Agreement (Purchase Order) #: _____

☒ CHAPTER 60GG-1, F.A.C. – INFORMATION TECHNOLOGY PROJECT MANAGEMENT AND OVERSIGHT STANDARDS

Governed by the Department of Management Services' Division of State Technology (DST), Chapter 60GG-1, Florida Administrative Code (F.A.C.), Florida Information Technology Project Management and Oversight Standards, establishes project management principles that State Agencies are required to follow when implementing information technology projects. the Department must adhere to the State project management standards and ensure that all project documentation created by the Vendor, the Department, or in collaboration, is developed and maintained in accordance with Chapter 60GG-1 F.A.C. The Vendor must be familiar with the State project management standards and be prepared to satisfy all requirements. It is important for the Vendor to recognize that documentation, monitoring, or reporting requirements may change mid-project, based on the project's DST Risk and Complexity Assessment, outlined in 60GG-1.002. The Vendor must be adaptable to changes required by Chapter 60GG-1 F.A.C., without increasing cost to the Department.

☒ CHAPTER 60GG-2, F.A.C. – FLORIDA CYBERSECURITY STANDARDS

Governed by the Division of State Technology, Chapter 60GG-2 F.A.C., Information Technology Security, also known as the Florida Cybersecurity Standards (FCS), establishes cybersecurity standards for information technology (IT) resources. State Agencies are required to follow these standards in the management and operations of state IT resources. the Department must adhere with the Florida Cybersecurity Standards for all IT projects created by the Vendor, Department, or in collaboration. The Vendor must be familiar with the State cybersecurity standards and be prepared to work with the Department to satisfy all requirements.

☒ CHAPTER 60GG-2.002, F.A.C. SYSTEM SECURITY PLANS

In support of the Florida Cybersecurity Standards, 60GG-2 F.A.C. Section 60GG-2.002, the Department requires that all IT systems have a system security plan (SSP). The SSP must address the security setup of the system, ensuring that security controls required by Section 60GG-2.003(5)(g)(4) are in place. The SSP must be submitted by the Vendor and approved by the Department Information Security Manager (ISM) prior to system implementation. The SSP must be completed using the SSP template made available from the Department ISM. The SSP must be submitted during the System Design/Configuration phase to allow time for changes in the security design that may be required. Upon receipt of the SSP, the Department will have ten (10) business days to review. The ISM will respond with feedback, approval, or denial of the plan. The Vendor must allow time for adjustments to the plan and resubmittal to the ISM. After the SSP is approved, the Vendor shall keep the SSP updated as necessary or upon notification by the Department of a deficiency in the SSP. Any change to the SSP must be reviewed by the Department and approved by the ISM.

☒ CHAPTER 60GG-2.002, F.A.C. BACKGROUND CHECKS FOR VENDOR STAFF

Florida Department of Transportation (Department) requires Vendor employees working on systems identified by the Department with a risk factor of moderate or higher to undergo an FBI Level II background check. The Vendor will pay the cost of their employee background checks. The Vendor will utilize the Department's Originating Agency Identifier (ORI). Contract employees must successfully pass the Level II background check before beginning work on the project.

☒ CHAPTER 60GG-2.002, F.A.C. RISK ASSESSMENTS

The Vendor that operates as a service provider agrees to perform a third-party risk assessment on vendor owned resources that contain Department information. The assessment will follow the schedule below, and create a risk mitigation plan that assigns risk levels and proposed controls. A Plan of Action and Milestones will be shared and communicated with the Department as risk is mitigated. An annual Attestation or Certification from a third-party assessment, or report or proof of certification such as but not limited to a System and Organization Controls (SOC) 2, International Organization for Standardization (ISO) 27001, etc. will be accepted in place of a third-party risk assessment.

Assessment categorization established as per Federal Information Processing Standards (FIPS) 199 Publication standards:

1. High – will be completed every 12 months
2. Moderate – will be completed every 18 months
3. Low – will be completed every 24 months

☒ CHAPTER 60GG-2.005, F.A.C. SECURITY INCIDENT RESPONSE

The Vendor agrees to provide a security incident response plan, which will be added as an addendum to the Department's overall security incident response plan. The Vendor's plan shall outline specific actions, response time frames, and roles and responsibilities. The Vendor agrees to align its services with the Department by monitoring and responding to security incidents of Department data and information according to section 282.318, F.S.

☒ COMPUTER HARDWARE/SOFTWARE LIABILITY

In any Agreement for the purchase or maintenance of machines or computer hardware/software or licensed programs, the Vendor's entire liability and the Department's exclusive remedy for damages to the Department related to the machine or computer hardware/software or licensed program which is the subject of this Agreement, or maintenance thereof shall be limited to, at the

Department's discretion, 1) the correction by the Vendor of the relevant defect(s); or 2) actual damages up to the greater of an amount equal to 12 months maintenance charges for said product or the purchase price of said product. Such maintenance charges will be those in effect for the specific product when the cause of action arose. The foregoing limitation of liability will not apply to (a) the payment of cost and damage awards resulting from liability in accordance with the Copyright and Patent Infringement paragraph below, or to (b) claims for reprocurement costs or the cost of cover pursuant to Rule 60A-1.006, Florida Administrative Code, or to (c) claims by the Department for personal injury or damage to real property or tangible personal property caused by the Vendor's negligence or tortious conduct.

☒ CONFIDENTIAL INFORMATION

Trade secrets are not solicited or desired as submissions with responses. Respondents are advised to submit a redacted version of the quote if the Vendor deems any portion of the documents, data or records submitted in response to this solicitation to be confidential, trade secret or otherwise not subject to disclosure pursuant to Chapter 119, Florida Statutes (F.S.), the Florida Constitution or other authority. Any confidential or trade secret submission must be conspicuously marked as such, and any redacted copy must be clearly titled "Proprietary and Confidential." Failure to provide a redacted version when confidentiality is claimed by the Vendor may be cause for determination of non-conformance**.**

☒ CONFLICT OF INTEREST

To prevent any bias, unfair competitive advantage, conflict of interest, or the appearance of any type of impropriety, Vendor personnel must not have been directly or indirectly involved in the development of the Scope of Services or related solicitation documentation by the Department. If Vendor personnel worked in conjunction with the Department on the development of the solicitation document, the Vendor is prohibited from submitting a bid for this solicitation. Vendor personnel assigned to other Department projects outside this Contract, shall hold and maintain any confidential information that could benefit the Vendor on future solicitations in strictest confidence. As a condition of the Agreement, the Department may require contracted personnel to sign a nondisclosure agreement. Violation of the non-disclosure agreement by contracted personnel may result in termination of the individual, and at the Department's discretion, disqualification of the Vendor from future solicitations.

☒ COPYRIGHT OR PATENT INFRINGEMENT

To the extent permitted by Florida Law, the Vendor, without exception, shall save, defend and hold harmless the Department and its employees from liability of any nature or kind, including cost and expenses, for or on account of any copyrighted, patented or unpatented invention, process, or article manufactured or supplied by the Vendor. The Vendor has no liability when such claim is solely and exclusively due to the combination, operation or use of articles supplied hereunder with equipment or data not supplied by Vendor or is based solely and exclusively upon the Department's alteration of the article. The Department will provide prompt written notification of a claim of copyright or patent infringement. Further, if such claim is made or is pending, the Vendor may, at its option and expense, procure for the Department the right to continued use of, or replace or modify the article to render it non-infringing. If the Vendor uses any design, device, or materials covered by letters, patent or copyright, it is mutually agreed and understood that, without exception, the Agreement price shall include all royalties or other costs arising from the use of such design, device, or materials in any way involved in the work. Copyrighted material will be accepted, as part of a technical Quote, only if accompanied by a waiver that will allow the Department to make paper and electronic copies necessary for use by the Department staff and agents. It is noted that copyrighted material is not exempt from the Public Records Law, Chapter 119, F.S. Therefore, such material will be subject to viewing by the public.

☒ DATA SECURITY AND CONFIDENTIALITY

The Vendor and its employees must comply with all Department security procedures while working on this Agreement. The Vendor shall provide immediate notice to the Department-OIT Application Services Manager and the Department – Transportation Technology Office (TTO) Information Security Manager (ISM) in the event it becomes aware of any security breach, any unauthorized transmission of State Data as described below or of any allegation or suspected violation of the Department security procedures. Except as required by law or legal process and after notice to the Department, the Vendor shall not divulge to third parties any confidential information obtained by the Vendor or its agents, distributors, resellers, subcontractors, officers or employees in the course of performing Agreement work, including, but not limited to, Chapter 60GG-2, F.A.C., security procedures, business operations information, or commercial proprietary information in the possession of the state and/or the Department.

a. Loss of Data

In the event of loss of any Department or State data or record where such loss is due to the negligence of the Vendor or any of its subcontractors or agents, the Vendor shall be responsible for recreating such lost data in the manner and on the schedule set by the Department at the Vendor's sole expense.

b. Data Protection

No state data or information will be transmitted to, stored in, processed in, or shipped to offshore locations or out of the United States of America, regardless of method, except as required by law. Examples of these methods include (but are not limited to): FTP transfer, DVD, tape, or drive shipping; regardless of level of encryption employed. Access to State Data shall only be available to approved and authorized staff, including remote/offshore personnel, that have a legitimate business need.

☒ DELIVERABLE WARRANTY

Vendor warrants that all Deliverables provided by Vendor shall comply with the form, content, performance, and functionality specified in the Scope or each applicable TWO. If at any time within the Warranty Period, the Department discovers that a Deliverable does not comply with this Warranty, the Vendor shall, at no cost to the Department and in a timely manner, make such Deliverable conform and comply with this Warranty.

Each Deliverable and any other work product provided by Vendor in performing the Services, does not and will not infringe and is not and will not misappropriate or infringe the intellectual property rights, privacy rights or other rights of any other person or entity, nor has any claim of such infringement been threatened or asserted, nor is such a claim pending against Vendor (or to the best of Vendor's knowledge, any entity from which Vendor has obtained such Deliverable, Work Product, or rights related thereto.

☒ ELECTRONIC ACCESSIBILITY

The Federal Electronic and Information Technology standard can be found at: https://www.section508.gov/. The Department standards set for section 508 compliance information for the supplies and services in this Agreement are available on the Department Standards and Guidance Set website.

☒ ESCROW OF SOURCE CODE

The Vendor shall maintain in escrow a copy of the source code for the licensed software. With each new release of the software provided to the Department, the Vendor shall maintain the updated source code in escrow. In the event the Vendor files for bankruptcy or ceases operations for any reason, the Department shall promptly be provided the current source code in escrow. The Department will only use the source code to support the licensed software subject to the same nondisclosure provisions of this Agreement.

☒ FACILITIES AND EQUIPMENT

Upon completion of Security Awareness Training by the Vendor's personnel assigned to this project, the Department shall provide necessary access to the Department network. The work will be conducted on-site in the Tallahassee Project Office. The Project will provide work space to use while on site. All property furnished by the Department for use by the Vendor during this Agreement will remain the property of the State of Florida.

☒ GUIDELINES AND STANDARDS

The Vendor agrees to comply with the Department's best practices and standards, including, but not limited to, the most current version available on the Department Standards and Guidelines Set website.

☒ OWNERSHIP OF WORKS AND INVENTIONS

The Department shall have full ownership of any works of authorship, inventions, improvements, ideas, data, processes, computer software programs, and discoveries (hereafter called intellectual property) conceived, created, or furnished under this Agreement, with no rights of ownership in Vendor or any subcontractors. Vendor and subcontractors shall fully and promptly disclose to the Department all intellectual property conceived, created, or furnished under this Agreement. Vendor or subcontractor hereby assigns to the Department the sole and exclusive right, title, and interest in and to all intellectual property conceived, created, or furnished under this Agreement, without further consideration. This Agreement shall operate as an irrevocable assignment by Vendor and subcontractors to the Department of the copyright in any intellectual property created, published, or furnished to the Department under this Agreement, including all rights thereunder in perpetuity. Vendor and subcontractors shall not patent any intellectual property conceived, created, or furnished under this Agreement. Vendor and subcontractors agree to execute and deliver all necessary documents requested by the Department to affect the assignment of intellectual property to the Department or the registration or confirmation of the Department's rights in or to intellectual property under the terms of this Agreement. Vendor agrees to include this provision in all its subcontracts under this Agreement.

All work materials developed or provided by the Vendor under this Agreement and any prior agreement between the parties shall be deemed to be work made for hire and owned exclusively by the State of Florida. Any intellectual property contained in a Deliverable and developed as a result of this Agreement shall be the sole property of the State of Florida. This provision will survive the termination or expiration of the Agreement. The Vendor retains all ownership rights in any proprietary methodologies, methods, processes, ideas, concepts, algorithms, trade secrets, software documentation, other intellectual property, or procedures of the Vendor that pre-exist or were developed outside the scope of this Agreement. If any such property of Vendor is contained in any of the Deliverables hereunder, the Vendor grants to the Department a royalty-free, paid-up, non-exclusive, perpetual license to use such Vendor intellectual property in connection with the Department's use of the Deliverables.

☒ PROJECT PLAN SCOPE LANGUAGE

The Department requires that the Vendor create and submit a Project Plan that demonstrates how the creation and maintenance of the application will be carried out. The Project Plan template may be found at https://www.fdot.gov/it/docs/dispFiles.shtm, and is the template which the Department requires the Vendor to follow. The Project Plan must be submitted to the Department within thirty (30) business days after execution of Agreement or as indicated in the Scope of Work. Upon receipt of the Project Plan, the Department will have fourteen (14) business days to review and approve the Project Plan in its sole discretion. No other work may begin prior to the submission and approval of the Project Plan. After the Project Plan is approved, the Vendor shall keep the Project Plan updated as

necessary or upon notification by the Department of a deficiency in the Project Plan. Any change to the Project Plan must be approved by the Department.

☒ Purchase of Tangible Personal Property

Contractual services that provide for the Vendor to purchase tangible personal property, as defined in Section 273.02, F.S., for subsequent transfer to the Department may be entered into only in accordance with Rule 60A-1.017, F.A.C. Technology products (e.g., software, networking equipment, etc.) purchased by the Vendor shall be subsequently transferred to the Department and shall be of first quality, supplied by the original product manufacturer or an authorized reseller, and warrantied as appropriate. Technology products procured by the Contractor outside of authorized distributors/retailers are not deemed acceptable to the Department. The Agreement shall specify the quality of the technology products to be acquired, and provisions for warranty, service, and mandatory transfer of ownership to the Department.

☒ SECURITY OF CONFIDENTIAL PERSONAL INFORMATION

The Vendor must implement procedures to ensure the protection and confidentiality of all data, files, and records involved with this Agreement.

Except as necessary to fulfill the terms of this Agreement and with the permission of the Department, Vendor and Vendor's employees shall not divulge to third parties any confidential information obtained by Vendor or its agents, distributors, resellers, subcontractors, officers, or employees in the course of performing work on this Agreement, including, but not limited to, security procedures, business operations information, or commercial proprietary information in the possession of the State or the Department. If Vendor or Vendor's employees have access to confidential information in order to fulfill Vendor's obligations under this Agreement, Vendor agrees to abide by all applicable Department Information Technology Security procedures and policies. For purposes of this Agreement, "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Department information in Vendor's possession. Vendor shall make a report to the Department not more than seven (7) business days after Vendor learns of such use or disclosure.

Vendor's report shall identify, to the extent known: (i) the nature of the unauthorized use or disclosure, (ii) the confidential information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Vendor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Vendor has taken or shall take to prevent future similar unauthorized use or disclosure.

In the event a "Security Incident" also includes a "breach of security", as defined by section 501.171, F.S., as amended, concerning confidential personal information involved with this Agreement, Vendor shall comply with section 501.171, F.S. When notification to affected persons is required under this section of the statute, Vendor shall provide that notification, but only after receipt of the Department's approval of the contents of the notice. Defined statutorily, and for purposes of this Agreement, "breach of security" or "breach" means the unauthorized access of data in electronic form containing personal information.

☒ THIRD PARTY TOOLS

Vendors may not use third-party tools which impose licensing responsibility on the Department without written approval by the Department.

☒ TRAINING

The Vendor shall provide, at its own expense, training necessary for keeping Vendor staff abreast of industry advances and for maintaining proficiency in equipment and systems that are available on the commercial market.