# Sample Security Plan

## XXXX Example Office

# XXXX Example Application (DEA)

VERSION: 8.3 REVISION DATE: August 15, 2022

**Instructions:**
This is a SAMPLE template of the XXXX System Security Plan.

- To request a new System Security Plan to be initiated, please email the Information Security Office. Please include the following information in this initial request: System Name and Acronym; Technology Proposal Number and ROADS ID number (if applicable). Names of the System Owner, System Developer, Project Manager and Functional Application Coordinator.
- For vendor access to the System Security Plan, please contact either the Project Manager or the Information Security Office.Upon request, we are able provide a copy of the system security plan document via XXXX secure file transfer.

Approval of the Security Plan indicates an understanding of the purpose and content described in this document, based on my areas of responsibility as listed in Section 8: Roles and Responsibilities.

| Approver Name | Title | Signature | Date |
|---|---|---|---|
| System Owner | System Owner | | |
| Functional Coordinator | Functional Coordinator | | |
| Project Manager | Project Manager | | |
| System Security Coordinator | System Security Coordinator | | |
| Information Security Manager | Information Security Manager | | |

| Approval Type | Description | Date |
|---|---|---|
| Plan Accepted | The Information Security Management Office (ISMO) has reviewed the Security Plan and approves the planned Security Design. The Project Team may move forward with development, purchase or configuration efforts for the System. Should the Security Design of the system change, the Security Plan must be updated and submitted for re-review. | |
| Vulnerability Assessment | The ISMO has completed vulnerability scans of the information technology components involved in this project. All vulnerabilities have been (1) addressed within acceptable limits or (2) accepted and documented as a risk to the project. | |
| Final Approval | The System has been developed and is ready for production. If the System goes through a major | |

| | | |
|---|---|---|
| | modification or update, then the Security Plan has to be updated and approved. | |

# *Table of Contents*

# *Section 1 Purpose and Handling of the Security Plan Document*

***Note: For instructions on completing this template, please reference the XXX Security Plan Instructions.***

This Security Plan outlines the security configuration of the system, identifies risks and vulnerabilities, and addresses how the risks will be mitigated. Use of this template ensures that the requirements from Chapter 60GG-2, F.A.C., are addressed. The objectives of the Security Plan are to:

- Ensure confidentiality, integrity, and availability of the system data
- Identify confidential or sensitive information in the system
- Define system security methods, requirements and procedures
- Promote consistency and uniformity in the system's security practices

The purpose of each section in this document is to address risk management and reduce exposure to the Department by identifying controls to offset threats and protect the Department's resources. All sections should be addressed, unless deemed inapplicable to your system. If a section is not applicable, please mark it accordingly in the security plan. Do not remove sections of the template.

It is expected that the Security Plan will be developed during the system development life cycle (e.g., the Security Plan may be revised after testing is complete, but before going into production). It is understood that Security Plans submitted in the early phases of development will not be able to address all questions. These questions can be addressed later as the system moves through the developmental life cycle. All questions must be answered, and the Security Plan shall have Final Approval status before the system moves to production. Information about the submission and review process for security plans can be accessed at the Instructions for Project Managers link on the Security Assessment and Authorization page.

The Security Plan is a living document that must be updated to incorporate new and/or modified security controls any time the system goes through a major modification. The plan will be maintained as changes occur to the system that could potentially impact the security of the system. Please reference the XXX Security Plan Instructions document for the conditions under which a system change will require an updated security plan to be submitted to the Information Security Management Office (ISMO) for approval.

Security Plans are considered confidential and exempt from Section 119.07(1), F.S., pursuant to Sections 282.318, F.S. System Security Plans shall only be made available to those individuals with a business need to view, process, or maintain the plan. The system Security Plan document must be stored in the Draft folder on the secured SharePoint site during the submission and review process. After approval, the Security Plan document will be moved to the Approved folder on the SharePoint site. Please contact the InfoSec team if access to a Security Plan needs to be granted for internal staff. **In the situation where the Security Plan must be shared with external staff or placed on external locations, access must be limited to only those staff with a direct need to access the Security Plan. When Security Plans must be transmitted externally, use secured methods such as the Department's File Transfer Appliance (FTA).**

# *Section 2 System Overview*

*Provide an overview of the system by completing sections below. The System Description (2.1) must include a 1-2 paragraph summary that describes the business use and key functionality of the system being developed, enhanced or purchased. Also, describe the types of users (internal, external, general public) that will utilize the system. If you will be referring to your system with an acronym, ensure that it is unique to the Department by checking the Application System List* and/or the *ROADS Applications and Reporting Inventory under Configuration Items in the Cherwell Portal.*

## Section 2.1 System Description

| | |
|---|---|
| **System Name (Acronym):**<br>**System URL:** | XXXX Example Application (DEA)<br>www.dea.com/dea |
| **Description of the System**<br>Provide a general overview of the system including the business purpose, processes and data addressed by the system. ***Optional***: *If you have system documents that would assist the ISM Team in understanding the system (user manual, functional specifications, etc.), that can be attached separately.* | |
| **Description of System Data** Describe at a high-level the data being used and/or collected. Also describe how the data will be used within the application. | |
| **Technology Proposal** link and/or Project Development website (if applicable) | |
| **ROADS ID Number (**All Systems must be entered into ROADS. Contact your Enterprise Data Steward for assistance.**)** | |

## Section 2.2 System Technical Details

| | | Server or Azure Resource Name | IP/IP Range |
|---|---|---|---|
| **System Server** | | | |
| **(Unit Test/Dev):** | ☐ N/A | | |
| **(System Test):** | ☐ N/A | | |
| **(Production):** | ☐ N/A | | |
| **Database Server** | | | |
| **(Unit Test/Dev):** | ☐ N/A | | |
| **(System Test):** | ☐ N/A | | |
| **(Production):** | ☐ N/A | | |
| **Support Teams** | | | |
| **System Server Support Team:** | ☐ N/A | | |
| **Database Server Support Team:** | ☐ N/A | | |

## Section 2.3 System Scope

| | | |
|---|---|---|
| ☐ | Statewide | |
| ☐ | District Specific | District(s): |
| ☐ | Office Specific | Office Name(s): |
| **Explanation:** | | |

## Section 2.4 System Operational Status

| | | |
|---|---|---|
| ☐ | Operational | The system is operating and in production. |
| ☐ | Under Development | The system is being designed, developed, acquired or implemented. |
| ☐ | Major Modification | The system is undergoing a major change, development, or transition. |
| ☐ | Technology Refresh | The system is undergoing a major change focusing on updating the underlying technology with only minor changes to the business functionality. |
| ☐ | Other | Document details below. |
| **Explanation (include projected implementation date if applicable):** | | |

## Section 2.5 System Type

| | | |
|---|---|---|
| ☐ | XXXX Developed System | Version: |
| ☐ | Vendor Developed System | |
| ☐ | Vendor/XXXX Joint Developed System | |
| ☐ | Commercial off the Shelf (COTS) System<br>☐ Managed by XXXX<br>☐ Managed by Service Provider | |
| ☐ | Other: | |
| **Explanation:** | | |

## Section 2.6 Web Presence

| **Select all that apply:** | | | | |
|---|---|---|---|---|
| ☐ XXXX Intranet | | ☐ Internet | | ☐ No Web Presence |
| **Managed by:** | ☐ XXXX OIT | ☐ XXXX Non-OIT | ☐ Vendor<br>*List Vendor Name Below* | ☐ Other: |
| This system supports the standard XXXX browsers: | | | ☐ Google Chrome | ☐ Microsoft Edge |
| **Explanation:** | | | | |

## Section 2.7 System Automated Email

| | | |
|---|---|---|
| Automated emails are sent to users through this system: | ☐ No | ☐ Yes |
| **Email recipients are:** | ☐ XXXX Email Accounts* | ☐ Non-XXXX Email Accounts |
| **The email is sent from:**<br>*(List sender email address here)* | ☐ XXXX Email Account | ☐ Non-XXXX Email Account*<br>*(such as a vendor service)* |
| *Note: If XXXX email accounts will receive automated system notifications from a non-XXXX email address, please coordinate with the Office 365 Messaging Team to ensure these emails will not be flagged as spam in Outlook. Approval for SMTP relay may also be needed and can be requested through the SMTP Relay Request Form. | | |
| **Comments:** | | |

## Section 2.8 Digital Certificates and Electronic Signatures [Link to definition]

| | | |
|---|---|---|
| This system uses Digital Certificates: | No ☐ | Yes ☐ |
| This system uses DocuSign for electronic signatures: | No ☐ | Yes ☐ |
| This system uses another digital certificate for electronic signatures: | No ☐ | Yes ☐ |
| Is the digital certificate on the Department's standards list? [Link to approved authorities] | No ☐ | Yes ☐ |
| Digital certificate vendor name: (list here) | | |
| **Explain how digital certificates and electronic signatures will be used in this system:** | | |

# *Section 3 Authentication and Authorization Risk Analysis*

*Identify the risks associated with this system and document how those risks will be mitigated. Answer the questions below and provide any additional details that are pertinent. In areas where this system does not follow XXXX standards ensure to provide greater details.*

## Section 3.1 System Roles and System Access Requests

Complete the table below with the roles from your system. Include all roles, even those that are automatically granted broadly (example: Read Only access to anyone with an AD Account) (Sample)

**All access to xxxx systems must be requested and approved through the Automated Access Request Form System. List the selections (Access Items) that are provided for each role in this system.**

One or more access items should be established for a new application. Each system role listed below that can be assigned to XXXX users should be documente. If one access Item is used for more than one system role (e.g., system roles are listed in the addendum of a single entry item), please explain in the comments section below. Mark the Access Item Name as N/A if it is a read-only unauthenticated role or if the role is only assigned to external system users.

| System Role | Description of System Role Capabilities, including Scope of Control | Names of AD Security Groups, RACF Profiles, ISA Roles, etc. used to grant system role. | Access Item Name |
|---|---|---|---|
| *e.g., XXX System Role* | *Can create and edit requests* | *XX_SS_XX_Role* | *e.g. XXX System Role* |
| | | | |
| | | | |
| | | | |

| System Role | Description of System Role Capabilities, including Scope of Control | Names of AD Security Groups, RACF Profiles, ISA Roles, etc. used to grant system role. | Access Item Name |
|---|---|---|---|
| **Comments:** | | | |

## Section 3.2 Authentication Method

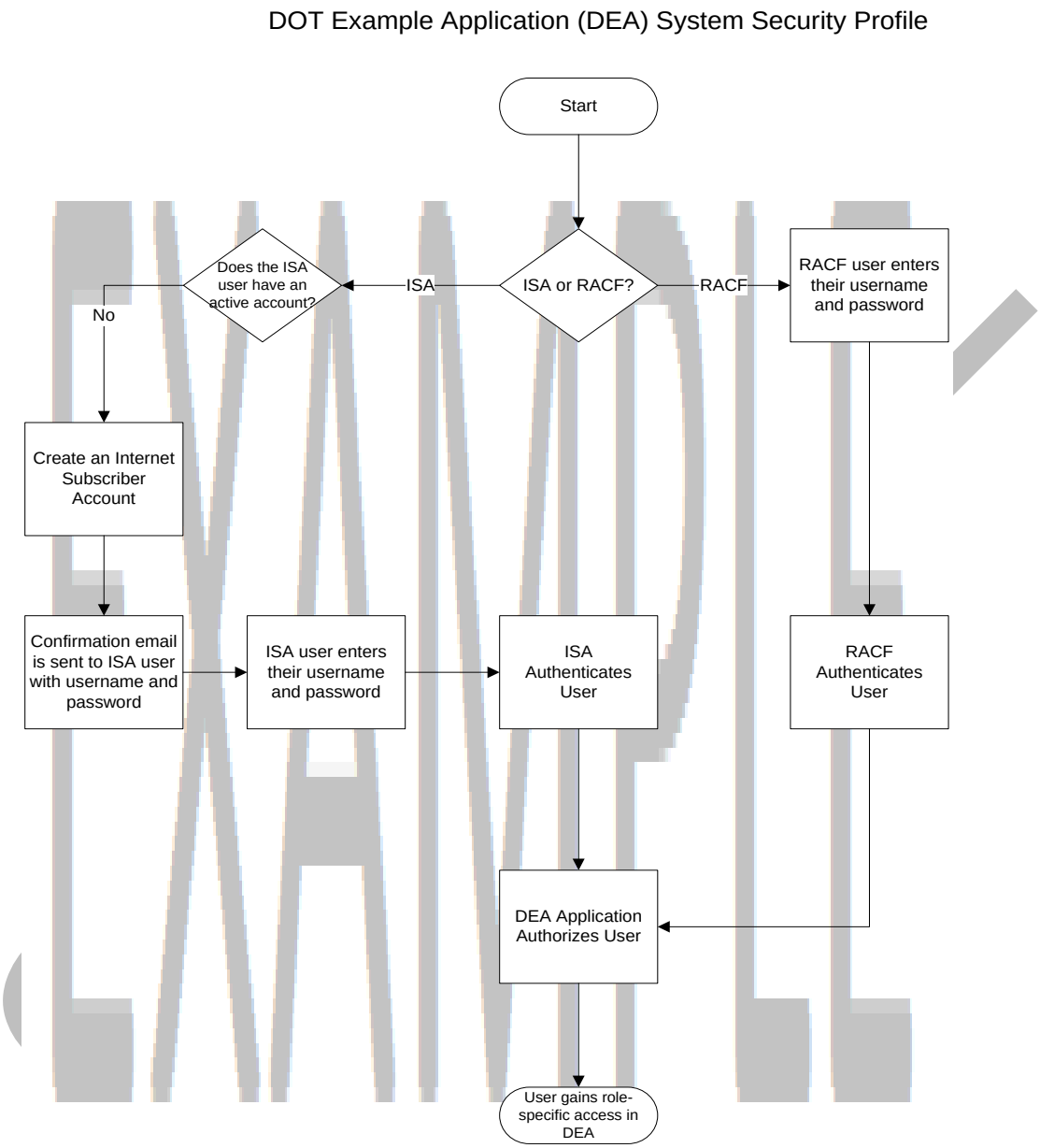
| **Authentication Method** | **Internal Users** (XXXX Staff/ Staff Aug) [Definition] | **External Users** With an XXXX Account (i.e. RACF, ISA or Azure B2C) [Definition] | **External Users** with out XXXX Account | **Not Used** |
|---|---|---|---|---|
| No Access Granted. (Select if the group in the listed column has NO access to this system). | ☐ | ☐ | ☐ | ☐ |
| RACF (Resource Access Control Facility/Mainframe) | ☐ | ☐ | ☐ | ☐ |
| AD (Active Directory) | ☐ | ☐ | ☐ | ☐ |
| Microsoft Azure - AD | ☐ | ☐ | ☐ | ☐ |
| Microsoft Azure – ADFS *(If used, explain below why the standard Azure AD is not being used)* | ☐ | ☐ | ☐ | ☐ |
| ISA (Internet Subscriber Account) | Not Allowed | ☐ | ☐ | ☐ |
| Azure B2C | Not Allowed | ☐ | ☐ | ☐ |
| Security Token Service (STS) *(If used, explain below)* | ☐ | ☐ | ☐ | ☐ |
| Other Method or No Authentication Method (*If used, explain below*) | ☐ | ☐ | ☐ | ☐ |
| **Explanation:** | | | | |

## Section 3.3 Authentication Details

| **Details Specific to This System** | **Internal Users** (XXXX Staff/ Staff Aug) | **External Users** With an XXXX Account (I.E. RACF, ISA or Azure B2C) [Definition] | **External Users** with out XXXX Account | **Not Used** |
|---|---|---|---|---|
| Multi-Factor Authentication *If Internal/External selected, explain how implemented below* | ☐ | ☐ | ☐ | ☐ |
| Passwords can be reset manually by an administrator of this system | ☐ | ☐ | ☐ | ☐ |
| This system allows for self-service password recovery (Username or Password) | ☐ | ☐ | ☐ | ☐ |
| The user is forced to reset their password in this system after being reset using self-service or by an administrator of this system | ☐ | ☐ | ☐ | ☐ |
| This system sends out password expiration reminders | ☐ | ☐ | ☐ | ☐ |
| This system can disable an account programmatically | ☐ | ☐ | ☐ | ☐ |
| This system allows for inactivity or session timeouts | ☐ | ☐ | ☐ | ☐ |
| This system follows XXXX's standard password requirements *If Not Used/No selected, explain the standards that are followed below* | ☐ | ☐ | ☐ | ☐ |
| **Explanation:** | | | | |

## Section 3.4 Security Profile Diagram

*Provide a Security Profile Diagram for your system. The diagram should illustrate your authentication mechanism and authorization process, including what method of authentication is used as listed in Section 3.3 (i.e., AD, RACF, ISA).*



# *Section 4 Configuration Risk Analysis*

*Identify the risks associated with this system and document how those risks will be mitigated. Answer the questions below and provide any additional details that are pertinent. In areas where this system does not follow XXXX standards ensure to provide greater details.*

## Section 4.1 Graphical User Interface

| **Interface Type** | **Internal Users** (XXXX Staff/ Staff Aug) | **External Users** With an XXXX Account (I.E. RACF, ISA or Azure B2C) [Definition] | **External Users** with out XXXX Account |
|---|---|---|---|
| This system is accessed via a web browser | ☐ | ☐ | ☐ |
| This system is accessed via a thick application client | ☐ | ☐ | ☐ |
| This system is accessed via a mobile app | ☐ | ☐ | ☐ |
| **Comments:** (Please list all mobile apps) | | | |

## Section 4.2 Generic and/or Service Accounts

| This system uses generic and/or service accounts | No ☐ | Yes ☐ |
|---|---|---|

| **Generic and/or Service Account Name** | **Purpose** | **Documented in XXXX?** |
|---|---|---|
| | | ☐ |
| | | ☐ |
| **Comments:** | | |

## Section 4.3 Development Environment

| This system will utilize XXXX's Development Environment Standards to establish a standard enterprise development environment.<br>Mark this section N/A if this is a vendor developed or COTS system, and also complete Section 4.12 Securing Vendor Provided Systems. | ☐ N/A | ☐ Yes | ☐ No |
|---|---|---|---|

**Provide a brief description about the development environment to include items such as test environments, production data replication, migration between environments, stress testing, etc. You may describe below or provide a link to an existing document or upload a document to the security plan folder.**

## Section 4.4 Application Programming Interfaces (API) - Consumption

| This system utilizes application programming interfaces (APIs) to access other systems. List the APIs used below. If you use APIs from the XXXX Enterprise Library (FEL) you may list them separately, or just reference that the system uses FEL/FEL Version Number. | No ☐ | Yes ☐ |
|---|---|---|

| API Name | Purpose of API | Includes Confidential/PII? | Method of Securing API |
|---|---|---|---|
| | | ☐ No ☐ Conf ☐ PII | |
| | | ☐ No ☐ Conf ☐ PII | |
| | | ☐ No ☐ Conf ☐ PII | |

## Section 4.5 Application Programming Interfaces (API) – Hosted API

| This system utilizes application programming interfaces (APIs) to provide/host data to other systems. List the APIs used below. | No ☐ | Yes ☐ |
|---|---|---|

| API Name | Purpose of API | Includes Confidential/PII? | API Method | Data Format | Method of Securing API |
|---|---|---|---|---|---|
| | | ☐ No ☐ Conf ☐ PII | ☐ Restful ☐ SOAP ☐ Other | ☐ XML ☐ JSon ☐ Other | |
| | | ☐ No ☐ Conf ☐ PII | ☐ Restful ☐ SOAP ☐ Other | ☐ XML ☐ JSon ☐ Other | |
| | | ☐ No ☐ Conf ☐ PII | ☐ Restful ☐ SOAP ☐ Other | ☐ XML ☐ JSon ☐ Other | |

## Section 4.6 System Dependencies

| This system **is dependent on** or **is a dependency to** other systems. List the system(s) below. Add more lines or upload separate document to security plan folder if additional space is needed.<br>*If you listed an API in Section 4.4 or 4.5, you do not need to list it again in this section.* | No ☐ | Yes ☐ |
|---|---|---|

| System Name | Summary of Dependency |
|---|---|
| | |
| | |
| | |

## Section 4.7 Port Settings

| List all ports required by the system and provide a brief description: | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Port Number:** | **Service** | **Description** | **Inbound** | **Outbound** | **Local FW** | **XXXX FW** | **XXX FW** |
| 80 | HTTP | Unsecure browsing in relation to app | ☐ | ☐ | ☐ | ☐ | ☐ |
| 443 | HTTPS | Secure browsing in relation to app | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ | ☐ | ☐ |

## Section 4.8 Specialty Hardware

Describe any specialty hardware that would need to be considered when reviewing the security risk of the system. Specialty hardware would be any hardware that is not XXXX standard hardware such as a custom desktop, IP cameras or a kiosk machine. Reference the manufacturer name, model or version numbers if known. Provide links to product specifications, diagrams and online manuals where possible or provide this information in an appendix.

| This system contains specialty hardware | No ☐ | Yes ☐ |
|---|---|---|

| Manufacturer | Make/Model/Version | Description of Hardware |
|---|---|---|
| | | |
| | | |

## Section 4.9 Patch Management, Software Updates and Firmware Upgrades

| | Managed by | | | | |
|---|---|---|---|---|---|
| **Endpoints, network equipment, and IoT devices** | XXX | XXXX Enterprise Patch Mgmt. Team | District/CO OIT | Vendor / Other (List in Comments) | Not Applicable to System |
| Firmware upgrades | ☐ | ☐ | ☐ | ☐ | |
| Operating System software updates and patches | ☐ | ☐ | ☐ | ☐ | |
| Application/System specific software | ☐ | ☐ | ☐ | ☐ | |
| 3rd party software updates and patches (e.g. Java, Flash Player) | ☐ | ☐ | ☐ | ☐ | ☐ |
| Specialty Hardware (As listed above) | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Comments:** | | | | | |

## Section 4.10 Physical Security

| | |
|---|---|
| This system resides at the XXXXX (XXX) Data Center and will be subjected to its physical security policies and procedures | ☐ |
| This system resides at an XXX Datacenter and will be subjected to its security policies and procedures | ☐ |
| This system resides in the XXXX Azure environment and XXXX staff/vendors will have no physical access to the system. | ☐ |
| This system resides in a location not hosted by XXXX. List the level of physical access allowed to XXXX staff/vendors. If there is physical access, explain how it is managed. | ☐ |
| Other: | ☐ |
| **Explanation:** | |

## Section 4.11 Cloud Environment

| | | | | |
|---|---|---|---|---|
| The infrastructure of this system is hosted in a cloud environment: | | | No ☐ | Yes ☐ |
| Cloud Model (Help): | ☐ Software as a Service (SaaS) | ☐ Platform as a Service (PaaS) | ☐ Infrastructure as a Service (IaaS) | |
| Cloud Vendor used: | ☐ Windows Azure | ☐ Amazon Web Services | ☐ Other, specify: | |
| IP Restrictions: | ☐ None | ☐ Internal Network | ☐ Other, specify: | |
| Select services that apply: | Web Apps ☐ | SQL Services ☐ | Storage ☐ | Virtual Machines ☐ |
| Utilizes: | Azure Key Vault ☐ | | Single Sign-On ☐ | |
| | Transparent Data Encryption (Azure SQL Service Only) ☐ | | Azure Disk Encryption ☐ | |
| | Azure Application Gateway ☐ *(see document)* | | App Service over HTTPS only ☐ | |
| | Azure Access Control ☐ | | ☐ Other, specify: | |
| Document steps taken according to “Azure Security Best Practices and Patterns”: | | | | |

## Section 4.12 Securing Vendor Provided Systems

| | | |
|---|---|---|
| This system is hosted/managed by a vendor: | No ☐ | Yes ☐ *Complete below and 4.12 A-C* |
| All default passwords on vendor provided systems have been reset | Yes ☐ | No ☐ |
| **Explanation:** | | |

| | | |
|---|---|---|
| **4.12(A) Incident Management Contacts.** Any Security Incidents which involve XXXX data, equipment or systems must be reported to the Information Security Manager. For Hosted Solutions (those not hosted/managed by XXXX) provide below a contact name, email address and/or phone number for use by the Information Security Manager for reporting and information on security incidents.<br>Contact Name and Title:<br>Email Address:<br>Phone Number: | | |
| The vendor has been made aware that all security incidents must be reported to the XXXX Information Security Manager at xxx-xxx-xxxx or Email@domain.com. If another method of reporting is used, please describe:<br>*When reporting via email, do not include sensitive or confidential information.* | No ☐ | Yes ☐ |

| | | |
|---|---|---|
| **4.12(B) System Hardening Guidelines.** The vendor, or other entity, provides system hardening guidelines**.**<br>**Please document in Section 11 References and upload copies to the Draft folder* | Yes* ☐ | No ☐ |
| This system conforms to the guidelines that were provided by the vendor | Yes ☐ | No ☐ |
| **Explanation:** | | |

| | | |
|---|---|---|
| **4.12(C) Certification or Attestation.** List any certification or attestation for the system, if available. | | |
| FedRAMP Certified (search FedRAMP) ☐ | SOC 2 Compliance ☐ | ISO 27000 Standards ☐ |
| Other: | | ☐ |
| **Describe:** | | |

# *Section 5 Data Risk Analysis*

*Identify the risks associated with this system and document how those risks will be mitigated. Answer the questions below and provide any additional details that are pertinent. In areas where this system does not follow XXXX standards ensure that you provide greater details.*

## Section 5.1 Database Information

| This system utilizes database(s): | | No ☐ | | Yes ☐ |
|---|---|---|---|---|
| ☐ Oracle | ☐ MSSQL | ☐ DB2 | ☐ Azure SQL | ☐ Other, specify database: |
| ☐ The database(s) will be managed by OIT | | ☐ The database(s) will be managed by non-OIT<br>Managed by: | | |
| If the data is stored in a cloud infrastructure, the provider has agreed not to house XXXX data offshore: | | ☐ Yes | ☐ No | ☐ Not Applicable |

## Section 5.2 External User Data Entry

| External user roles will be entering data the Department or its constituents have a dependency on: | ☐ No | ☐ Yes |
|---|---|---|
| **Explain the types of data external users will enter:** | | |

## Section 5.3 Specialized Reporting

| Does this system utilize specialized reporting tools or process batch jobs outside of the primary application? | No ☐ | Yes ☐ |
|---|---|---|
| **List the tool(s) used and the types of data sent in the report(s) and/or batch job(s):** | | |

## Section 5.4 Data Encryption

| This system encrypts data in transit | Yes ☐ | No ☐ |
|---|---|---|
| This system encrypts data at rest | Yes ☐ | No ☐ |
| **Methods used to protect the data's confidentiality:** | | |

## Section 5.5 Electronic Document Storage

| | | | |
|---|---|---|---|
| This system requires the upload and attachment of electronic documents: | No ☐ | | Yes ☐ |
| Attachments are uploaded by: | ☐ Internal Users (XXXX Staff/ Staff Aug) | **External Users** With an XXXX Account (I.E. RACF, ISA or Azure B2C) [Definition] | ☐ **External Users** with out XXXX Account |
| This system uses the following for electronic document storage: | | | |
| ☐ | Department's Enterprise Electronic Document Management System (EEDMS) - Describe the type of documents stored: | | |
| ☐ | Other – Describe the type of documents stored: | | |
| This system requires the upload of documents that may contain confidential or sensitive information: | ☐ Yes | | ☐ No |
| If No is checked above, are users notified that they should not upload documents with confidential or sensitive information? | ☐ Yes | | ☐ No |

## Section 5.6 Confidential or Sensitive Information and Personally Identifiable Information (PII)

| | | |
|---|---|---|
| This system contains information that is classified as confidential or sensitive according to the Florida Public Records Act, Section 119.071, Florida Statutes,<br>AND / OR<br>This system contains information that is classified as personally identifiable information (PII) according to Security of Confidential Personal Information, Section 501.171, Florida Statutes. **(Help)** | No ☐ | Yes ☐<br>***Complete below*** |

| **List Business Data Elements and Indicate Category:** *(explain below how data will be secured)* | | | **Business Data Element Available To:** | | | ****Business Data Element Included in External Transmission:** *(explain below)* | | |
|---|---|---|---|---|---|---|---|---|
| **Business Data Element Name** | **Conf./ Sensitive** | **PII** | **Internal Users** | **External Users** | ***Unauth. Users** *(explain below)* | **Batch Jobs** | **Reports** | **Email or FTP** |
| | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

| |
|---|
| **Explain the method(s) used to secure each type of confidential/sensitive information and/or PII inside the system:** |
| ***If any confidential/sensitive information or PII in the system is available to unauthenticated users (users without a system account), please explain:** |
| ****Describe method(s) to protect data exposed through batch jobs, reports intended for extract or printing, and/or electronic means such as email or FTP:** |

## Section 5.7 Credit Card Processing

| | | |
|---|---|---|
| This system will process credit card information | No ☐ | Yes ☐ |
| Does this system allow XXXX Staff/System Users to input credit card information on behalf of someone else?<br>If Yes, Which System Role allows this? | No ☐ | Yes ☐ |
| Does this system allow XXXX Staff/System Users to view credit card information submitted by someone else?<br>If Yes, what information is viewable?<br>**Viewable Information**:<br>If Yes, which System Role allows this? | No ☐ | Yes ☐ |
| A Desk Procedure must be established to document how credit card information must be handled and protected. Include the Desk Procedure as an appendix to this plan. | Required | |
| Who is your Credit Card Processing Vendor? | | |
| Reminder: Credit Card Processing Surveys are required annually by the Florida CFO. Surveys are sent directly to the System Owners for systems that process credit card transactions. These must be completed and returned. | | |

# *Section 6 Critical Resources*

*State whether or not the system is considered a critical resource by the system's Functional Coordinator. Explain the system criticality status, requests, events, logs, and transactional history. Also, explain the backup and recovery procedures, and the records retention requirements.*

## Section 6.1 System Criticality Status

| | | |
|---|---|---|
| **Is this a Critical System?**<br>▪ Systems and assets, whether physical or virtual so vital to the U.S. that the incapacity or destruction of such systems and assets would have **a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.**<br>▪ Applies to Applications, XXX Resources and Other Agency Tools | No ☐ | Yes ☐ |
| **Is this a Critical Process?**<br>▪ A process that is susceptible to fraud, cyberattack, unauthorized activity, or **seriously impacting an agency's mission.**<br>▪ Applies to XXXX Business Intelligence Reports, Dashboards and Other Reporting Tools | No ☐ | Yes ☐ |
| This system requires essential personnel to be on call in emergency situations | No ☐ | Yes ☐ |
| **Describe:** | | |

## Section 6.2 Events, Logs, and/or Transaction History

| | | |
|---|---|---|
| Does this system have business unit requirements (policy, statute, functional, etc.) for audit logs, event logs or transaction history? | No ☐ | Yes ☐ |
| **Explain the requirement and how it is met:** | | |

## Section 6.3 Backup and Recovery

| This system's equipment resides at the following: | | |
|---|---|---|
| XXX Datacenter | | ☐ |
| District Datacenter (District #) | | ☐ |
| Azure | | ☐ |
| Other. Specify location: | | ☐ |
| Documented backup and recovery processes at the above location(s) are followed for this system's equipment: | Yes ☐ | No ☐ |
| **Explanation:** | | |

## Section 6.4 Record Retention

| This system includes records that must be retained according to the State of Florida General Records Schedule GS1 or XXXX Specific Records Schedule | No ☐ | Yes ☐ |
|---|---|---|

| Schedule Item Name and Number | Minimum Retention Period | System Meets Requirement? | System Exceeds Requirement? |
|---|---|---|---|
| | | Yes ☐ No ☐ | Yes ☐ No ☐ |
| | | Yes ☐ No ☐ | Yes ☐ No ☐ |

| Do you have a documented manual or automated process that removes records when they have met their wanted retention? If so, describe in Explanation section below. | No ☐ | Yes ☐ |
|---|---|---|
| Explanation: | | |

# *Section 7 Federal Information Processing Standards 199 Potential Impact Categorization*

The Federal Information Process Standards (FIPS), Publication 199 is the standard that determines the risk category of a system. FIPS 199 categorizes the risk of a system according to three measures: Confidentiality, Integrity and Availability. Within these three measures, a rating of Low, Medium or High is determined. The steps include:

1. Identifying the Information Types in the system.
2. Determine the potential impact of Confidentiality on all Information Types in the system.
3. Determine the potential impact of Integrity on all Information Types in the system.
4. Determine the potential impact of Availability on all Information Types in the system.
5. Identify the overall System category based on the information in steps 2-4.

## Section 7.1 Identifying Information Types

*Read the February 2004 Federal Information Processing Standards (FIPS) Publication and identify the potential impact for each FIPS security objective for this system and the data it will contain. Consider the impact to XXXX and the impact to any possible external users and stakeholders when determining the impact for each security objective (Confidentiality, Integrity, and Availability).*

*An Information Type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation. For example, a vehicle rental system could have information types such as* ***Vehicle Specifications, Customer Information,*** *and* ***Inventory Data****. It is understood that users could potentially enter information that is not expected. The Information Types listed here are the Information Types that* ***are expected*** *to be entered into the system by design and/or intent.*

*Identify all the Information Types in the system and place them in Table 1. List those information types in Tables 2, 3 and 4 to determine the overall rating for Confidentiality, Integrity and Availability. Use this information to determine the Potential Impact Summary (Table 5). Instructions and a sample of the completed tables can be referenced in the XXX Security Plan Instructions document.*

**Table 1: System Information Types**

| DEA Information Types | |
|---|---|
| **Information Type** | **Description** |
| | |
| | |
| | |

## Section 7.2 Confidentiality Potential Impact

*List each Information Type in Table 1 in Table 2 and determine the Potential Impact regarding Confidentiality.*

**Table 2: Confidentiality Potential Impact Table**

| POTENTIAL IMPACT – Confidentiality | | | |
|---|---|---|---|
| Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542] | | | |
| **Information Type** | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. **LOW** | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. **MODERATE** | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. **HIGH** |
| | ☐ | ☐ | ☐ |
| | ☐ | ☐ | ☐ |
| | ☐ | ☐ | ☐ |
| **Overall Confidentiality** *Select the highest level chosen in this table.* | **Low** ☐ | **Moderate** ☐ | **High** ☐ |

## Section 7.3 Integrity Potential Impact

List each Information type in Table 1 in Table 3 and determine the Potential Impact regarding Integrity.

**Table 3: Integrity Potential Impact Table**

| POTENTIAL IMPACT – Integrity | | | |
|---|---|---|---|
| Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542] | | | |
| **Information Type** | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. **LOW** | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. **MODERATE** | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. **HIGH** |
| | ☐ | ☐ | ☐ |
| | ☐ | ☐ | ☐ |
| | ☐ | ☐ | ☐ |
| **Overall Integrity** *Select the highest level chosen in this table.* | **Low** ☐ | **Moderate** ☐ | **High** ☐ |

## Section 7.4 Availability Potential Impact

List each Information type in Table 1 in Table 4 and determine the Potential Impact regarding Availability.

**Table 4: Availability Potential Impact Table**

| POTENTIAL IMPACT - Availability | | | |
|---|---|---|---|
| Availability - Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542] | | | |
| **Information Type** | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. **LOW** | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. **MODERATE** | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. **HIGH** |
| | ☐ | ☐ | ☐ |
| | ☐ | ☐ | ☐ |
| | ☐ | ☐ | ☐ |
| **Overall Availability** *Select the highest level chosen in this table* | **Low** ☐ | **Moderate** ☐ | **High** ☐ |

## Section 7.5 Potential Impact Table

The potential impact for the entire system is based on the highest value (high-water mark) represented in the Confidentiality, Integrity and Availability Tables above. Use the highest ranked value from the information types identified.

**Table 5: System Potential Impact Table**

| POTENTIAL IMPACT SUMMARY | | |
|---|---|---|
| **Low** ☐ | **Moderate** ☐ | **High** ☐ |

# *Section 8 Roles and Responsibilities*

*Identify the system roles involved in maintaining the integrity and security of the system, and identify the individuals who will fulfill the responsibilities of those roles.*
*NOTE: If your system does not use ISA, that section should be marked Not Applicable.*

This section identifies the positions within the Department responsible for the security of the system. The policies and procedures for the system security are formulated and directed by these positions.

## Section 8.1 System Owner

The System Owner is the manager responsible for the business function the system supports.

The System Owner for this system is: **System Owner**— Office

The System Owner's responsibilities include:

1. Designating an individual to serve as the System Security Coordinator
2. Designating an individual to serve as the Functional Coordinator
3. Ensuring the system is developed to comply with the XXXX policies, procedures, and other statutory requirements which apply to the business function(s) covered by the system
4. Ensuring the Project Team is made aware of business requirements which may impact the security specifications of the system. This includes information about data risk (Section 5) and data classification (Section 7)
5. Annual recertification of all user access and permission levels (this task can be delegated no lower than the System Security Coordinator)
6. Reporting any security incidents immediately to Information Security. Security incidents include, but are not limited to, unauthorized access to the system, confidential data exposure, personally identifiable information (PII) exposure, and misuse of the application or its data.

## Section 8.2 System Security Coordinator

The System Security Coordinator is a representative from the functional business area charged with monitoring and implementing security controls for the system.

The System Security Coordinator for this system is: **System Security Coordinator** — Office

The System Security Coordinator's responsibilities include:

1. Verifying that all system users possess a valid XXXX user ID
2. Managing user access to the system by approving the addition and removal of user system access in XXXX as listed in Section 3.1 System Roles and System Access Requests
3. Grants the appropriate access to the system by assigning users to a group for the system's user roles listed in Section 3.1 System Roles and System Access Requests
4. Reviewing the system's Security Plan and attending security training sessions to stay informed of changes in security policies and procedures

5. Performing periodic audits of the authorized system users to ensure that only authorized personnel have access to the system and that each person has the appropriate authority for their function
6. Reporting any security incidents immediately to Information Security. Security incidents include, but are not limited to, unauthorized access to the system, confidential data exposure, personally identifiable information (PII) exposure, and misuse of the application or its data.

## Section 8.3 Functional Coordinator (FC)

The Functional Coordinator serves as a liaison between the Office of Information Technology and the functional office.

The Functional Coordinator for this system is: **Functional Coordinator** — Office

The Functional Coordinator's responsibilities include:

1. Coordinating with the appropriate functional staff to clarify requests
2. Ensuring the Project Team is aware of the XXXX policies, procedures and other statutory requirements which apply to the business function(s) covered by the system
3. Establishing priorities when multiple requests exist
4. Coordinating timely and complete functional acceptance testing
5. Providing approval to progress any work from on phase to another, including final approval to move application modifications to the production environment.
6. Reporting any security incidents immediately to Information Security. Security incidents include, but are not limited to, unauthorized access to the system, confidential data exposure, personally identifiable information (PII) exposure, and misuse of the application or its data.

## Section 8.4 Enterprise Data Steward

The Enterprise Data Steward (EDS) is a Data Steward who is responsible for managing the Data Steward Working Group for their assigned functional area. Data Stewards are business-focused individuals from both the District and Central Offices who serve as the business function experts for their functional area data. Enterprise Data Stewards work closely with the Data Stewards within their functional area to establish appropriate data governance policies, processes, and procedures.

Review the list of Enterprise Data Stewards or email the list xxxx-xxx Leadership for assistance in identifying the Enterprise Data Steward.

The Enterprise Data Steward for this system is: **Name** – Office

The Enterprise Data Steward's responsibilities include:

1. Lead the Data Steward Working Group
2. Ensures Data Governance Compliance
3. Works with Data Stewards and Custodians

## Section 8.5 ISA System Administrator

The ISA System Administrator is responsible for assisting their system users with ISA-related issues.

The ISA System Administrator for this system is: **Name** — Office (mark this item N/A if the system does not use ISA.)

The ISA System Administrator's responsibilities include:

1. Maintaining ISA user access to the system by activating or inactivating ISA users as necessary
2. Granting the appropriate access to the system by placing them in a group for the system's user roles
3. Supporting the system's ISA users with login-related issues
4. Resetting ISA passwords for external users
5. Reporting any security incidents immediately to Information Security. Security incidents include, but are not limited to, unauthorized access to the system, confidential data exposure, personally identifiable information (PII) exposure, and misuse of the application or its data.

# *Section 9 XXXX Policies and Procedures*

*The XXXX Policies and Procedures listed below are applicable to all systems.* ***Add any additional policies and procedures not listed below that are applicable to your system.***

**Department of XXXXXXXXX Policies, Procedures and Governing Statutes**

The Department's policies and procedures relating to access of computers and data are governed by statutes, codes and procedures. The policies and procedures identified are included in their entirety by reference and are only repeated selectively.

- Chapter 119, Florida Statutes: Public Records Law
- Chapter 282, Florida Statutes: Communications and Data Processing
- Chapter 815, Florida Statutes: Computer Related Crimes
- XXXXXXX Technology Manual, Chapter 2, *Access to the Department's XXXXXX Technology Resources*, effective July 1, 2019
- XXXXXXX Technology Manual, Chapter 5, *Electronic Security for Public Records Exemptions*, effective July 1, 2020
- Procedure 325-060-020 Security and Use of Information Technology Resources
- Florida Administrative Code 60GG-1: Project Management and Oversight
- Florida Administrative Code 60GG-2: Florida Cybersecurity Standards (FCS)
- Florida Administrative Code 60GG-5: Identity Management

## *Section 10 Document Revision History*

*Identify revisions to the document starting with initial creation. This section should be updated when an approval is required (i.e., initial creation, change request, new mandated change, etc.).*

| Version | Date | Name | Description |
|---|---|---|---|
| Version 1.0 | Month Day, 20xx | Jim Bob | Initial creation |
| | | | |

## *Section 11 References*

*Identify any other documents referenced in this Security Plan and provide links if they are available. This can include documents such as user manuals and functional specifications.*

| Document No. | Document Title | Date | Author |
|---|---|---|---|
| | | | |
| | | | |

# *Section 12 Vulnerability Assessment*

*Information Security will conduct a vulnerability scan on the system and then analyze the results and provide any recommendations. Allow 5-7 business days for the scan, analysis, and recommendations to be complete.*

**NOTE**: This section will be completed by the Information Security team after the Security Plan is submitted.

| | |
|---|---|
| ☐ | **The resources are located in Azure.** |
| ☐ | **The resources are located in a different cloud service. Vulnerability management is handled by the company providing the service.** |
| ☐ | **Other:** |
| ☐ | **Vulnerability scans performed are listed below:** |

| Date Scanned | Host Name or IP Address | Scanning Tool Used | Person or Team performing scan | Summary of Scan Results |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

# *Section 13 Appendices*

*Include any relevant appendices.*

# *Appendix A: Definitions and Standards*

Enterprise Business Glossary

Application Owner (System Owner)

The business unit that requested the application be developed and/or purchased; the individual (usually a manager) from the business unit(s) for which an application is acquired who has responsibility and authority to make decisions related to the application, such as requirements, deliverable approvals, access, etc.

**Application Programming Interface (API)**

A set of routines, protocols, and tools for building software applications.

**Automated Access Request Form (XXXX)**

XXXX is XXXX's system to request access to applications and systems statewide. XXXX is used to request the creation of Active Directory and RACF accounts, and to request access to individual systems. XXXX presents a list of Access Items that can be requested. Some systems have multiple access items to represent the varying levels of access (referred to as roles or entitlements) that can be granted. Access requests must be approved by appropriate staff before system access is granted. The XXXX system notifies the teams that can grant access once approval is received. The XXXXXXX Technology Manual (Chapter 2, Section 2.2.1) requires that all system access is requested through XXXX **(**Instructions for including your system in XXXX).

**Digital Certificates and Electronic Signatures**

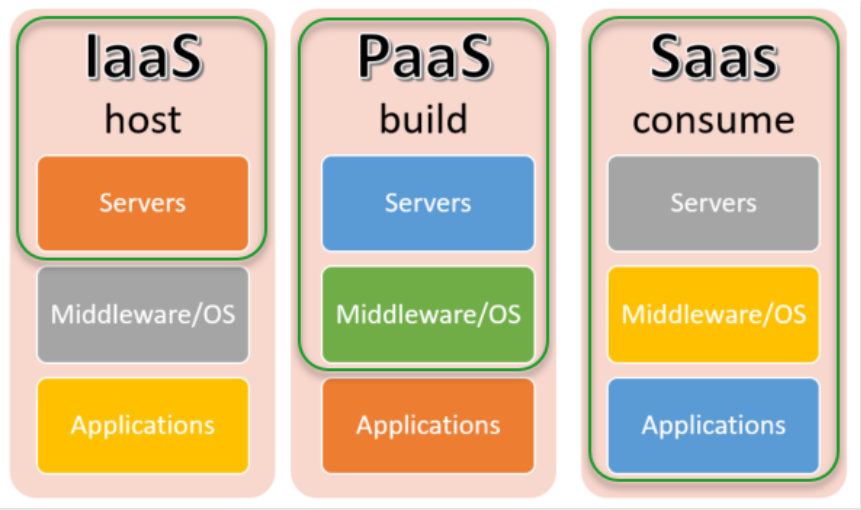
- A certified digital certificate "means a computer-based record which: identifies the certificate authority, identifies the subscriber, contains the subscriber's public key, [and] is digitally signed by the certification authority," section 668.003(1)(a)-(d), F.S.
- An electronic signature "means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record," section 668.50(2)(h), F.S.

Please see Chapter 21 of the XXXXXXX Technology Manual for XXXX's minimum requirements and standards for acquiring, managing, and using digital certificates.

**Cloud Model**

Describes the type of cloud service (Section 4.11 Cloud Environment).

- Software as a Service (SaaS) – Software made available by a third-party provider that hosts the application and makes it available to customers over the Internet; these are often called Web Services. Microsoft Office 365 is a SaaS offering for productivity software and email services.
- Platform as a Service (PaaS) – Hosted development tools provided on the infrastructure of a third-party provider. Users access these tools over the Internet using APIs, Web portals or gateway software. Examples of PaaS providers include Salesforce.com, Windows Azure and Google App Engine.
- Infrastructure as a Service (IaaS) – Hosted form of cloud computing that provides virtualized computing resources over the Internet.




**Custom Off the Shelf (COTS)**

Software or hardware products that are ready made and available for purchase by the general public.

**Data Steward**

Data Stewards are business-focused individuals from both the District and Central Offices who serve as the business function experts for their functional area data. They work closely with their functional area Enterprise Data Stewards to establish appropriate data governance policies, processes, and procedures.

**Database**

An organized collection of data including tables, schemas, views, reports, and other objects.

**Encryption**

The reversible process of transforming readable text into unreadable text (cipher text).

**Enterprise Data Steward**

The Enterprise Data Steward (EDS) is a Data Steward who is responsible for managing the Data Steward Working Group for their assigned functional area. A job role that involves planning, implementing and managing the sourcing, use and maintenance of data assets in an organization. Data stewards enable an organization to take control and govern all the types and forms of data and their associated libraries or repositories.

**External Users**

XXXX has two types of External Users.

- System users such as external consultants, business partners that have been assigned access to XXXX Systems using XXXX's primary authentication method (Active Directory or RACF).

System users such as citizens and business partners that have been assigned access to XXXX Systems using secondary accounts such as ISA or Azure B2C. This can, at times, include unauthenticated access

**XXXX Developed System**

Custom-developed by XXXX staff or staff under contract by XXXX.

**XXXX's Password Requirements**

For password requirements, please reach out to the Information Security office.

**XXXX's Web Browser Standards (updated 08/08/2022)**

1. Microsoft Edge
2. Google Chrome

**Functional Coordinator (FC)**

Also known as Functional Application Coordinator (FAC). A dedicated resource from the functional office assigned to serve as liaison between the Office of Information Technology and the functional office. The Functional Coordinator may act as an agent for the application owner and is responsible and accountable for: (1) coordinating with the appropriate functional staff to clarify requests, (2) establishing priorities when multiple requests exist, (3) coordinating the timely and complete functional acceptance testing, and (4) providing approvals to progress any work from one phase to another, including final approval to move application modifications to the production environment. In cases where there are three or more closely related, interdependent applications that process together as a suite, A FC must be appointed to act as the overall coordinator for the applications within the suite. The suite FC is responsible for coordinating and communicating with the individual FCs and the Application Services Bureau on issues that affect the overall suite of applications. This includes coordination and prioritization of service requests among the functional application coordinators within the suite, production support, suite-wide maintenance releases, user notification, and system integration testing coordination.

**Generic Account**

An approved account used for such purposes as a training room and testing computer applications that have restricted access controls in place to prevent unauthorized use.

**High Availability**

Refers to a system or component that is continuously operational for a desirably long length of time. Availability can be measured relative to "100% operational" or "never failing."

**Information Type**

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

**Internal Users**

System users who are XXXX staff, including staff augmentation and internal consultants.

**Multi-Factor Authentication**

The requirement to provide at least two methods of authentication from the following categories: knowledge (something the know, ex. password), possession (something they have, ex. debit card), inherence (something they are, ex. biometrics).

**Network Port**

An endpoint of communication in an operating system. A logical construct that identifies a specific process or a type of service.

**Personally Identifiable Information (PII) (501.171, F.S.)**

(g)1. "Personal information" means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

**Project Manager**

A Department employee who ensures that project scope, cost, and schedule are maintained in accordance with the baselines established in the Project Management Plan. The Project Manager is responsible to lead the project team by planning, assigning, and overseeing the deliverables of the project towards achieving the project's objectives.

**Production**

The Production environment is used for production work only. The System Administrators grant access to this environment for update and create authority. Developers do not have access to production or production data.

**Production Migration Procedures**

Upon approval by the System Owner or Functional Coordinator, the Project Manager submits an email to their Program Manager identifying the application components being requested to move to Production. The Program Manager reviews and approves the production move and emails the appropriate support group. If there are any database issues, an Electronic Florida DOT Database Administration Form is submitted by the Program Manager to the DBA group for processing.

**Service Account**

An account used by a computer process and not by a human (e.g., an account used by the backup process for file access). Normally service accounts may not log on to a system.

**System** (Application)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information resources include components such as database servers, web servers, application servers, custom-written applications, custom off the shelf (COTS) systems and hosted arrangements such as Software as a Service (SaaS). Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

**System Administrator**

A person who manages the technical aspects of a system. Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

**System Hardening**

Reducing the attack surface or surface of vulnerability by following a process or by configuring a system in a particular manner.

**System Owner** (Application Owner)

The business unit that requested the application be developed and/or purchased; the individual (usually a manager) from the business unit(s) for which an application is acquired who has responsibility and authority to make decisions related to the application, such as requirements, deliverable approvals, access, etc.

**System Security Coordinator** (Application Security Coordinator)

The role assigned to individuals that are responsible for monitoring and implementing security controls and ensuring compliance with procedures for applications or information technology environments. A Traditional Select Exempt Service (SES) or Senior Management Service (SMS) manager selects computer security coordinators.

**System Test**

The System Test environment is the second level testing environment. This is where the Users will perform their User Acceptance testing and is the staging environment for Production migrations. The system test environment is also used for production problem resolution and debugging. This environment and the production environment should be identical in terms of system versions and programs.

**Thick Client Application** (Fat Client Application, Rich Client Application)

An application that resides on a computing workstation that has most resources (Hard Drives, Memory, applications, etc.) installed locally.

**Unit Test**

The Unit Test environment is used to perform testing of new system releases, patches and programs. It is the first level testing environment where developers can perform integration testing to ensure that the application works correctly in XXXX's server environment and with the other enterprise systems it might be interacting with.