT.

Reporting Information Security Events (13.1.2)

Information security events should be reported through appropriate channels using the State of Tennessee Cyber Incident Response Plan (CIRP).

Data Breach and Disclosure (13.1.2.1)

Any State of Tennessee agency that discovers a breach of the information security controls set forth in this document which results in disclosure of unencrypted "personal information" about persons to unauthorized third parties must provide notice of the disclosure in accordance with TCA 47-18-2107 or any other applicable state and/or federal statute or regulations).

Reporting Information Security Weakness (13.1.3)

Employees and outsourced employees using the State's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to the STS Customer Care Center.

Assessment of and Decision on Information Security Events (13.1.4)

Information security events should be assessed and a determination made on whether to classify the event as an incident in accordance with the CIRP.

Response to Information Security Incidents (13.1.5)

Information security incidents will be managed in accordance with the documented procedures in the State of Tennessee Incident Response, Alerting and Communications Plan.

Learning from Information Security Incidents (13.1.6)

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Collection of Evidence (13.1.7)

EHI should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

14. CRYPTOGRAPHY

Cryptographic Controls (14.1)

Objective: To ensure proper and effective use of cryptography to protect the confidentiality and integrity of data owned or managed by or on behalf of the State. Confidential information must be encrypted by the use of valid encryption processes for data at rest and in motion as required by state or federal statute or regulation. This includes but is not limited to sensitive information stored on mobile devices, removable drives and laptop computers.

Use of Cryptographic Controls (14.1.1)

Cryptographic controls should be based on the classification and criticality of the data. In deciding what strength and type of control to be deployed, both stand- alone and enterprise level encryption solutions should be considered. Attention should be given to regulations, national restrictions (e.g. export controls) that may apply to the use of cryptographic techniques.

Transmission Integrity (14.1.2)

Information systems should protect the integrity of transmitted information traveling across both internal and external communications. This control applies to communications across internal and external networks.

Transmission Confidentiality (14.1.3)

Information systems should protect the confidentiality of transmitted information. The State will employ mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

Cryptographic Module Authentication (14.1.4)

Information systems must use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal statutes, state statutes, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. The list of cryptographic modules in use will be compared to the list of NIST validated cryptographic modules quarterly to ensure compliance.

Cryptographic Module Authentication (14.1.5)

Information systems will obtain and issue supported public key and Transport Layer Security (TLS) certificates from an approved service provider. This control focuses certificates with visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services. Secure Socket Layer (SSL) protocol must be disabled on all devices.

Wildcard Certificates (14.1.5.1)

Wildcard certificates used for Internet facing systems must be approved by the EHI Office of the CISO

Key Management (14.1.6)

A secured environment should be established to protect the cryptographic keys used to encrypt and decrypt information. Cryptographic key management and establishment will be performed using automated mechanisms with supporting manual procedures. Keys should be securely distributed and stored. Access to keys should be restricted only to individuals who have a business need to access them. All access to cryptographic keys requires authorization and should be documented. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

15. COMPLIANCE

Compliance with Legal and Contractual Requirements (15.1) Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Identification of Applicable Legislation and Contractual Requirements (15.1.1)

All relevant legislative, statutory, regulatory, contractual requirements and the State's approach to meet these requirements should be explicitly identified, documented and kept current for each information system, each agency and each entity that stores, processes or transmits data on behalf of the State.

Intellectual Property Rights (15.1.2)

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and the use of proprietary software products.

Protection of Records (15.1.3)

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with state or federal statutory, regulatory, contractual and business requirements.

Privacy and Protection of Personally Identifiable Information (15.1.4)

The privacy and protection of personally identifiable information should be ensured as required by relevant federal or state statute or regulation.

Regulation of Cryptographic Controls (15.1.5)

Cryptographic controls should be used in compliance with state or federal statutory, regulatory, contractual and business requirements.

Information Security Reviews (15.2)

Objective: To ensure that information security is implemented and operated in accordance the organizational policies and procedures.

Independent Review of Information Security (15.2.1)

The State's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently and at planned intervals or when significant changes occur.

Risk Assessment (15.2.1.1)

A Risk Assessment of the State environments where servers reside that process State data will be performed within every 365 days.

Compliance with Security Policies and Standards (15.2.2)

Managers should regularly review the compliance of information processing and procedures within their area of responsibility for accuracy and applicability with the appropriate security policies, standards and any other security requirements.

Technical Compliance Review (15.2.3)

Information systems should be regularly reviewed for compliance with the State's information security policies and standards.

16. HUMAN RESOURCE

Prior to Employment (16.1)

Objective: To ensure all full- and part-time employees of the State of Tennessee and all third parties, outsourced employees, or vendors understand their responsibilities in regard to information security requirements for the State of Tennessee's computing environments.

Screening (16.1.1)

Background and verification checks on all candidates for employment should be conducted in accordance with relevant statutes and published state policies.

Acceptable Use Policy (16.1.2)

All agencies should ensure that their full- and part-time employees of the State of Tennessee and all third parties, outsourced employees, or vendors who use State of Tennessee's IT resources have read and accept the terms of the relevant State's Acceptable Use Policies. Proof of employee acceptance and acknowledgement will be maintained by the agency.

During Employment (16.2)

Objective: To ensure employees and outsourced employees are aware of and fulfill their information security responsibilities.

Management Responsibilities (16.2.1)

Management should ensure that all employees and outsourced employees are aware of and fulfill their information security responsibilities.

Information Security Awareness, Education and Training (16.2.2)

All non-Executive Branch State employees who have access to State systems and where relevant, outsourced employees should utilize State-provided security awareness education and training when first employed and at least bi-annually thereafter.

All Executive Branch State employees who have access to State systems and, where relevant, outsourced employees should utilize State-provided security awareness education and training when first employed and within every 365 days thereafter.

17. VERSION HISTORY

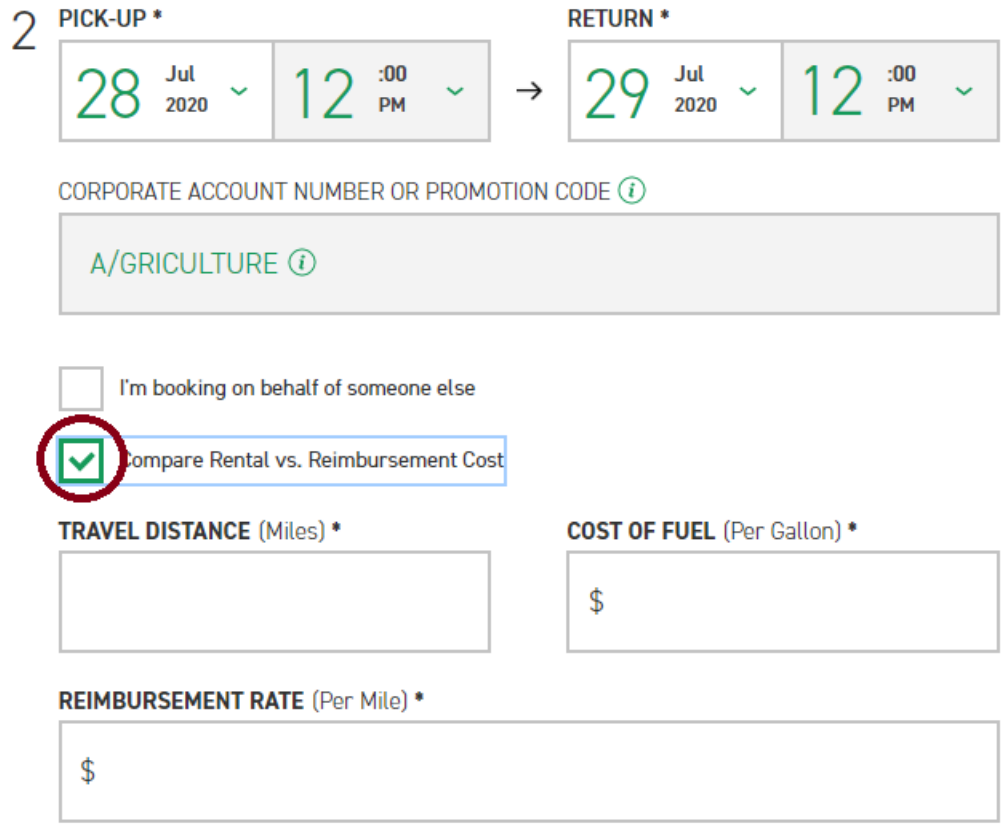
Version 2.1 – December 15, 2016	*Converted Office for Information Resources to Strategic Technology Solutions. Updated policy link in 2.4 Made agency specific policies mandatory for agency specific requirements in 3.1.2. Minor wording changes to sections 13.1.1 and 13.1.2. Updated technology requirement for encryption in 14.1.5. Aligned training periodicity with ISC vote in 16.2.2.*
Version 2.2 – December 14, 2017	*Updated policy link in 2.4*
Version 2.3 – December 21, 2018	*Inserted language regarding cloud technologies and contractor hosted solutions in Executive Summary, Introduction and Scope. Converted Security Advisory Council to STS Executive Management Team. Combined 3.1.3 into 3.1.1 and clarified 3.1.2. Updated link in 6.2.3.5 and corrected numbering throughout 6.2.3. Added Cloud Services Procurement 6.4.4.1. Differentiated training requirements between Executive Branch and non-Executive Branch in 16.2.2. Added Risk Assessments 15.2.1.1. Change annual reviews to within review within 365 days throughout document.*
Version 2.4 – January 29, 2020	*Removed "Confidential" status from the policy. Adjusted terminology throughout policy to align with ISC policies and AUPs, Adjusted references. Converted ELT to Policy Review Committee in Review (2.4). Adjusted patch schedule in Patch Management (4.5.1.1) and added section Software Maintenance (4.5.1.2). Added sections System/Application Account Use (5.4.2.4) and System Administrator Account Use (5.4.2.5) adjusted associated minimum requirements, Added language to Removal or Adjustment of Access Rights (5.2.6). Added F&A policy reference to Inventory of Assets (6.1.1). Added PA-DSS requirement to Payment Card Information Classification and Control (6.2.3.5). Added language to Workstation Platform Disposal (6.4.3). Adjusted sections throughout 12. BUSINESS CONTINUITY MANAGEMENT to align with ISC Policy 9, Added section Wildcard Certificates (14.1.15.1). Removed appendices. Removed Terms and Conditions.*

Policy Name	Document Ref # 300-POL-001	
Enterprise Information Security Policies	**Version #**	2.4
	Signed	Stephanie Dedmon
	Signed	Feb 1, 2020 Stephanie Dedmon (Feb 1, 2020) Jan 29, 2020 Curtis Clan (Jan 29, 2020)
	Approval Date	1/29/2020
	Implementation Date	2/01/2020
	Last Reviewed by Policy Review Committee	12/09/2019

Enterprise Rent-a-Car – Comparing Mileage Reimbursement Cost:

- **To compare the cost of renting to reimbursing mileage**→
  - Choose the "Enterprise Rent-A-Car OFFICIAL STATE BUSINESS DIRECT BILL ONLY option
  - Choose your agency
  - On the first booking page, underneath the "Corporate Account Number" section, enter in your trip's anticipated distance, the local cost of fuel (estimate), and the rate of reimbursement
    - Continue, filling in your rental reservation as needed
  - On the last page prior to confirming your reservation, you will see the cost difference between renting and paying mileage on the **bottom left-hand pane**

NOTE **UNCHECK** the "Compare Rental vs. Reimbursement Cost" box to continue without the comparing mileage reimbursement cost.



- For **personal-use trips**, select **Personal Use Customer Pay**
  - NOTE: These rentals will require your personal credit card and will not be billed to your department; discounted rates do apply
  - Normal taxes, fees, and surcharges will apply

Enterprise Rent-a-Car – FREE PICKUP SERVICE (non-airport location rentals only):

- To request Enterprise's **free pickup service**→
  - make your reservation online, then
  - call the branch directly to schedule your ride.
    - NOTE – press * when the playback message starts, and you will be sent directly thru to the branch line.
    - NOTE – as a general rule of thumb, Enterprise branches offer free pickup service to customers who are within a 10-mile radius of the location. Call the desired branch to confirm pickup availability and protocol.

LOCAL

ENTERPRISE TRUCK RENTAL

For either **official approved business trips** select **Enterprise Truck Rental** for **Commercial Trucks** and **Vehicles**

AIRPORTS

NATIONAL CAR RENTAL

For **official approved business trips**, select **Airport OFFICIAL STATE BUSINESS**

- Select your Department
- Enter city or airport in "Pickup Location"
- Enter "Pickup" and "Return" dates and times
- Optional: Enter "Last Name" and "Emerald Club Number"
  - To obtain your membership information, contact the Enterprise representative listed above
  - If you have forgotten your membership information, click on the blue link "Forgot your info?" and follow the instructions
- Click green "Start Reservation" button
- Select your vehicle from the provided list of available vehicles
  - Refer to Attachment A SWC 205 Vehicle Rental Pricing for the list of available vehicles under this Contract
  - Click green "Select" button under the selected vehicle
- Unless instructed by your Agency, do not select any "Optional Items" that appear on the next screen. Click the green "Continue" button.
  - Sales Tax will appear while making a reservation but will not be applied to any rentals that originate in Tennessee (rentals originating outside of Tennessee will have tax applied)
- Review the reservation information on the next screen
  - Provide your contact information in "Driver Information"

        - Provide your employment information in “Manager/Supervisor Authorizing Travel” and “Speed Chart” (if you do not know your speed chart number, contact your department’s fiscal office)
        - NOTE: Your supervisor will receive confirmation of your reservation
        - Optional: Provide your flight information under “Frequent Traveler”
    - Click the green “Reserve” button
    - The next screen will display the reservation information
        - Make note of your rental confirmation number
        - You can print this page or refer to the confirmation email

- For **personal-use trips**, select **Personal Use Customer Pay**
    - NOTE: These rentals will require your personal credit card and will not be billed to your department; discounted rates do apply
    - Normal taxes, fees, and surcharges will apply

REQUISITION AND PURCHASE ORDER GENERATION:

For information on how to create a requisition and/or purchase order please use the "Guide to Agency Purchasing" document in Edison under the Procurement Tab, Procurement Information box. For webinars and job aids on requisitions and purchase orders, please visit the CPO Intranet Training page at http://intranet.state.tn.us/generalserv/cpo/cpotraining.html.

BILLING AND PAYMENT INSTRUCTIONS:

The Contractor shall submit an itemized invoice, with all necessary supporting documentation, to the reserving agency's fiscal personnel. Purchase Orders to Enterprise will be issued after receipt of the invoice which may occur after the rental has taken place.

Enterprise will not charge the State any sales & use tax for rentals that originate at a Tennessee Enterprise location, however there are applicable Surcharges and Fees that may be charged to the users under this Contract. These charges may appear on the invoice as a "tax". If you have questions about any of these charges, please contact the Contract Administrator. A list of the Surcharges and Fees can be found in Attachment A SWC 205 Vehicle Rental Pricing or in Edison.

It is the responsibility of the agency to notify the Contractor in the event the contact person at the agency changes. All Enterprise invoices will be directed to the main contact person identified by each agency's fiscal office.

MISCELLANEOUS INFORMATION:

1. Should the State employee become involved in an accident, theft, or incur any other damage to the vehicle during the rental, they are responsible for reporting the incident to Enterprise immediately.

2. Upon arrival at the Enterprise or National branch location to pick-up a reserved vehicle, the State employee must present a State issued driver's license and authorization from their department to proceed with the rental. The State employee will be required to sign a standard rental agreement. Please sign this agreement; the terms of this statewide contract will govern in the event of any conflicts between the agreement and this Contract.

3. All vehicles must be re-fueled by the State employee prior to return of the vehicle. The vehicle must be at the same or greater fuel level it was at when picked up. This rule applies to all vehicle categories (Traditional, Commercial).
   a) Traditional Vehicles: you must re-fuel the vehicle using your personal credit card and request reimbursement
   b) Commercial Vehicles: you must re-fuel the vehicle using your personal credit card and request reimbursement

4. All State employees can become a member of the Enterprise loyalty program, Emerald Club, which provides special privileges to renters. More information can be found on the Enterprise website: https://www.nationalcar.com/en_US/car-rental/loyalty/enrollment/benefits.html

5. The following items are NOT permitted in any State of Tennessee vehicle rented for business use: a.
   a) Animals
   b) Non-State employees
   c) Weapons
   d) Smoking

6. Should the State employee receive a traffic violation while using a rental vehicle, the employee will be responsible for paying the violation. Notification of the violation will be sent to the department's contact person. Contact your department's fiscal office for more information on how this process is managed.

7. If a rental lasts longer than 30 days, you must contact the Enterprise or National rental location in which the vehicle originated and report the mileage. This must be done every 30 days until the vehicle is returned. No vehicle rental can last longer than 6 months.

8. Rented vehicles for business use must not be taken outside of the continental United States. Travel to Mexico or Canada is strictly prohibited.

HOW TO ENROLL (LOYALTY PROGRAMS)

NATIONAL & ENTERPRISE

EMERALD CLUB

Enroll here: https://www.nationalcar.com/en/emerald-club/enroll.html
Earn benefits at both National Car Rental & Enterprise Rent-A-Car.

- At National, members are eligible for counter-bypass and their own choice of vehicle from the corresponding aisle. *Reserve* the Emerald Aisle and pay the mid-size car price. *Rent* from the Emerald Aisle and choose any car on the Aisle (mid-size or larger)!
- At Enterprise, free pickup services (non-airport) and fast-track your checkout process

ENTERPRISE ONLY

ENTERPRISE PLUS

Enroll here: https://www.enterprise.com/en/enroll.html
Earn benefits at Enterprise Rent-A-Car

- At Enterprise, earn points towards free rental days and fast-track your checkout process

FREQUENTLY ASKED QUESTIONS

Who can book reservations?

- All State of Tennessee employees — Full- and part-time State employees, City and County employees, and students of state colleges and universities conducting business on behalf of the state entity (with department approval).
- Personal rentals are also available but do not include coverages and require personal method of payment.

How should a renter choose between brands?

- Use the Enterprise brand when renting off or on-airport locations when renting traditional passenger vehicles. When in need of commercial trucks, utilize Enterprise Truck Rental
- Use the National brand when renting at the airport

What loyalty program do I enroll in?

- Emerald Club is the loyalty program that works at both Enterprise and National, providing renters with exclusive benefits and privileges to make renting faster and easier for both brands via personal profiles, stored method of payment, rental preferences, etc.
- At most major North American National airport locations, members with a midsize car reservation can bypass the rental counter and proceed to the Emerald Club Aisle. There they may simply take any vehicle— midsize or larger.
- Regardless of the vehicle selected in the Emerald Aisle, a member is charged only the midsize rate.
- Status match to competitor loyalty programs.
- Accrue free rental days with National.
- Earn Emerald Club reward at Enterprise.
- Enroll now: https://www.nationalcar.com/offer/XZ56801

What are the benefits of booking with National Car Rental and Enterprise Rent-A-Car?

- Special negotiated rates for all car classes
- Damage Waiver & Liability coverage included on all business-use rentals
- 24/7 Roadside Assistance
- Complimentary Emerald Club membership access
- Award-winning customer service
- Singular Account Number for both brands
- Enterprise Holdings (Enterprise + National) boasts the most coverage of any rental car company in the world; Enterprise locations are within 15 miles of 90% of the U.S. population

What payment method should I use for business travel?

- Utilize your department's Direct Bill option or a department-approved State P-Card for business-use transactions
    - Your department's Billing Number information can be accessed by contacting your contract administrator
    - If your agency does not have a Billing Number and would like the Direct Bill option, please contact our Enterprise contact, Jonathan Peters at jonathan.e.peters@ehi.com
- Renters must use their own personal payment method for all personal-use rentals
    - Be sure to reference Account Number XZ56TNP for personal-use rentals

Does my negotiated rate include insurance coverage?

- Business Rentals include Damage Waiver (DW) and third-party liability protection.
- DW relieves eligible renters and authorized drivers from financial responsibility for loss of or damage to the rental vehicle.
- Liability protection covers the renter and authorized drivers against claims (e.g., property damage, bodily injury, etc.) brought by third parties.
- Note that the DW is subject to the terms and conditions of the applicable rental agreement.

What if I need a one-way rental?

- Check the "return to a different location" box when booking
- One-way rentals within the State of Tennessee will have no fees associated
- One-way rentals outside of the State of Tennessee will be subject to a $0.40/mile charge

What if I need delivery and collection?

- With minimal time restraints, the Enterprise "We'll Pick You Up" service is available to our customers. With a 24-hour notice, we will pick up an employee at any home or business address. Depending upon seasonal and business demands, this 24-hour notice might be reduced. Our local Enterprise branch will work closely with you to meet all your pick-up needs.
- In certain situations, Enterprise locations can deliver vehicles to a business address. We will require a 24-hour notice; the notice may increase during peak travel seasons. The local Enterprise branch will work closely with you to meet your delivery needs.

How far in advance should I make my reservation to ensure a rental?

- We recommend customers reserve a vehicle with their Account Number and Emerald Club member number at least 24 hours in advance.
- Specialty vehicles or vehicles rented within peak times may require more notice.

What if I need a rental before the rental location opens?

- Schedule the reservation for pick-up the evening before or at a location that has longer hours (often airport locations are open longer)
- Rates are calculated on a 24-hour period, beginning with the pickup time and ending when the vehicle is returned

What locations are available in the State of Tennessee?

- Enterprise and National have a vast network of airport and home-city locations to handle all your car rental needs.
- Please refer to the following pages to find us in your neighborhood.
    - Enterprise Rent-A-Car locations and hours of operations:
        - https://www.enterprise.com/en/car-rental/locations/us/tn.html
    - Enterprise Truck Rental locations and hours of operations:
        - https://www.enterprisetrucks.com/truckrental/en_US/locations.html
    - National Car Rental locations and hours of operations:
        - https://www.nationalcar.com/en/car-rental/locations/us.html

Enterprise Contact Information

- Enterprise Customer Service: 1-800-264-6350
- Enterprise General Reservations: 1-855-266-9289

National Contact Information

- National Customer Service: 1-800-227-7368
- National General Reservations: 1-844-382-6875

- Emerald Club Member Services: 800-962-7070
- Monday through Friday, 9 a.m. to 6 p.m. EST

For other questions, travelers should contact your in-house travel administrator.

24/7 Roadside Assistance

1-800-367-6767

SWC #205 Vehicle Rental

Traditional & Commercial Vehicle Rental Rates - Leisure Use*

*Leisure Usage rates do not include insurance

Compact Sedan

Enterprise Classification:	Specifications:
CCAR	2 or 4 doors, Automatic Transmission, Air Conditioning, AM/FM CD Player
Nissan Versa, Toyota Yaris, or similar	

Description	UOM	Contract Rate
Traditional - Compact Sedan, Hourly	HR	$ 8.37
Traditional - Compact Sedan, Daily	DA	$ 27.09
Traditional - Compact Sedan, Weekly	WK	$ 162.35
Traditional - Compact Sedan, Monthly	MO	$ 616.64

Intermediate/Mid-Size Sedan

Enterprise Classification:	Specifications:
ICAR	2 or 4 doors, Automatic Transmission, Air Conditioning, AM/FM CD Player
Toyota Corolla, Dodge Caliber, or similar	

Description	UOM	Contract Rate
Traditional - Intermediate/Mid-Size Sedan, Hourly	HR	$ 9.95
Traditional - Intermediate/Mid-Size Sedan, Daily	DA	$ 29.86
Traditional - Intermediate/Mid-Size Sedan, Weekly	WK	$ 179.16
Traditional - Intermediate/Mid-Size Sedan, Monthly	MO	$ 716.64

Full-Size Sedan

Enterprise Classification:	Specifications:
FCAR	4 doors, Automatic Transmission, Air Conditioning, AM/FM CD Player
Chevrolet Impala, Nissan Altima, or similar	

Description	UOM	Contract Rate
Traditional - Full-Size Sedan, Hourly	HR	$ 10.28
Traditional - Full-Size Sedan, Daily	DA	$ 30.85
Traditional - Full-Size Sedan, Weekly	WK	$ 185.10
Traditional - Full-Size Sedan, Monthly	MO	$ 740.40

Intermediate Sport Utility Vehicle (SUV)

Enterprise Classification:	Specifications:
IFAR/SFAR	Room to seat 5 Passengers, Automatic Transmission, AC, AM/FM CD Player, Power windows and power locks
Toyota RAV4, Nissan Pathfinder, or similar	

Description	UOM	Contract Rate
Traditional - Mid-Size SUV, Hourly	HR	$ 15.57
Traditional - Mid-Size SUV, Daily	DA	$ 46.70
Traditional - Mid-Size SUV, Weekly	WK	$ 280.20
Traditional - Mid-Size SUV, Monthly	MO	$ 1,120.80

1/2 Ton Pick-Up Truck

Enterprise Classification:	Specifications:
PPAR	Power Windows/Locks, Automatic Transmission, Cruise control, Crew Cab & Extended Cab, Seat 6, Air Conditioning, Power Steering
Ford F150, Chevrolet Silverado, Dodge Ram 1500, or similar	

Description	UOM	Contract Rate
Traditional - 1/2 Ton Pick-Up Truck, Hourly	HR	$ 12.65
Traditional - 1/2 Ton Pick-Up Truck, Daily	DA	$ 38.35
Traditional - 1/2 Ton Pick-Up Truck, Weekly	WK	$ 230.00
Traditional - 1/2 Ton Pick-Up Truck, Monthly	MO	$ 917.06

3/4 Ton Pick-Up Truck

Enterprise Classification:	Specifications:
OQAR	Tow Capable, Payload up to 9,000 lbs, 4 Wheel Drive, Power Windows/Locks, Automatic Transmission, Cruise control, Crew Cab, Seat 6 Air Condition, Power Steering
Ford F250, Chevrolet 2500, Dodge Ram 2500, or similar	

Description		UOM	Contract Rate
Traditional - 3/4 Ton Pick-Up Truck, Hourly		HR	$ 16.79
Traditional - 3/4 Ton Pick-Up Truck, Daily		DA	$ 50.88
Traditional - 3/4 Ton Pick-Up Truck, Weekly		WK	$ 231.00
Traditional - 3/4 Ton Pick-Up Truck, Monthly		MO	$ 840.00

16' Box Truck with Ramp

Enterprise Classification:	Specifications:
DBOX	Payload capable 5,500 lbs, Seats 3, Roll up cargo door, 2 Rows E-Trac for securing load, 4 Rows Wood slats for securing load, Automatic Transmission, Air Conditioning, Power Steering, Cruise control
Mitsubishi FE, Isuzu NPR, or similar	

Description	UOM	Contract Rate
Traditional - 16' Box Truck with Ramp, Hourly	HR	$ 24.73
Traditional - 16' Box Truck with Ramp, Daily	DA	$ 74.93
Traditional - 16' Box Truck with Ramp, Weekly	WK	$ 329.62
Traditional - 16' Box Truck with Ramp, Monthly	MO	$ 1,189.57

16' Box Truck with Lift Gate

Enterprise Classification:	Specifications:
DBOX	Lift Gate, Payload capable 5,500 lbs, Seats 3, Roll up cargo door, 2 Rows E-Trac for securing load, 4 Rows Wood slats for securing load, Automatic Transmission, Air Conditioning, Power Steering, Cruise control
Mitsubishi FE, Isuzu NPR, or similar	

Description	UOM	Contract Rate
Traditional - 16' Box Truck with Lift Gate, Hourly	HR	$ 24.73
Traditional - 16' Box Truck with Lift Gate, Daily	DA	$ 74.93

Traditional - 16' Box Truck with Lift Gate, Weekly	WK	$	329.62
Traditional - 16' Box Truck with Lift Gate, Monthly	MO	$	1,189.57

Large Sport Utility Vehicle (SUV)

Enterprise Classification:	Specifications:
FFAR	Room to seat 7 passengers, V8 engine, Air conditioning, Premium audio system with AM/FM/CD, Cruise control,Power windows and remote power locks
Chevy Tahoe, Ford Expedition, or similar	

Description	UOM	Contract Rate
Traditional - Large SUV, Hourly	HR	$ 24.07
Traditional - Large SUV, Daily	DA	$ 72.20
Traditional - Large SUV, Weekly	WK	$ 433.26
Traditional - Large SUV, Monthly	MO	$ 1,733.04

24' Box Truck with Lift Gate

Enterprise Classification:	Specifications:
GBOX	Lift Gate, Dock High, Payload 10,000 lbs, Seats 3, 2 Rows E-Trac for securing load, 5 Rows Wood Slats for securing load, Automatic Transmission, Air Conditioning, Power Steering, Driver Air-Ride Seat, Cruise Control
International Freightliner Hino, or similar	

Description	UOM	Contract Rate
Traditional - 24' Box Truck with Lift Gate, Hourly	HR	$ 26.43
Traditional - 24' Box Truck with Lift Gate, Daily	DA	$ 80.08
Traditional - 24' Box Truck with Lift Gate, Weekly	WK	$ 457.68
Traditional - 24' Box Truck with Lift Gate, Monthly	MO	$ 1,474.15

Minivan

Enterprise Classification:	Specifications:
MVAR	Room to seat 7 passengers, Automatic Transmission, Air Conditioning, AM/FM CD Player, 6-Cylinder Performance, Tilt/Cruise Control
Dodge Grand Caravan, Chrysler Town & Country, or similar	

Description	UOM	Contract Rate
Traditional - Minivan, Hourly	HR	$ 15.91
Traditional - Minivan, Daily	DA	$ 47.73
Traditional - Minivan, Weekly	WK	$ 286.38
Traditional - Minivan, Monthly	MO	$ 1,145.52

Cargo Van

Enterprise Classification:	Specifications:
RKAR	Tow Capable, Payload Capacity 3,000 lbs, Automatic Transmission, Seats 2, Air Conditioning, Standard Wheel Base & Long Wheel Base options, Power Steering
Ford Econoline E250, Chevrolet Express E2500, or similar	

Description	UOM	Contract Rate
Traditional - Cargo Van, Hourly	HR	$ 13.50
Traditional - Cargo Van, Daily	DA	$ 40.91
Traditional - Cargo Van, Weekly	WK	$ 203.35
Traditional - Cargo Van, Monthly	MO	$ 794.79

Passenger Van

Enterprise Classification:	Specifications:
FVAR	Front and Rear Air conditioning, AM/FM and CD player, Cruise control, V-8 Performance, Remote power locks, Power windows, Privacy glass, 15 passenger seating
Chevrolet Express, Ford Econoline or similar	

Description	UOM	Contract Rate
Traditional - Passenger Van, Hourly	HR	$ 25.18
Traditional - Passenger Van, Daily	DA	$ 75.54
Traditional - Passenger Van, Weekly	WK	$ 453.24
Traditional - Passenger Van, Monthly	MO	$ 1,812.96

1 Ton Pick-Up Truck

Enterprise Classification:	Specifications:
UPAR/UQAR	Tow Capable, Payload up to 9,000 lbs, 4 Wheel Drive, Power Windows/Locks, Automatic Transmission, Cruise control, Crew Cab, Seat 6 Air Condition, Power Steering, Diesel Engine, Bumber or Gooseneck Hitch, Dual Rear Wheel
Ford F350, Chevrolet 3500, Dodge Ram 3500, or similar	

Description	Item ID	UOM	Contract Rate
Traditional - 1 Ton Pick-Up Truck, Hourly	1000194144	HR	$ 30.00
Traditional - 1 Ton Pick-Up Truck, Daily	1000194145	DA	$ 90.00
Traditional - 1 Ton Pick-Up Truck, Weekly	1000194146	WK	$ 484.00
Traditional - 1 Ton Pick-Up Truck, Monthly	1000194147	MO	$ 1,091.67

AMENDMENT ONE
OF CONTRACT 65939

This Amendment is made and entered by and between the State of Tennessee, Department of General Services, hereinafter referred to as the "State" and EAN Holdings, LLC, hereinafter referred to as the "Contractor." For good and valuable consideration, the sufficiency of which is hereby acknowledged, it is mutually understood and agreed by and between said, undersigned contracting parties that the subject contract is hereby amended as follows:

1. Contract section E.10 Statewide Contract is deleted in its entirety and replaced with the following:

E. 10. Statewide Contract. This Contract establishes a source or sources of supply for all Tennessee State Agencies. "Tennessee State Agency" refers to the various departments, institutions, boards, commissions, and agencies of the executive branch of government of the State of Tennessee with exceptions as addressed in Tenn. Comp. R. & Regs. 0690-03-01-.01. The Contractor shall provide all goods or services and deliverables as required by this Contract to all Tennessee State Agencies. The Contractor shall make this Contract available to the following entities who are authorized to and who may purchase off of this Statewide Contract ("Authorized Users"):

a. all Tennessee State governmental entities (this includes the legislative branch; judicial branch; and, commissions and boards of the State outside of the executive branch of government);
b. Tennessee local governmental agencies;
c. members of the University of Tennessee or Tennessee Board of Regents systems;
d. any private nonprofit institution of higher education chartered in Tennessee; and,
e. any corporation which is exempted from taxation under 26 U.S.C. Section 501(c) (3), as amended, and which contracts with the Department of Mental Health and Substance Abuse to provide services to the public (Tenn. Code Ann. § 33-2-1001).
f. National Guard service members on Federal orders performing work on behalf of the State of Tennessee Emergency Management Agency. The State may purchase directly for these National Guard service members or in accordance with any applicable guidance.

These Authorized Users may utilize this Contract by purchasing directly from the Contractor according to their own procurement policies and procedures. The State is not responsible or liable for the transactions between the Contractor and Authorized Users.

Required Approvals. The State is not bound by this Amendment until it is signed by the contract parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this contract, said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).

Amendment Effective Date. The revisions set forth herein shall be effective upon all necessary approvals. All other terms and conditions of this Contract not expressly amended herein shall remain in full force and effect.

IN WITNESS WHEREOF,

EAN Holdings, LLC:

	9/11/20
SIGNATURE	**DATE**

Mike Long Vice President of Finance

PRINTED NAME AND TITLE OF SIGNATORY (above)

CENTRAL PROCUREMENT OFFICE

STATE OF TENNESSEE, DEPARTMENT OF GENERAL SERVICES:

8/21/2020

MICHAEL F. PERRY, CHIEF PROCUREMENT OFFICER **DATE**

Memorandum of Understanding #1
For Statewide Contract #205
Edison Contract # 65939

This Memorandum of Understanding ("MOU") is made and entered by and between the State of Tennessee, Department of General Services, Central Procurement Office, hereinafter referred to as the "State" and EAN Services, LLC, hereinafter referred to as the "Contractor." The purpose of this MOU is to add a 1 ton pick-up truck and associated information to SWC #205, Edison Contract #65939, the Vehicle Rental contract between the State and the Contractor ("Contract"). For good and valuable consideration, the sufficiency of which is hereby acknowledged, it is mutually understood and agreed by and between said undersigned contracting parties as follows:

I. Terms and Conditions

Pursuant to Special Terms and Conditions Section, E.2. Additional lines, items, or options:
"At its sole discretion, the State may make written requests to the Contractor to add lines, items, or options that are needed and within the Scope but were not included in the original Contract. Such lines, items, or options will be added to the Contract through a Memorandum of Understanding ("MOU"), not an amendment.

a. After the Contractor receives a written request to add lines, items, or options, the Contractor shall have ten (10) business days to respond with a written proposal. The Contractor's written proposal shall include:
    (1) The effect, if any, of adding the lines, items, or options on the other goods or services required under the Contract;
    (2) Any pricing related to the new lines, items, or options;
    (3) The expected effective date for the availability of the new lines, items, or options; and
    (4) Any additional information requested by the State.
b. The State may negotiate the terms of the Contractor's proposal by requesting revisions to the proposal.
c. To indicate acceptance of a proposal, the State will sign it. The signed proposal shall constitute a MOU between the Parties, and the lines, items, or options shall be incorporated into the Contract as if set forth verbatim.

Only after a MOU has been executed shall the Contractor perform or deliver the new lines, items, or options."

1 Ton Pick-Up Truck	
Respondent Classification:	**Specifications:**
UPAR/UQAR	Tow Capable, Payload up to 9,000 lbs, 4 Wheel Drive, Power Windows/Locks, Automatic Transmission, Cruise control, Crew Cab, Seat 6 Air Condition, Power Steering, Diesel Engine, Bumber or Gooseneck Hitch, Dual Rear Wheel
Ford F350, Chevrolet 3500, Dodge Ram 3500, or similar	

Description	UOM	State Business Contract Rate	State Employee Leisure Use Rate
Traditional - 1 Ton Pick-Up Truck, Hourly	HR	$ 30.00	$ 30.00
Traditional - 1 Ton Pick-Up Truck, Daily	DA	$ 90.00	$ 90.00
Traditional - 1 Ton Pick-Up Truck, Weekly	WK	$ 484.00	$ 484.00
Traditional - 1 Ton Pick-Up Truck, Monthly	MO	$2.091.67	$2.091.67

II. Effective Date.

The revisions set forth herein shall be effective upon the completion of all required approvals. All other terms and conditions contained in the Contract remain in full force and effect.

IN WITNESS WHEREOF,

EAN SERVICES, LLC

/s/ Meredith Perkins 4/2/21

SIGNATURE **DATE**

Meredith Perkins Authorized Officer

PRINTED NAME AND TITLE OF SIGNATORY (above)

Central Procurement Office

State of Tennessee, Department of General Services:

4/7/2021

Michael F. Perry, Chief Procurement Officer **DATE**

C2022004
CPR #: _____

Aug. 5, 2021
Date Received: _____

To be completed by the Procurement Division

☐ **Requires Finance Director's review.**

☒ **Cooperative Purchase is approved.**

☐ **Cooperative Purchase is denied.**

PURCHASING AGENT: Michelle A Hernandez Lane

9/2/2021 | 9:47 AM CDT
Date: _____

NOTE: Should this cooperative purchase request be approved, please remember to attach this signed form to your corresponding requisition as the "procurement authorization" within iProcurement when you set up your purchase order. PLEASE BE SURE TO REFERENCE THE COOPERATIVE CONTRACTING ORGANIZATION AND CONTRACT NUMBER IN THE DESCRIPTION.

DocuSign

Certificate Of Completion

Envelope Id: 9E1A72C22CEA43559432B5C5CC2F70D5
Status: Completed
Subject: Cooperative Form for General Services - C2022004 Enterprise Rent A Car
Source Envelope:
Document Pages: 117
Signatures: 2
Certificate Pages: 15
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-06:00) Central Time (US & Canada)

Envelope Originator:
Procurement Resource Group
730 2nd Ave. South 1st Floor
Nashville, TN 37219
prg@nashville.gov
IP Address: 170.190.198.185

Record Tracking

Status: Original
8/5/2021 7:06:45 PM
Holder: Procurement Resource Group
prg@nashville.gov
Location: DocuSign

Security Appliance Status: Connected
Pool: StateLocal

Storage Appliance Status: Connected
Pool: Metropolitan Government of Nashville and Davidson County
Location: DocuSign

Signer Events	Signature	Timestamp
Judy Cantlon judy.cantlon@nashville.gov Security Level: Email, Account Authentication (None)	**Completed** Using IP Address: 170.190.198.185	Sent: 8/5/2021 7:10:27 PM Viewed: 8/5/2021 7:11:21 PM Signed: 8/5/2021 7:11:53 PM
Electronic Record and Signature Disclosure: Accepted: 8/5/2021 7:11:21 PM ID: fc1c1c2b-c8b6-4057-9f06-2d821b6f49c0		
Velvet Hunter Velvet.Hunter@nashville.gov Security Level: Email, Account Authentication (None)	Velvet Hunter Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 8/5/2021 7:11:59 PM Viewed: 8/6/2021 9:14:32 AM Signed: 8/6/2021 9:15:01 AM
Electronic Record and Signature Disclosure: Accepted: 8/6/2021 9:14:32 AM ID: b77c41ca-50c9-4d41-9893-076d6588b504		
Michelle A Hernandez Lane michelle.lane@nashville.gov Chief Procurement Officer/Purchasing Agent Metro Security Level: Email, Account Authentication (None)	Michelle A Hernandez Lane Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 8/6/2021 9:15:07 AM Viewed: 9/2/2021 9:46:19 AM Signed: 9/2/2021 9:47:40 AM
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
Chuck Yancey Charles.Yancey@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 9/2/2021 9:47:46 AM
Amber Gardner amber.gardner@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 6/15/2021 8:11:35 AM ID: 2e7a3648-100c-4cdd-bc05-31b2620fd191	COPIED	Sent: 9/2/2021 9:47:47 AM
PRG prg@nashville.gov Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 9/2/2021 9:47:48 AM
Terri L. Ray Terri.Ray@nashville.gov Senior Procurement Officer Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 9/2/2021 9:47:49 AM

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	8/5/2021 7:10:27 PM
Certified Delivered	Security Checked	9/2/2021 9:46:19 AM
Signing Complete	Security Checked	9/2/2021 9:47:40 AM
Completed	Security Checked	9/2/2021 9:47:49 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

DocuSign

Certificate Of Completion

Envelope Id: 549BE58053D943CE8B9A5FD53115AD71
Status: Sent
Subject: Council Legislation - Rental Cars
Source Envelope:
Document Pages: 135
Signatures: 4
Certificate Pages: 16
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-06:00) Central Time (US & Canada)

Envelope Originator:
Procurement Resource Group
730 2nd Ave. South 1st Floor
Nashville, TN 37219
prg@nashville.gov
IP Address: 170.190.198.185

Record Tracking

Status: Original
5/16/2022 6:01:07 PM
Holder: Procurement Resource Group
prg@nashville.gov
Location: DocuSign

Security Appliance Status: Connected
Pool: StateLocal

Storage Appliance Status: Connected
Pool: Metropolitan Government of Nashville and Davidson County
Location: DocuSign

Signer Events	Signature	Timestamp
Rose Wood rachel.jones@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Signed by link sent to rachel.jones@nashville.gov Using IP Address: 170.190.198.185	Sent: 5/16/2022 6:10:36 PM Viewed: 5/17/2022 9:06:02 AM Signed: 5/17/2022 12:47:55 PM
Electronic Record and Signature Disclosure: Accepted: 5/17/2022 9:06:02 AM ID: 38e210f0-1c77-4695-ab2d-fc4235cf00c8		
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 Signed by link sent to michelle.lane@nashville.gov Using IP Address: 170.190.198.190	Sent: 5/17/2022 12:47:58 PM Viewed: 5/18/2022 12:33:53 PM Signed: 5/18/2022 12:34:13 PM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Kelly Flannery/MJW MaryJo.Wiggins@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Signed by link sent to MaryJo.Wiggins@nashville.gov Using IP Address: 170.190.198.100	Sent: 5/18/2022 12:34:16 PM Viewed: 5/18/2022 2:13:42 PM Signed: 5/18/2022 2:15:02 PM
Electronic Record and Signature Disclosure: Accepted: 5/18/2022 2:13:42 PM ID: 1931360e-5cb8-4ae0-b35a-92635bdfa7d6		

Signer Events	Signature	Timestamp
Procurement Resource Group prg@nashville.gov Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		Sent: 5/18/2022 2:15:07 PM

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
Sally Palmer sally.palmer@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 5/18/2022 7:42:15 AM ID: 95a8830c-2130-495a-82fd-f1b20014590f	COPIED	Sent: 5/18/2022 2:15:05 PM Viewed: 5/18/2022 2:16:57 PM
Macy Amos macy.amos@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 5/11/2022 1:57:16 PM ID: dfd26b19-2c04-40d0-8c31-9c01cfb0ea5d	COPIED	Sent: 5/18/2022 2:15:06 PM Viewed: 5/18/2022 2:15:50 PM
Amber Gardner Amber.Gardner@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 12/29/2021 9:46:41 AM ID: b64cc054-f106-4570-a33d-2a6a0d637898		
Austin Kyle publicrecords@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 5/17/2022 1:25:53 PM ID: f22f30c7-b009-450f-acec-d7997aae75d8		

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	5/16/2022 6:10:36 PM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure