

{Insert Company Name}

Security Policy

System and Services Acquisition

**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

1 Introduction ............................................................................................................................................. 1

2 Purpose .................................................................................................................................................... 1

3 Scope ........................................................................................................................................................ 2

4 Roles and Responsibilities ........................................................................................................................ 2

5 Management Commitment ..................................................................................................................... 2

6 Authority .................................................................................................................................................. 3

7 Compliance .............................................................................................................................................. 3

8 Policy Requirements ................................................................................................................................ 4

8.1 System and Services Acquisition Policies and Procedures [SA-1] .................................................... 4

8.2 Allocation of Resources [SA-2] ......................................................................................................... 4

8.3 System Development Life Cycle [SA-3] ............................................................................................ 4

8.4 Acquisitions Process [SA-4, SA-4 (1,2,9,10). {SA-4 (5) High Only}] ................................................... 5

8.5 Information System Documentation [SA-5] ..................................................................................... 6

8.6 Security and Privacy Engineering Principles [SA-8] .......................................................................... 6

8.7 External System Services [SA-9, SA-9 (1,2,5)] .................................................................................. 6

8.8 Developer Configuration Management [SA-10] ............................................................................... 7

8.9 Developer Testing and Evaluation [SA-11, SA-11 (1,2)] ................................................................... 8

8.10 Developer Process, Standards, and Tools [SA-15, SA-15 (3)] ......................................................... 9

8.11 Developer-Provided Training [{SA-16 High Only}] ......................................................................... 9

8.12 Developer Security Architecture and Design [{SA-17 High Only}] ................................................. 9

8.13 Developer Screening [{SA-21 High Only}] .................................................................................... 10

8.14 Unsupported System Components [SA-22] ................................................................................. 10

# Introduction

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

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies 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 policies 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 information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security 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. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology 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 policies 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 policies 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.

# Policy Requirements

The following personally identifiable information processing and transparency controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

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

8.1 System and Services Acquisition Policies and Procedures [SA-1]

This document is intended to serve as the *System and Services Acquisition Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *System and Services Acquisition Policy* and related controls have been developed, documented, and disseminated to all applicable personnel.

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief privacy officer, ISSO, and/or similar roles or their designees: [SA-1 (a)]

* An organizational-level System and Services Acquisition Policy that: [SA-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [SA-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [SA-1 (a) (1) (b)]
* Procedures to facilitate the implementation of System and Services Acquisition Policy and the associated System and Services Acquisition controls [SA-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the System and Services Acquisition policy and procedures. [SA-1 (b)]

{Insert Company Name} must review and update the current System and Services Acquisition: [SA-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [SA-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [SA-1 (c) (2)]

8.2 Allocation of Resources [SA-2]

{Insert Company Name} must include a high-level determination of information security requirements for information in mission and business process planning. [SA-2 (a)] All resources required to protect information must be identified, documented, and allocated as part of {Insert Company Name} capital planning and investment control process. [SA-2 (b)] Additionally, a discrete line item must be established for information security in organizational programming and budgeting documentation. [SA-2 (c)]

8.3 System Development Life Cycle [SA-3]

{Insert Company Name} has acquired, developed, and manages the system using a System Development Life Cycle (SDLC) that incorporates information security and privacy considerations. [SA-3 (a)] {Insert Company Name} has integrated the organizational information security and privacy risk management process into the system development lifecycle activities. [SA-3 (d)] {Insert Company Name} has identified the individuals who have information security and privacy roles and responsibilities. [SA-3 (c)] {Insert Company Name} has defined and documented information security and privacy roles and responsibilities throughout the system development life cycle. [SA-3 (b)]

8.4 Acquisitions Process [SA-4, SA-4 (1,2,9,10), {SA-4 (5) High Only}]

{Insert Company Name} shall have the following requirements, descriptions, and criteria, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, and standards, which may be in the form of standardized contract language for the system, system component, or system service: [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 information security, privacy, and supply chain risk management, and [SA-4 (h)]
* Acceptance criteria [SA-4 (j)]

{Insert Company Name} requires system developers to provide a description of the functional properties of the security controls to be implemented in the system, system component, or system service. [SA-4 (1)] Developers 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)]

{Insert Company Name} must employ information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability within systems used by the Federal government. [SA-4 (10)]

**For high impact systems only:**

{Insert Company Name} requires system developers to deliver systems, components, or services adhering to the hardening guidelines contained within the Configuration Management Policy Section 8.6 *Configuration Settings*. [SA-4 (5) (a)] {Insert Company Name} requires the developer’s system, components, or services to implement the hardening guidelines contained within the Configuration Management Policy in Section 8.6 *Configuration Settings*, as the default of any subsequent system, component, or service reinstallation or upgrade. [SA-4 (5) (b)]

8.5 Information System Documentation [SA-5]

{Insert Company Name} must obtain or develop administrator documentation for the system, system component, or system service that describes:

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

{Insert Company Name} must obtain or develop user documentation for system, system component, or system service that describes:

* User-accessible security and privacy functions and mechanisms and how to effectively use those security functions and 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)]

{Insert Company Name} must document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and create the documentation in response. [SA-5 (c)] The documentation shall be distributed to all employees or contractors who have a need to know and to include, at a minimum, the agency ISSO. [SA-5 (d)]

8.6 Security and Privacy Engineering Principles [SA-8]

{Insert Company Name} must apply systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components using an industry recognized Risk Management Framework (RMF) appropriate for the information system and as required by the system’s intended clientele such as NIST SP 800-53r5, NIST CSF 2.0, SSAE 18 SOC 2, or ISO27001. [SA-8]

* Systems hosting Federal government data or metadata must adhere to the FedRAMP RMF and be listed in the FedRAMP marketplace.
* Systems hosting state government data or metadata must adhere to the StateRAMP RMF and at a minimum have a StateRAMP progressing snapshot available.
* Systems hosting corporate data should have a SOC2 or similar verification report available and must be approved by the Information Security management prior to implementation.

8.7 External System Services [SA-9, SA-9 (1,2,5)]

{Insert Company Name} must:

* Require that providers of external information system services comply with organizational security and privacy requirements. [SA-9 (a)]
  + If Federal information is processed or stored within the external system, the external provider must employ the appropriate FedRAMP Security Controls Baselines
* Define and document organizational oversight and user roles and responsibilities regarding external information system services [SA-9 (b)]
* Employ processes, methods, and techniques to monitor control compliance by the external service providers on an ongoing basis and document the trust relationship to be monitored [SA-9 (c)]
  + If Federal or state government information is processed or stored within the external system, the provider must utilize NIST SP 800-137 Continuous Monitoring guidance
  + If corporate data is processed or stored within the external system, {Insert Company Name} should work with the vendor to develop Service Level Agreements (SLAs) that define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance
* Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services [SA-9 (1) (a)]
* Verify that the acquisition or outsourcing of dedicated information security services is approved by the AO, AO Designated Representative, or appropriate {Insert Company Name} personnel [SA-9 (1) (b)]
* Require providers of any external system services to identify the functions, ports, protocols, and other services required for the use of such services on all external systems where government information is processed or stored [SA-9 (2)]
* Restrict the location of information processing, information or data, and system services to U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction based on all impact level data, systems, or services [SA-9 (5)]

8.8 Developer Configuration Management [SA-10]

{Insert Company Name} must require that the developer of information systems, system components, or system services to: [SA-10]

* Perform configuration management during system, component, or service design, development, implementation, and operation [SA-10 (a)]
* Document, manage, and control the integrity of changes to the system components throughout the configuration management process [SA-10 (b)]
* Implement only organization-approved changes to the system, component, or service [SA-9 (10) (c)]
* Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes [SA-10 (d)]
* Track security flaws and flaw resolution within the system, component, or service and report findings to the {Insert Company Name} Technology Team and agency defined personnel [SA-10 (e)]

8.9 Developer Testing and Evaluation [SA-11, SA-11 (1,2)]

{Insert Company Name} requires the developer of systems, system components, or system services, at all post-design stages of the system development life cycle to partner with security personnel to complete the following activities: [SA-9 (11)]

* Create and implement a plan for ongoing security and privacy control assessments [SA-11 (a)]
* Perform unit, integration, system, and/or regression testing or evaluation throughout the life cycle using static analysis, dynamic analysis, and/or binary analysis [SA-11 (b)]
* Produce evidence of the execution of the security assessment plan and the results of the security testing and evaluation [SA-11 (c)]
* Implement a verifiable flaw remediation process [SA-11 (d)]
* Correct flaws identified during security testing and evaluation [SA-11 (e)]

On systems storing or processing Federal or State government data, {Insert Company Name} must require the developer of the system, system component, or system service to:

* Employ static code analysis tools to identify common flaws and document the results of the analysis. The service provider must document its methodology for reviewing newly developed code for the Service in its Continuous Monitoring Plan. If static code analysis cannot be performed (for example, when the source code is not available), then dynamic code analysis must be performed. [SA-11 (1)]
* Perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that: [SA-11 (2)]
  + Uses the following contextual information: [SA-11 (2) (a)]
    - Information concerning impact
    - Environment of operations
    - Known or assumed threats
    - Acceptable risk levels
  + Employs one or more of the following tools and methods: [SA-11 (2) (b)]
    - Dynamic code analysis scanner
    - Static code analysis scanner
    - Binary code analysis scanner
    - Unit testing
    - Integration testing
    - System testing
    - Regression testing
    - Functional testing
  + Conducts the modeling and analyses at a level of rigor that is appropriate for the data hosted in the system, system component, or system service [SA-11 (2) (c)]
  + Produces evidence that meets the defined acceptance criteria [SA-11 (2) (d)]

8.10 Development Process, Standards, and Tools [SA-15, SA-15 (3)]

{Insert Company Name} requires the developer of the system, system component, or system service to follow a documented development process that:

* 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 tools options and tool configurations used in the development process [SA-15 (a) (3)]
* Documents, manages, and ensures the integrity of changes to the process and/or tools used in development [SA-15 (a) (4)]

If Federal or state government information is processed or stored within the external system, {Insert Company Name} must review the development process, standards, tools, tool options, and tool configurations throughout the System Development Life Cycle (SDLC) to determine if the process, standards, tools, tool options, and tool configurations before first use and annually thereafter. {Insert Company Name} must ensure the prescribed NIST controls are met. [SA-15 (b)]

{Insert Company Name} requires the developer of the system, system component, or system service to perform a criticality analysis prior to acquisition or any upgrade point and at a level of rigor sufficient to maintain the integrity throughout the system development life cycle. [SA-15 (3)]

8.11 Developer-Provided Training [{SA-16}]

**For high impact systems only:**

{Insert Company Name} requires the developer of the system, system component, or system service to provide training on the Open Web Application Security Project (OWASP) Top 10. The training covers correct use and operations of implemented security and privacy functions, controls, and/or mechanisms. [SA-16]

8.12 Developer Security Architecture and Design [{SA-17 High Only}]

**For high impact systems only:**

{Insert Company Name} requires the developer of the system, system component, or system service to produce a specific security and privacy architecture design that: [SA-17]

* Is consistent with the security and privacy architecture that is integral throughout {Insert Company Name} enterprise architecture [SA-17 (a)]
* Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components [SA-17 (b)]
* Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection towards least privilege and testing, prior to integration within {Insert Company Name} [SA-17 (c)]

8.13 Developer Screening [{SA-21 High Only}]

**For high impact systems only:**

{Insert Company Name} must verify the screening of external developers prior to conducting any work. Internal screening is addressed by the {Insert Company Name} Personnel Security Policy. Because the systems, system components, or system services may be used in critical activities essential to the national or economic security interests of government agencies.

{Insert Company Name} must assure developers have appropriate access authorizations as determined by assigned role. [SA-21 (a)] Screening criteria must include clearance verification, background checks, and/or citizenship verification. [SA-21 (b)]

8.14 Unsupported System Components [SA-22]

{Insert Company Name} shall replace system components when support for the components is no longer available from the developer, vendor, or manufacturer. [SA-22 (a)] As an alternative, {Insert Company Name} may make alternative arrangements for continued support of sunset components, such as in-house support or open-source software value-added vendors. [SA-22 (b)]