



Information Security Foundations Policy

TABLE OF CONTENTS

- 1. INTRODUCTION 3
 - 1.1 Purpose 3
 - 1.2 Background 3
 - 1.3 Scope..... 3
 - 1.4 Roles and Responsibilities 4
- 2. POLICY 5
 - 2.1 Access Control (AC)..... 5
 - 2.2 Awareness and Training (AT)..... 5
 - 2.3 Audit and Accountability (AU) 6
 - 2.4 Assessment, Authorization, and Monitoring (CA) 6
 - 2.5 Configuration Management (CM) 7
 - 2.6 Contingency Planning (CP)..... 7
 - 2.7 Identification and Authentication (IA)..... 7
 - 2.8 Incident Response (IR) 8
 - 2.9 Maintenance (MA)..... 8
 - 2.10 Media Protection (MP) 9
 - 2.11 Physical and Environmental Protection (PE) 9
 - 2.12 Planning (PL) 9
 - 2.13 Program Management (PM)..... 10
 - 2.14 Personnel Security (PS)..... 10
 - 2.15 Personally Identifiable Information Processing and Transparency (PT) 11
 - 2.16 Risk Assessment (RA)..... 11
 - 2.17 System and Services Acquisition (SA)..... 12
 - 2.18 System and Communication Protection (SC) 12
 - 2.19 System and Information Integrity (SI) 13
 - 2.20 Supply Chain Risk Management (SR)..... 13
- 3. DEFINITIONS 14
- 4. ENFORCEMENT 17

5. AUTHORITIES	17
6. APPROVAL.....	18
7. COMPLIANCE AND CONTROL MAPPING	18
8. RELATED DOCUMENTS	19
9. DOCUMENT REVISION CONTROL	19

1. INTRODUCTION

1.1 Purpose

To establish high-level requirements, organizational responsibilities, and managerial commitment for a foundational Information Security Policy that ensures the confidentiality, integrity, and availability of information systems within the purview of the Agency of Digital Services (ADS), and in compliance with all applicable State and Federal Laws, regulations, or policies.

This policy aligns with the National Institute of Standards and Technology (NIST) Special Publication 800-53 and sets the minimum security requirements that will be followed to establish a consistent baseline. If an information system contains data compliance requirements based on classification of data types, those data compliance requirements may supersede those outlined in this policy. Data compliance requirements may include Federal Tax Information (FTI), Criminal Justice Information Services, (CJIS), Health Insurance Portability and Accountability Act (HIPAA), Social Security Administration (SSA), and Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E). Information systems without a data compliance requirement based on classification of data types will adhere to this policy.

1.2 Background

This document provides the foundation for the State of Vermont (SoV) ADS Information Security Policy to ensure a consistent manner in which minimum security and compliance requirements are met, and mitigates the risk of compromise to the confidentiality, integrity, or availability of State information systems.

Failure to identify risks and implement proper controls can result in data loss, reputational exposure, loss of public trust, compromise to information systems or networks, financial penalties, and legal liability. This policy facilitates a more consistent, comparable, and repeatable approach to securing information systems, projects, and applications to meet State business needs.

1.3 Scope

Policies herein apply to all SoV Executive Branch Agencies and Departments, State employees, contractor personnel acting on behalf of the State, and any other third-party individual or organization with access to SoV data or information systems.

All the aforementioned stakeholders play a critical role in ensuring the required safeguards of this policy are met. Security of State data and information systems cannot be accomplished without this shared responsibility.

1.4 Roles and Responsibilities

ADS Secretary/Chief Information Officer (CIO)

- Approves this policy.
- Ensures communication of policy alignment to State executive leadership.
- Reports compliance-related activities to the Governor.

ADS Chief Information Security Officer (CISO)

- Reviews and approves this policy prior to ADS Secretary.
- Reports all compliance-related activities pertaining to this policy to the ADS Secretary and any affected Agency Secretary.
- Facilitates communication and collaboration between ADS divisions.

ADS Security

- Defines standards and guidelines for the implementation and maintenance of information systems.
- Identifies threats against and vulnerabilities to information systems.
- Evaluates and recommends security controls to mitigate risk.
- Works with development and IT teams to implement security measures.
- Participates in incident response planning and execution.
- Reviews this policy at a minimum annually and updates if necessary.

ADS Agency Staff

- Implement technological solutions to ensure that information systems, networks, and infrastructure are operating in accordance with SoV Information Policies and Standards.
- Ensure information systems and devices are securely configured and hardened to minimize the risk of unauthorized access and exploitation.
- Promote a culture of security awareness among peers and stakeholders, emphasizing their role in protecting the organization's assets and data.

State Agency/Department Business Owner

- Defines business requirements and objectives for information systems and applications.
- Promotes a culture of security awareness and compliance in their business units.
- Collaborates with ADS divisions to address security risks and incidents affecting their business units.
- Collaborate with ADS Agency Director(s) of Digital Services before engaging in procurement activities to ensure security requirements are met.
- Ensures that information security policies are adhered to by employees and information systems within their purview.
- In the event that information security policies cannot be met, submit a security exception request to ADS Security.

State Employee

- Participate in and remain up to date with all required information security training.
- Adhere to SoV Information Security Policies and Standards.
- Remain vigilant and proactive in identifying and reporting potential security risks and vulnerabilities that may be encountered in day-to-day activities.

- Report security incidents, breaches, or suspicious activities to help ensure prompt detection and response to security threats.

2. POLICY

2.1 Access Control (AC)

Summary: Access control can be considered the cornerstone of any security program. The various features of physical, technical, and administrative access control mechanisms work together to construct the security architecture necessary to protect critical and sensitive information assets.

Purpose: The administration of user access to electronic information systems is required to apply the principles of least privilege in accordance with their assigned roles and responsibilities. Accounts will be administered to ensure that the appropriate level of access control is applied to protect the information assets within each application or information system. Equally important is the removal of access for departing employees and contractors to ensure access to information systems and data is terminated in a timely manner.

Policy Objectives: SoV Agencies and Departments will limit information system access to authorized users; processes acting on behalf of authorized users or devices (including other information systems); and the types of transactions and functions that authorized users are permitted to exercise consistent with NIST 800-53 Rev5 control #'s AC-1-25 and any associated SoV information security standards that apply. Additionally, only users authorized by the CISO will be granted administrative access to workstations in order to download, install, and execute new applications.

2.2 Awareness and Training (AT)

Summary: A strong information security program cannot be put in place without significant attention given to training employees, contractors, and information system users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure information resources. In addition, those in ADS who manage infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to pay attention to security awareness training puts an enterprise at great risk because the security of information systems and assets is just as much of a human issue as it is a technology issue.

Purpose: The purpose of security awareness training is to develop a security-conscious workforce capable of identifying and mitigating potential cybersecurity threats, thereby reducing the likelihood of security incidents.

Policy Objectives: All new SoV employees will complete information system security awareness training upon hire. Current State employees will undergo information system security awareness training at a minimum annually to maintain access to information assets. Records of training completion will be retained for all

employees and contractors consistent with NIST 800-53 Rev5 control #'s AT-1-6, NIST 800-50, and any associated SoV information security standards that apply.

2.3 Audit and Accountability (AU)

Summary: The ability to audit events and activities on a network provides information necessary to determine if an information system or asset has been compromised. Audit and accountability capabilities also help mitigate issues as they are developing.

Purpose: A chronological record of activities involving information system events and user activity, which enables the reconstruction, review, and examination of the sequence of activities concerning each event, is required.

Policy Objectives: SoV Agencies and Departments will create, protect, and retain information system audit records to the extent needed for monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and ensure that the actions of individual information system users can be uniquely traced to those individuals so they can be held accountable for their actions, consistent with NIST 800-53 Rev5 control #'s AU-1-16 and any associated SoV information security standards that apply. The most restrictive between the audit log retention schedules defined by the Vermont State Archives & Records Administration (VASARA) and data retention requirements as outlined by federal data compliance standards will apply.

2.4 Assessment, Authorization, and Monitoring (CA)

Summary: In today's environment where many, if not all, SoV mission-critical functions are dependent upon information technology, the ability to manage this technology and to assure confidentiality, integrity, and availability of information is essential. Ongoing monitoring is a critical part of the Security Assessment and Authorization process. Timely, relevant, and accurate information is vital, particularly when resources are limited, and Agencies and Departments must prioritize their efforts.

Purpose: The purpose of information security continuous monitoring is to maintain ongoing awareness of security control effectiveness, vulnerabilities in information systems, threats to information systems and assets, support risk mitigation efforts, and inform enterprise risk management decisions.

Policy Objectives: SoV Agencies and Departments will: periodically assess the security controls in information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in information systems; authorize the operation of information systems and any associated information system connections; and monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls, consistent with NIST 800-53 Rev5 control #'s CA-1-9 and any associated SoV information security standards that apply.

ADS Security will continuously monitor information security vulnerabilities and threats, and report identified changes to the Agency Director of Digital Services and senior management in ADS, consistent with National Institute of Standards and Technology, Special Publication 800-137.

2.5 Configuration Management (CM)

Summary: An information system is comprised of many components that can be interconnected in a multitude of arrangements to meet a variety of business, mission, and information security needs. How these information system components are networked, configured, and managed is critical in providing adequate information security and supporting the State's risk management process.

Purpose: Implementing new information systems and changing existing systems results in some adjustment to system configurations. To ensure that the required adjustments to system configurations do not adversely affect the security of the information system or the users from operation of the information system, a well-defined configuration management process that integrates information security is needed.

Policy Objectives: ADS will establish and maintain baseline configurations and inventories of State information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles and establish and enforce security configuration settings for information technology (IT) products employed in enterprise, agency, and department information systems, consistent with NIST 800-53 Rev5 control #'s CM-1-14, NIST 800-128, and any associated SoV information security standards that apply.

2.6 Contingency Planning (CP)

Summary: Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.

Purpose: Because information system resources are so essential to the SoV's success, it is critical that services provided by these systems can operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable an information system to be recovered as quickly and effectively as possible following a service disruption.

Policy Objectives: SoV Agencies and Departments will establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for State information systems to ensure the availability of critical information resources and continuity of operations in emergency situations, consistent with NIST 800-53 Rev5 control #'s CP-1-13, NIST 800-34 Rev 1, and any associated SoV information security standards that apply.

2.7 Identification and Authentication (IA)

Summary: A foundational aspect of information security is knowing who has been granted access to information systems and assets. The identification and authentication of users and processes allows the SoV to restrict access to only authorized users and processes.

Purpose: The protection of information systems and assets from unauthorized modification, disclosure, or destruction to ensure that it is accurate, remains confidential, and is available when needed is a requirement of federal and state regulatory statute.

Policy Objectives: SoV Agencies and Departments will identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to information systems, consistent with NIST 800-53 Rev5 control #'s IA-1-12 and any associated SoV information security standards that apply.

2.8 Incident Response (IR)

Summary: Any technology security incident is a violation or imminent threat of violation to information security policies, acceptable use policies, or standard security practices.

Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware, running the tool has infected their computer and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the State does not pay a designated sum of money.
- A user distributes illegal copies of software to others through peer-to-peer file sharing services.
- An unencrypted laptop computer or information storage device is lost or stolen.
- An attacker attempts to compromise authentication of an information asset using brute force.

Purpose: Rapid and effective incident response is required because attacks can compromise the confidentiality, integrity, or availability of information systems. It is critically important to respond quickly and efficiently when these incidents occur. An incident response capability will support incidents systematically so that appropriate and consistent actions are taken.

Policy Objectives: ADS will establish an operational incident handling capability for enterprise information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and track, document, and report incidents to appropriate State Officials and/or authorities, consistent with NIST 800-53 Rev5 control #'s IR-1-10, NIST 800-61 Rev2, and any associated SoV information security standards that apply.

2.9 Maintenance (MA)

Summary: Information systems and equipment require service and/or frequent updates in order to operate at their highest capability and remain secure.

Purpose: Periodic and timely maintenance of information systems, including effective patch management processes, is a requirement of a comprehensive security program.

Policy Objectives: SoV Agencies and Departments with system maintenance responsibilities will perform periodic and timely maintenance on information systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance, consistent with NIST 800-53 Rev5 control #'s MA-1-7 and any associated SoV information security standards that apply.

2.10 Media Protection (MP)

Summary: Information systems capture, process, transmit, and store information using a wide variety of media. This information is located not only on the intended storage media but also on devices used to create, process, or transmit this information. This media may require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality. Efficient and effective management of information created, processed, transmitted, and stored by an information system throughout its lifecycle (from inception through disposal) is a primary concern of a media protection strategy.

Purpose: The SoV will provide a reasonable assurance, in proportion to the confidentiality of the data, that all digital and paper media containing sensitive information must be protected at all times from unauthorized access.

Policy Objectives: SoV Agencies and Departments will protect information system media, both paper and digital; limit access to data on information system media to authorized users; and sanitize or destroy information system media before disposal or release for reuse, consistent with NIST 800-53 Rev5 control #'s MP-1-8, NIST 800-88, and any associated SoV information security standards that apply.

2.11 Physical and Environmental Protection (PE)

Summary: In order to minimize disruption, damage, or loss of information and technology resources utilized by the State, requirements for physical and environmental protection of information assets are mandatory. For the purposes of this policy, 'facilities' is defined to include all areas that contain information assets, including general workspace, but special focus should be placed on concentrations of information assets, such as data centers, server rooms, network/data transmission hubs (i.e., telephone/data/wiring closets), concentrated cable runs, and technology or records staging/storage areas.

Purpose: The SoV will use reasonable means to protect its information systems from threats posed by attackers with malicious intent, environmental hazards, and other activities or events that pose potential risks to information systems and assets.

Policy Objectives: SoV Agencies and Departments will limit physical access to information systems, equipment, and the respective operating environments to authorized users and protect the physical infrastructure for information systems, including the protection of information systems against environmental hazards and providing appropriate environmental controls in facilities containing information systems, consistent with NIST 800-53 Rev5 control #'s PE-1-23 and any associated SoV information security standards that apply.

2.12 Planning (PL)

Summary: The objective of information system security planning is to improve the security posture of information system resources. All SoV information systems have some level of sensitivity and require protection. The protection of an information system will be documented in a System Security Plan (SSP).

Purpose: The purpose of the SSP is to provide an overview of the security requirements of the information system and describe the controls in place or planned for meeting those requirements.

Policy Objectives: ADS Security will coordinate with Agency Directors of Digital Services to develop, implement, and review annually a SSP, where required, for information systems consistent with NIST 800-53 Rev5 control #'s PL-1-11, NIST 800-18 Rev 1, and any associated SoV information security standards that apply.

2.13 Program Management (PM)

Summary: The selection and implementation of appropriate security controls for an information system is an important task that can have major implications on the operations and information assets of an Agency or Department, as well as the welfare of individuals and the general public. Security controls are the management, operational, and technical safeguards or countermeasures employed within information systems to protect the confidentiality, integrity, and availability of the system and its information.

Purpose: The purpose of Security Program Management is to appropriately address the following questions:

- What security controls are needed to adequately mitigate the risk incurred by the use of information and information systems in the execution of organizational missions and business functions?
- Have selected security controls been implemented or is there a realistic plan for their implementation?
- Are the selected security controls, as implemented, effective in their application?

Policy Objectives: ADS Security will identify and monitor on an ongoing basis the risks arising from the use of information and information systems, and report on the effectiveness of existing security controls to the Agency Director of Digital Services and senior management in ADS, consistent with NIST 800-53 Rev5 control #'s PM-1-32, NIST 800-122, and any associated SoV information security standards that apply.

2.14 Personnel Security (PS)

Summary: In response to increasing threats, a personnel security program is needed to prevent unauthorized access to information systems and assets. Specific trustworthiness and capability criteria for personnel security and information system integrity are needed. The personnel security program will consider an individual background, qualifications, and operational restrictions prior to granting an individual access to sensitive data and information systems. The overall objective is to ensure that users who are granted access are trustworthy, capable, and operationally safe. Also, the SoV--including the employees, contactors, and the environment in which they function--should operate securely so that they do not constitute an unacceptable security risk that could impact other personnel or the public.

Purpose: Effective information security requires that users granted access to information systems and data be vetted to ensure that information security objectives can be maintained.

Policy Objectives: SoV Agencies and Departments will ensure that individuals occupying positions of responsibility within the State (including third-party service providers) are trustworthy and meet established security criteria for those positions. In addition, Agencies and Departments must ensure that State information

and information systems are protected during and after personnel actions such as terminations and transfers and employ formal sanctions for personnel failing to comply with organizational security policies and procedures, consistent with NIST 800-53 Rev5 control #’s PS-1-9 and any associated SoV information security standards that apply.

2.15 Personally Identifiable Information Processing and Transparency (PT)

Summary: Breaches involving Personally Identifiable Information (PII) can be hazardous to both the SoV and individuals we serve. SoV harms may include a loss of public trust, legal liability, or remediation costs. Individual harm may include identity theft, embarrassment, or blackmail. A risk-based approach should be taken to appropriately protect the confidentiality of PII.

Purpose: Managing risk from inadequate collection, processing, and maintenance of PII helps to safeguard sensitive data. Focus will be given to consent and privacy. The risk of data breaches can be lowered by properly managing PII.

Policy Objectives: Processing of PII will be restricted to only that which is authorized. SoV Agencies and Departments will take steps to ensure that PII is only processed for authorized purposes, including training personnel on the authorized processing of PII, and monitoring and auditing use of PII, consistent with NIST 800-53 Rev5 control #’s PT-1-8 and any associated SoV information security standards that apply. Individuals will be provided with notification about and give consent for the processing of PII.

2.16 Risk Assessment (RA)

Summary: An effective risk assessment process is an important component of a successful information security program. The principal goal of a risk assessment process is to protect SoV Agencies and Departments and their ability to perform their mission, not just their information assets. Therefore, the risk assessment process should not be treated primarily as a technical function carried out by ADS, who operate and manage the information systems, but rather as an essential management function of the Agencies and Departments.

Purpose: The purpose of performing a risk assessment is to enable the Agencies or Department to accomplish their mission:

- By better securing information systems that store, process, or transmit Agency or Department information.
- By enabling Business Owners to make well-informed risk management decisions.
- To justify the expenditures related to information security.
- By assisting Business Owners in authorizing (or accrediting) information systems on the basis of the supporting documentation resulting from the performance of a risk assessment.

Policy Objectives: SoV Agencies and Departments will periodically assess the risk to State operations (including mission, functions, image, or reputation), information assets, and users, resulting from the operation of information systems and the associated processing, storage, or transmission of State information, consistent with NIST 800-53 Rev5 control #’s RA-1-10, NIST 800-30 Rev 1, NIST 800-39, and any associated SoV information security standards that apply.

2.17 System and Services Acquisition (SA)

Summary: To be most effective, information security must be integrated into the System Development Life Cycle (SDLC) from system inception to implementation and ongoing maintenance and operations (M&O). Early integration of security in the SDLC enables the maximum return on investment in a security program, through:

- Early identification and mitigation of security vulnerabilities and misconfiguration, resulting in lower cost of security control implementation and vulnerability mitigation.
- Awareness of potential engineering challenges caused by mandatory security controls.
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques.
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner.

The consideration of security in the SDLC is essential to implementing and integrating a comprehensive strategy for managing risk for all information assets in the SoV.

Purpose: Adequate security controls must be integrated into processes used for systems and services acquisition, including internal development, purchasing, and outsourcing to ensure that information assets used by the SoV are protected.

Policy Objectives: All software application and system development or the acquisition of applications and information systems, including externally provided services (such as cloud-based), by the SoV will employ a System Development Lifecycle (SDLC) methodology approved by ADS that incorporates security planning and review during each phase of development or acquisition and adheres to a secure-coding methodology. This approach requires that project and development teams, in collaboration with the Agency Director of Digital Services and ADS Security, assess risks to the development and implementation or acquisition of information systems and assets while incorporating controls into the process to mitigate such risks. A SDLC methodology will be developed and maintained by ADS, consistent with NIST 800-53 Rev5 control #'s SA-1-23 and any associated SoV information security standards that apply.

2.18 System and Communication Protection (SC)

Summary: The protection of information assets at rest and in transit is fundamental to the SoV's security program.

Purpose: The SoV uses reasonable means, commensurate with risk, to protect the confidentiality, availability, and integrity of information assets in storage and during transmission.

Policy Objectives: ADS will monitor, control, and protect communications (i.e., information transmitted or received by information systems) at the external boundaries of the enterprise network and at designated internal boundaries of information systems; and employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within Agency,

Department, and enterprise information systems, consistent with NIST 800-53 Rev5 control #'s SC-1-51 and any associated SoV information security standards that apply.

2.19 System and Information Integrity (SI)

Summary: The two key components of information system integrity are software authenticity and the assurance of user identity. The following best practices will be routinely evaluated in current SoV environments to achieve these objectives:

Logging for all centralized authentication services will be enabled and include the IP address of the system accessing the service, the username, the resource accessed, and whether the attempt was successful or not.

The number of authentication attempts will be limited, and the user will be locked out if the limit is reached. A manual review will be conducted before unlocking the account and automatic unlocks after a specified time period will be prohibited.

Near real-time log review for failed attempts per user and per unit of time independent of successful logins; abnormal successful logins; and lockouts will be conducted. This data will be correlated to identify anomalous activity.

- Limit remote access.
- Restrict access by IP address wherever possible.
- Limit concurrent logins to one per user.
- Maximize complexity of passwords, passphrases, and personal identification numbers (PINs) whenever possible.
- Enable defenses against key logging such as forced frequent credential changing and updated anti-virus (AV) signatures.
- Validate software.

Purpose: The SoV uses reasonable means to protect its information systems from threats posed by viruses, spam, hackers, malware, and other malicious activities by installing, maintaining, and monitoring appropriate technical controls to protect its information systems.

Policy Objectives: SoV Agencies and Departments will identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within State information systems; and monitor information system security alerts and advisories and take appropriate actions in response, consistent with NIST 800-53 Rev5 control #'s SI-1-23 and any associated SoV information security standards that apply.

2.20 Supply Chain Risk Management (SR)

Summary: Information Technology (IT) relies on a complex, globally distributed, and interconnected supply chain ecosystem that is long, has geographically diverse routes, and consists of multiple tiers of outsourcing. This ecosystem is composed of public and private sector entities (e.g., acquirers, system integrators, suppliers, and external service providers) and technology, law, policy, procedures, and practices that interact to design,

manufacture, distribute, deploy, and use IT products and services. This ecosystem has evolved to provide a set of highly refined, cost-effective, reusable IT solutions.

IT supply chain risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices. These risks can lead to decreased visibility into, and understanding of, how the technology that is acquired is developed, integrated, and deployed.

Purpose: Identifying, assessing, selecting, and implementing risk management processes and mitigating controls is essential in managing the risks associated with supply chain and third-party service provider related threats.

Policy Objectives: ADS will employ processes and procedures to protect against supply chain and vendor risk to information systems and assets and to limit the harm or consequences from supply chain related threats consistent with NIST 800-53 Rev5 control #'s SR-1-12, NIST 800-161, and any associated SoV information security standards that apply.

3. DEFINITIONS

Access Control: Access privileges granted to a user, program, or process or the act of granting those privileges.

Application: A software program hosted by an information system.

Attacker: A party, including an insider, who acts with malicious intent to compromise a system.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Availability: Ensuring timely and reliable access to and use of information.

Baseline Configuration: A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.

Business (Information) Owner: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management: A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Configuration Settings: The set of parameters that can be changed in hardware, software, or firmware that affects the security posture and/or functionality of the system.

Continuous Monitoring: Maintaining ongoing awareness to support organizational risk decisions.

Contractor: An individual performing work on behalf of the SoV pursuant to a contract.

Data: Any piece of information suitable for use in a computer.

Device(s): Endpoints connected to a network, includes Servers, Workstations, IoT, smart phones, tablets, network devices, etc.

Equipment: Computer hardware, software, servers, peripheral devices, telephones and other telecommunications products, office products such as photocopiers and fax machines, or other technology or devices that is used in the creation, conversion, or duplication of data or information.

Facilities: All areas that contain information assets, including general workspace, data centers, server rooms, network/data transmission hubs (i.e., telephone/data/wiring closets), concentrated cable runs, and technology or records staging/storage areas.

Incident: An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Asset: A distinct piece of information technology, including hardware, software, and firmware, such as workstations, servers, network components, applications, and mainframes, the sum of which comprises an information system.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology: Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use, or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help–desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.

Integrity: Guarding against improper information modification or destruction and includes ensuring information non–repudiation and authenticity.

Least Privilege: The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Maintenance: Any act that either prevents the failure or malfunction of equipment or restores its operating capability.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Media: Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips, and printouts (but excluding display media) onto which information is recorded, stored, or printed within a system.

NIST SP 800-53: A publication from the National Institute of Standards and Technology which provides a comprehensive set of security and privacy controls to protect information systems. It outlines various controls across different families and is widely used by government agencies and other organizations to manage security and privacy risks effectively.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Patch Management: The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Risk Management: The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Sensitive Information: Data that requires protection because its loss, misuse, modification, or unauthorized access will negatively impact the welfare, privacy, assets, or security of an organization or individual. Examples include security numbers, personal financial information, debit/credit card numbers, personally identifiable information (PII), protected health information (PHI), and any other data that is identified by law, regulation, policy, or practice as confidential.

Spam: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

State Data: Any data that the State processes, stores, maintains, supports, or transmits.

State Employee: Any individual employed by the SoV on a permanent or limited status basis. For the purposes of this policy, it also includes contractors with State partner accounts.

System Development Life Cycle (SDLC): The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

System Security Plan (SSP): A formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The System Security Plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems.

Third-Party Service Provider: Suppliers, integrators, vendors, telecommunications, and infrastructure support that are external to an organization that operates or maintains an information system.

Threat(s): Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

User: Individual, or (system) process acting on behalf of an individual, authorized to access a system.

Virus: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

4. ENFORCEMENT

ADS has the authority to initiate reviews, assessments, or other means to ensure that policies, standards, or procedures are being followed.

Failure to comply may result in temporarily discontinuing or suspending user access to, or the operation of, the information system until such compliance is established.

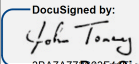

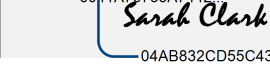
If any portion of the minimum requirements outlined in this policy cannot be met, the Business Owner, in coordination with the Agency Director of Digital Services will file for a security exception. The documented security exception will define compensating controls, length of exception, and plan of action for resolving the exception that can allow the information system to remain in operation for a defined amount of time until the required safeguard(s) can be implemented.

5. AUTHORITIES

- National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5
- Centers for Medicare and Medicaid Services (CMS), Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.2, September 16, 2021

- IRS Publication 1075 (Rev. 11-2021)
- Social Security Administration (SSA), *Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with The Social Security Administration, Version 11.0, 06/10/2024*
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45 CFR Part 160 and Subparts A and C of Part 164
- Criminal Justice Information Services (CJIS), Security Policy, Version 5.9.5, 07/09/2024

6. APPROVAL

NAME/TITLE	DATE	SIGNATURE
John Toney, Chief Information Security Officer – Agency of Digital Services (ADS)	11/15/2024	
Denise Reilly-Hughes, Secretary/CIO - Agency of Digital Services (ADS)	11/18/2024	
Sarah Clark, Secretary - Agency of Administration (AOA)	12/5/2024	

7. COMPLIANCE AND CONTROL MAPPING

NIST 800-53	MARS-E	IRS PUB 1075	SSA	HIPAA	CJIS
AC-1	AC-1	AC-1	AC-1	164.308(a)(1)(ii)(D)	AC-1
AT-1	AT-1	AT-1	AT-1	164.308(a)(5)(ii)(C)	AT-1
AU-1	AU-1	AU-1	AU-1	164.310(a)(2)(iv)	AU-1
CA-1	CA-1	CA-1	IR-1	164.310(d)(2)(iii)	CM-1
CM-1	CM-1	CM-1	PL-1	164.312(b)	CP-1
CP-1	CP-1	CP-1	RA-1	164.308(a)(3)(ii)(B)	IA-1
IA-1	IA-1	IA-1		164.308(a)(3)(ii)(C)	IR-1
IR-1	IR-1	IR-1		164.308(a)(4)(i)	MA-1
MA-1	MA-1	MA-1		164.308(a)(4)(ii)(B)	MP-1
MP-1	MP-1	MP-1		164.308(a)(4)(ii)(C)	PE-1
PE-1	PE-1	PE-1		164.312(a)(2)(i)	PL-1
PL-1	PL-1	PL-1		164.312(a)(2)(ii)	RA-1
PM-1	PM-1	PM-1		164.312(a)(2)(iii)	SC-1
PS-1	PS-1	PS-1		64.312(d)	SI-1
PT-1	RA-1	PT-1		164.308(a)(1)(i)	
RA-1	SA-1	RA-1		164.308(a)(2)	
SA-1	SC-1	SA-1		164.308(a)(3)	
SC-1	SI-1			164.308(a)(4)	
SI-1				164.314	
SR-1				164.316	
				164.308(a)(1)(ii)(C)	

				164.308(a)(3)	
--	--	--	--	---------------	--

8. RELATED DOCUMENTS

DOCUMENT

Various Supporting Documents

9. DOCUMENT REVISION CONTROL

VERSION NO.	DATE	AUTHOR	COLLABORATORS	DESCRIPTION OF CHANGES
1.0	11/15/2024	ADS Security Office	ADS, AOA, DHR	Released and published to SoV users