

GovRAMP

{Insert CompanY Name}

Security Procedures

System Services and Acquisition [SA]

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

Table of Contents[Document Revision History 1](#_Toc196464729)

[Table of Contents 2](#_Toc196464730)

[1 Introduction 4](#_Toc196464731)

[2 Purpose 4](#_Toc196464732)

[3 Scope 4](#_Toc196464733)

[4 Roles and Responsibilities 4](#_Toc196464734)

[5 Management Commitment 5](#_Toc196464735)

[6 Authority 6](#_Toc196464736)

[7 Compliance 6](#_Toc196464737)

[8 Procedural Requirements [SA-1] 7](#_Toc196464738)

[8.1 Allocation of Resources [SA-2] 7](#_Toc196464739)

[8.2 Software Development Life Cycle [SA-3] 7](#_Toc196464740)

[8.3 Acquisitions Process [SA-4] 8](#_Toc196464741)

[8.4 Information System Documentation [SA-5] 9](#_Toc196464742)

[8.5 Security and Privacy Engineering Principles [SA-8] 10](#_Toc196464743)

[8.6 External Information System Services [SA-9, SA-9 (2), SA-9 (5)] 10](#_Toc196464744)

[8.7 Developer Configuration Management [SA-10] 11](#_Toc196464745)

[8.8 Developer Security Testing and Evaluation [SA-11] 12](#_Toc196464746)

[8.9 Development Process, Standards, and Tools [SA-15] 13](#_Toc196464747)

[8.10 Unsupported System Components [SA-22] 13](#_Toc196464748)

# Introduction

{Insert Company Name} has developed corporate procedures that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These procedures are set forth by {Insert Company Name}’s management and in compliance with the System Services and Acquisition family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

# Purpose

The purpose of these procedures is to establish processes for acquiring, developing, and managing system services within {Insert Company Name}. These procedures ensure secure and compliant acquisitions while maintaining the integrity, confidentiality, and availability of organizational systems, in alignment with the System Services and Acquisition Policy and applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these procedures pertain to all {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These procedures apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

|  |  |  |
| --- | --- | --- |
| **Individual or Group** | **Role** | **Responsibility** |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for {Insert Information Security Department Name} objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with {Insert Information Security Department Name} policies, procedures, and controls. Has final responsibility for {Insert Information Security Department Name} program. |
|  | Information Owner | Has statutory, management, or operational authority for {Insert Company Name} information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | {Insert Individual or Team Name} | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | {Insert Individual or Team Name} | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | {Insert Information Technology Department Name} Director | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
| System Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company Name} and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company Name} Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these procedures is mandatory. It is {Insert Company Name}’s policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these procedures by using an independent audit performed by an external vendor and/or internal self-assessments to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Procedural Requirements [SA-1]

The following system and services acquisition requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company Name} information systems.

## Allocation of Resources [SA-2]

{Insert Information Security Department Name} and privacy requirements are developed and documented during the planning process for the {Insert Information System Name} Information System. [SA-2 (a)] The {Insert Individual or Team Name}, in coordination with the {Insert Individual or Team Name} and the {Insert Individual or Team Name}, are responsible for documenting and maintaining the security requirements for the information system on an ongoing basis. These requirements are reviewed annually to ensure the mitigation of current security risks and legal requirements.

Prior to the introduction of a new information system component, the {Insert Individual or Team Name}, in coordination with the {Insert Individual or Team Name} and the {Insert Individual or Team Name}, must ensure the {Insert Information Security Department Name} requirements are considered and addressed in the planning and certification of the information system. [SA-2 (b)]

{Insert Company Name} Leadership, in coordination with the {Insert Individual or Team Name} and the {Insert Individual or Team Name}, will, on a yearly basis, ensure that appropriate funding is forecasted and provided for the functions of the {Insert Individual or Team Name} and components utilized by that team, thereby ensuring the protection of the {Insert Information System Name} Information System. Once the requirements are determined, they are presented to executive leadership for final approval, which determines the security budget for the {Insert Information System Name} Information System. [SA-2 (c)]

## Software Development Life Cycle [SA-3]

{Insert Company Name}’s Software Development Lifecycle (SDLC) is based upon the Agile framework and incorporates security and privacy best practices. [SA-3 (a)]

{Insert Company Name} identifies individuals having {Insert Information Security Department Name} roles and responsibilities in its Software Development Lifecycle Policy (SDLC), version {Insert Version Number}, dated {Insert published date}, Section {Insert section identifier}. [SA-3 (b)]

The first phase of the SDLC is design and planning, which begins when a new feature is being considered. Each new feature consideration is entered into {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)} to track and manage the workflow.

The {Insert Software Development Team Name} in conjunction with the {Insert Individual or Team Name}, where appropriate, determines the security and privacy requirements for the new feature. Once the requirements are approved by the {Insert Software Development Team Name} and the Product Owner, the feature is moved into the development queue to be built and tested. [SA-3 (c)]

Development personnel are responsible for writing the code for the new feature and having it peer reviewed. Multiple features are bundled together along with legacy code to produce a new build of the {Insert Information System Name} application. In addition to peer reviews, builds undergo login tests and code analysis using a static code scanning tool.

The build is then passed to the {Insert Quality Assurance Team Name} Team for further review and testing, including regression and manual testing. If any bugs or issues are found, the code is sent back to the {Insert Software Development Team Name} for remediation. All test results are documented within {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}.

Once the build has passed all required testing, it is prepared for deployment to production and notifications are posted in {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)} to announce the changes.

The security risk management process is integrated into the SDLC through static code analysis and vulnerability identification and risk monitoring. In addition to being applied to the production environment, the same security and privacy risk assessment methodologies are implemented in the development environment to provide security considerations during the entire SDLC process. [SA-3 (d)]

## **Acquisitions** Process [SA-4]

Prior to the acquisition or outsourcing of dedicated {Insert Information Security Department Name} services, the requirements for the service below are determined and documented explicitly or by reference. The {Insert Individual or Team Name} and {Insert Individual or Team Name} review the requirements and list of potential products and vendors. The {Insert Individual or Team Name} engages with the {Insert Procurement Department Name} to begin the product qualification process once the requirements are defined. Once a product is chosen and approved, the {Insert Procurement Department Name} acquires the product or service. {Insert Company Name} requires these descriptions and criteria for information system acquisition contracts: [SA-4]

* Security and privacy functional requirements [SA-4 (a)]
* Strength of mechanism requirements [SA-4 (b)]
* Security and privacy assurance requirements [SA-4 (c)]
* Controls needed to satisfy the security and privacy requirements [SA-4 (d)]
* Security and privacy documentation requirements [SA-4 (e)]
* Requirements for protecting security and privacy documentation [SA-4 (f)]
* Description of the system development environment and environment in which the system is intended to operate [SA-4 (g)]
* Allocation of responsibility or identification of parties responsible for {Insert Information Security Department Name}, privacy, and supply chain risk management, and [SA-4 (h)]
* Acceptance criteria [SA-4 (j)]

{Insert Company Name} requires {Insert Information System Name} developers to provide a description of the functional properties of the security control to be implemented in the system, system component, or system service. [SA-4 (1)] Developers (including internal resources) of the system, system component, or system services are required to provide design and implementation information of the security controls. The implementation documentation information must include: [SA-4 (2)]

• Security-relevant external system interfaces

• High-level or low-level design such as source code

• Configuration changes

• Architectural summary

{Insert Company Name} requires developers of systems, system components, or system services to identify the functions, ports, protocols, and services required for use. [SA-4 (9)]

## Information System Documentation [SA-5]

The {Insert Individual or Team Name} ensures that user documentation, including user-accessible security functions, methods for user interaction and secure access, and user responsibilities is made available. {Insert Company Name} {Insert Information Security Department Name}, {Insert Information Technology Department Name}, and {Insert Software Development Team Name} teams are responsible for ensuring documentation is available that describes:

* Secure configuration, installation, and operation of the information system, system component, or system service [SA-5 (a) (1)]
* Effective use and maintenance of security and privacy features/functions [SA-5 (a) (2)]
* Known vulnerabilities regarding configuration and use of administrative or privileged functions [SA-5 (a) (3)]

{Insert Company Name} obtains user documentation for the information system, system component, or information system service that describes: [SA-5 (b)]

• User-accessible security and privacy functions/mechanisms and how to effectively use those security and privacy functions/mechanisms [SA-5 (b) (1)]

• Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy [SA-5 (b) (2)]

• User responsibilities in maintaining the security of the system, component, or service and privacy of individuals [SA-5 (b) (3)]

If an attempt is made to retrieve specific documentation that is unavailable or nonexistent, a request is made to the manufacturer of the information system, system component, or information system service for the documentation. The {Insert Individual or Team Name} works to obtain the documentation from the vendor or works with the applicable stakeholders to create the documentation themselves. [SA-5 (c)]

{Insert Company Name} uses {Insert Name of Document Repository} to house all administrative documentation. {Insert Name of Document Repository} uses authentication mechanisms for users to gain access and provides a file structure for documentation storage. {Insert Company Name} implements least privilege when granting user privileges within {Insert Name of Document Repository}. Users are only able to review documentation that is associated with their specific role and responsibility. [SA-5 (d)]

## Security and Privacy Engineering Principles [SA-8]

The Software Development Lifecycle (SDLC) methodology used for the {Insert Information System Name} Application is built into the configuration management process through the use of security and privacy engineering principles for the development and ongoing maintenance of the {Insert Information System Name} Application. The SDLC adheres to the NIST security and privacy principles. The workflows for the SDLC process are managed and tracked within {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}.

{Insert Company Name} performs ongoing vulnerability scanning and flaw remediation to mitigate security vulnerabilities and reduce risk to an acceptable level. {Insert Company Name} performs system scans to discover any potential vulnerabilities. Additional scans are conducted when an application or service is added or reconfigured within the {Insert Information System Name} Information System. [SA-8]

## External Information System Services [SA-9, SA-9 (2), SA-9 (5)]

Third-party providers must comply with the {Insert Company Name} Information System security requirements and have deployed security controls that are in accordance with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. [SA-9 (a)] The {Insert Individual or Team Name} ensures the contract contains requirements for adequate security controls, including organizational oversight and user roles and responsibilities, and that these controls are documented when contracting with third-party providers. [SA-9 (b)]

{Insert Company Name} conducts an organizational assessment of risk prior to the acquisition or outsourcing of {Insert Information Security Department Name} services. [SA-9 (1) (a)] The acquisition or outsourcing of these dedicated {Insert Information Security Department Name} services, if needed, is approved by the Authorizing Official, Authorizing Official designated representative, or appropriate {Insert Company Name} personnel. [SA-9 (1) (b)]

{Insert Company Name} requires that providers of external information system services identify the functions, ports, protocols, and other services required for the use of such services. [SA-9 (2)] This information is recorded in {Insert Company Name}’s {Insert Name of Document Repository}. {Insert Company Name} also employs or verifies safeguards on all external information systems where StateRAMP information is processed or stored.

The {Insert Individual or Team Name} is largely responsible for the acquisition and ongoing operation of external services. The IT and {Insert Individual or Team Name}s work closely with the team dependent on the external service to continue evaluation and oversight of the external service.

The external information system services used to support the {Insert Information System Name} web application include: {Modify list, below, as necessary}

* **{Insert Hosting Provider}** contains the infrastructure used to run and manage the {Insert Information System Name} web application.
* **{Insert Identity Provider}** is used for allowing users to sign into the {Insert Information System Name} web application.
* **{Insert Vulnerability and Compliance Scan Tool Name}** is used for vulnerability management and policy compliance
* **{Insert Password Manager Tool Name}** is used to store passwords for the environment
* **{Insert Multi-factor Authentication Tool Name}** is used for Multi-Factor Authentication

{Insert Vulnerability and Compliance Scan Tool Name}, {Insert Identity Provider}, {Hosting Provider}, {Insert Password Manager Tool Name}, and {Insert Multi-factor Authentication Tool Name} are StateRAMP or FedRAMP authorized to store, process, and transmit government data or metadata, and are therefore required to adhere to StateRAMP or FedRAMP’s continuous monitoring program. [SA-9 (c)]

{Insert Company Name} restricts the location of information processing, information data, and information system services to StateRAMP or FedRAMP Authorized {Insert Hosting Provider} datacenter facilities. All physical system components reside within {Insert Hosting Provider} datacenters within the continental United States. [SA-9 (5)] All storage, processing, and transmission of system data is done in accordance with customer contracts and SLA requirements.

## Developer Configuration Management [SA-10]

{Insert Company Name} SDLC process and configuration management policy include steps associated and built for security. These processes are performed during development, implementation, and operation of the {Insert Information System Name} Information System. [SA-10 (a)] All SDLC changes are submitted via a ticket through {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)} for approval by the Product Owner. All information regarding the change is included in the ticket for documentation and tracking purposes.

The SDLC and configuration management documentation includes an in-depth explanation of all approval gates configured within {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}. These approval gates ensure integrity of code changes. [SA-10 (b)] All code must be peer reviewed and attached to a ticket and approved. To check in and deploy code, someone other than the requestor must approve the code to the staging environment.

A release of code through {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)} to production must be approved by a manager. [SA-10 (c)] The full Responsible Accountable Consulted Informed (RACI) matrix is located in the Software Development Lifecycle policy.

All artifacts related to a change are included as a part of the ticket and release in {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}. Updates or changes to code are captured by the ticket in {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}. Approvals for changes to code are documented in the release in {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}, along with the potential security and privacy impacts of the changes if necessary. [SA-10 (d)]

{Insert Company Name} tracks all security flaws and flaw remediation details of the {Insert Information System Name} Information System within bugs in {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}. These are automatically created when the static code scan is run. The static code scan is run {Insert frequency}. Scan history is stored within the static code analysis tool. [SA-10 (e)]

## Developer Security Testing and Evaluation [SA-11]

{Insert Company Name} SDLC includes steps associated with security and privacy. [SA-11 (a)] All features and releases go through multiple tests before being deployed into production. Once the requirements are defined, approved, and the build begins, {Insert Quality Assurance Team Name} develops a test plan. The build is tested against functionality and security requirements. The build is put through a series of tests once received from the {Insert Software Development Team Name}. Builds are scanned via the static code analysis tool, and the resulting security findings are documented as bugs in {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)} and assigned to the team for remediation by the Product Owner.

As part of the SDLC process, testing is performed for all releases. In the development phase, {Insert Quality Assurance Team Name} creates and reviews a test plan for each release. Once development is complete, it is deployed to {Insert Quality Assurance Team Name} for review and testing. The tests include manual testing and regression testing. [SA-11 (b)] All test results are documented within {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}. [SA-11 (c)] Automated unit tests are run for every code commit.

Prior to any review or testing of a build, {Insert Quality Assurance Team Name} documents an associated test plan within {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}. If there are any non-security related flaws found, they are documented in {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)} to ensure they are remediated prior to being pushed to production. Any security flaws discovered are documented and tracked as bugs within {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)} to ensure they are mitigated according to severity level. [SA-11 (d)] Critical findings are remediated prior to code deployment into production. Other severity levels (high, medium, low) are prioritized into an upcoming sprint. [SA-11 (e)] Once the flaw has been remediated, {Insert Quality Assurance Team Name} and the static code scans validate remediation of the finding. [SA-11 (1)]

{Insert Company Name} performs threat modeling and vulnerability analysis during development that takes into consideration the information concerning impact, the environment of operations, the known or assumed threats, and/or the acceptable risk levels. [SA-11 (2) (a)] The modeling and analysis is conducted at a level of rigor that is appropriate for the data hosted in the {Insert Information System Name} Information System, component, or service. [SA-11 (2) (c)] The results produce evidence that ensures the design and implementation changes have been accounted for, and that vulnerabilities potentially created because of those changes have been reviewed and mitigated. [SA-11 (2) (d)]

{Insert Company Name} employs the following tools and methods for threat modeling and analysis during the {Insert Information System Name} development cycle prior to code being deployed into the boundary: [SA-11 (2) (b)]

* {Insert Code Analysis Scanner Name} static code analysis scanner
* {Insert Code Analysis Scanner Name} binary code analysis scanner
* {Insert Unit Testing Tool Name} automated unit testing
* **{Amend list as necessary to include all tools used for testing}**

{Insert Company Name} employs the following tools and methods for threat modeling and analysis during the {Insert Information System Name} development cycle after code is deployed into the boundary:

* {Insert Web Application Scanning/Dynamic Code Analysis Tool Name} Web Application Scanning performs dynamic code analysis scanning

## Development Process, Standards, and Tools [SA-15]

{Insert Company Name} follows the Software Development Lifecycle Policy, version {Version}, dated {Last Published Revision Date}. This policy explicitly addresses security and privacy requirements, [SA-15 (a) (1)] identifies the standards and tools used in the development process, [SA-15 (a) (2)] documents the specific options and tool configurations used in the development process, [SA-15 (a) (3)] and documents, manages, and ensures the integrity of changes to the process and/or tools used in development. [SA-15 (a) (4)]

{Insert Company Name} reviews the development process, standards, tools, tool options, and tool configurations throughout the System Development Lifecycle (SDLC) to determine if the process, standards, tools, tool options, and tool configurations satisfy the FedRAMP Security Authorization requirements at least annually. [SA-15 (b)]

{Insert Company Name} performs a criticality analysis reviews prior to acquisition and at a level a level of rigor sufficient to maintain the integrity throughout the system development life cycle. [SA-15 (3)] These reviews are performed and stored within {Insert name of SDLC system (Jira, Azure DevOps, Verion1, etc.)}. Newly acquired products are reviewed and approved by the {Insert Information Security Department Name}, {Insert Information Technology Department Name}, and {Insert Procurement Team Name} teams as part of a procurement request.

## Unsupported System Components [SA-22]

{Insert Company Name} prefers to replace system components when support for the components is no longer available from the developer, vendor, or manufacturer. [SA-22 (a)] Alternatively, if the need for the specific sunset component persists, {Insert Company Name} makes alternative arrangements, such as in-house support, or open-source software value-added vendors. [SA-22 (b)] {Insert Company Name} acquires the source code of unsupported open-source software and libraries to enable in-house support for the software and/or libraries.