		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Information Security Framework	Next Review:	Per policy
Number:	ISP-001		
Version:	1.1	Approved by:	CIO
Pages	9	Distribution:	SOA

1. Purpose

The State of Alaska (SOA) is responsible for the information assets (e.g., information and information systems and telecommunication systems) it creates, manages, processes, stores, or transmits in order to carry out its functions. The SOA must safeguard these assets from any threats to their confidentiality, integrity, and availability. This document establishes the framework of the Information Security Management System (ISMS) of the SOA, including the ISMS scope and policy. Each branch and agency of the SOA is responsible for the day-to-day management of information security practices and arrangements in accordance with this framework.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

SOA Internal

5. Framework Scope

5.1. Organization

This information security policy framework applies to all personnel including full-time, part-time and temporary employees, contractors, consultants, vendors, auditors, and other personnel engaged to perform work for or on behalf of the SOA, and collectively are referred to herein as "personnel" The information security policy framework further applies to the executive branch, legislative branch, judicial branch, corporations and commissions of the SOA and to the departments of those branches as illustrated in Figure 1 – Overview of State of Alaska Organization.

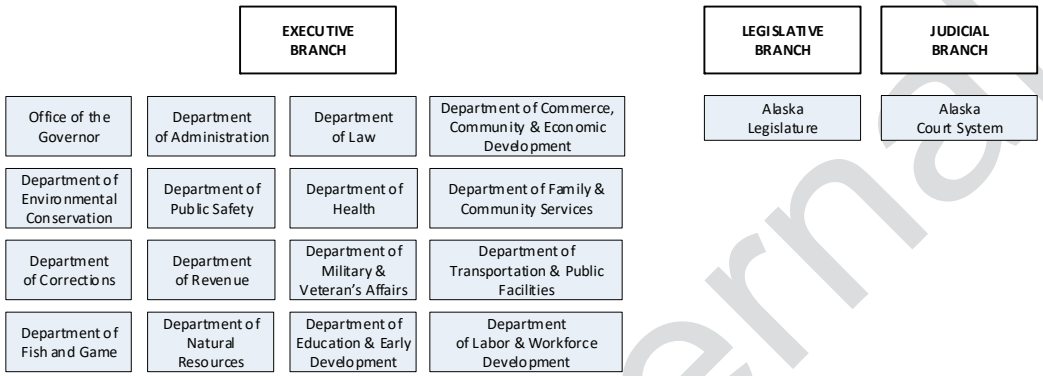

Figure 1 – Overview of State of Alaska Organization

5.2. Locations

This information security policy framework applies to all of the locations owned, leased, or otherwise occupied by the SOA and all logical access to SOA internal networks.

5.3. Assets and Technology

This information security policy framework applies to all the information the SOA creates, manages, processes, stores, or transmits and to all the information systems, which include computer systems, applications, networks, peripherals, or electronic media used to develop manage, and operate all SOA informational processes.

5.4. Limitations and Exclusions

This information security policy framework applies to information assets, in any form, throughout the information system and information technology lifecycle and to any stage of an activity, function, project, or product involving information assets. SOA branches, departments, divisions, agencies, corporations and commissions must adapt this framework to the needs of their organizations and fundamentals in accordance with the policy established herein and any applicable legal and regulatory requirements.

6. Policy

6.1. Information Security Strategy

SOA Internal

6.1.1 Essential and Sanctioned Function

The confidentiality, integrity, and availability of information and related internal controls are essential functions of the SOA, collectively referred to as "information security."

6.1.2 Requirement for Information Security Controls

Information security functions and administrative, technical, and physical controls are considered essential and are sanctioned by the SOA as a proactive service in keeping with industry best practice.

6.2. Establishment and Responsibility

6.2.1 Establishment of Information Security Management System (ISMS)

This framework establishes and serves as the charter for the SOA ISMS. The SOA ISMS supports the planning, implementation, monitoring, and improvement of security controls in concert with the information handling, processes, services and technology infrastructure supported and provided by the SOA.

6.2.2 Program Authority

The SOA has designated the State Security Office (SSO) as the single point of authority responsible for establishing the ISMS including information security strategy, policies, and controls.

To demonstrate Executive Management's commitment to the ISMS, Executive Management must:

- Establish the commitment of Departments to the information security policy process;
- Determine their organization's approach to managing information security;
- Ensure that appropriate plans and budgets are in place to support the information security objectives of the SOA;
- Establish, approve, publish, and communicate the SOA information security policies;
- Assign responsibility and accountability for information security, including responsibility for protection of individual assets (i.e., Information Owners) and carrying out specific security processes appropriately within the department;
- Establish the requirement for a formal, on-going information security training and awareness program within the department;
- Assign responsibility for internal audits of the ISMS and ensuring that such audits are performed and reported appropriately to Executive Management and the SSO;
- Ensure that necessary corrective and preventative actions are taken to identify, mitigate, and eliminate potential threats to department information assets; and
- Identify any potential exception to information security policy, communicating the exception to the SSO, and coordinating the appropriate activities and controls to reduce risk related to any such exceptions.

6.2.3 Information Owners and Custodians

Personnel defined as Information Owners must define the protective requirements for the information assets for which they are responsible, in accordance with SOA policies and applicable legal and regulatory requirements, and must ensure that assigned Information Custodians implement and maintain appropriate safeguards to protect those information assets.

SOA Internal

6.2.4 Individual Accountability

All personnel are responsible for protecting SOA information assets from all unauthorized access, modification, duplication, destruction, or disclosure. Personnel will be accountable for their actions and will apply due diligence to information asset security. Violations of unauthorized access, modification, duplication or disclosure may result in disciplinary action up to and including dismissal and/or criminal or civil prosecution in accordance with SOA or Federal statutes.

6.3. Security Principles

6.3.1 Awareness

Executive Management must ensure that all personnel have access to information security policies, standards, procedures, and practices. Executive Management must also ensure that ongoing training is conducted, under the guidance of the SSO, to ensure personnel awareness of responsibilities in safeguarding information assets.

6.3.2 Ethics

Executive Management must ensure that access to SOA information assets is granted for approved SOA purposes only. Personnel must use and administer information in an ethical manner. The SOA reserves the right to employ appropriate technologies and procedures to ensure that its information assets are used in an acceptable and ethical manner, in order to ensure the security of SOA information assets.

6.3.3 Safeguard by Default

Persons must safeguard information assets in accordance with SOA data classification schemes. When the classification of an information asset is unknown personnel must safeguard the asset as "**confidential**" until the classification has been determined.

6.3.4 Need to Know

Personnel who have access to data are prohibited from perusing data unrelated to assigned tasks or projects.

6.3.5 Applicable Law

Personnel must comply with all applicable laws and regulations with respect to the collection, storage, safeguarding, appropriate use, and disposal of information assets in accordance with SOA or Federal Statutes.

6.4. Asset Management

6.4.1 Asset Inventory and Classification

Executive Management must identify information assets and document the confidentiality, integrity, and availability requirements to determine a classification level for each asset.

6.4.2 Control According to Classification

Executive Management must ensure that controls are applied to safeguard information assets consistent with the classification level of the asset.

SOA Internal

6.5. Incident Management

6.5.1 Incident Reporting

Personnel must report known or suspected information asset security compromises or violation incidents, in a timely manner, according to incident reporting policies and procedures defined by the SOA.

6.5.2 Incident Response

The SSO must establish policies and procedures to identify, evaluate, contain, and address suspected information asset security compromises or violation incidents. The SSO must establish an organizational structure and a process to review the results of information asset security compromises or violation incident responses and implement corrective actions.

6.6. Risk Management

6.6.1 Risk Assessment

Executive Management must establish and implement a risk assessment process to identify and evaluate potential risks to SOA information assets.

6.6.2 Risk Treatment

Executive Management must regularly review the results of risk assessments and must establish and implement risk treatment plans to prioritize, evaluate, and address risks to SOA information assets identified as a result of those assessments.

6.7. Compliance

6.7.1 Compliance

Compliance with information security policies is critical to the secure functionality of the SOA business. The SOA is obligated to function with ethical and confidential management of all information assets.

6.7.2 Implications of Non-compliance

Non-compliance with information security policies may lead to disciplinary actions up to and including termination of employment. Under certain circumstances, violations of information security policies may give rise to civil and/or criminal liability. The SOA may also pursue legal action as deemed appropriate against third parties for unauthorized access, use or destruction of information assets.

6.7.3 Information Systems Compliance

Personnel must report any information asset that is found to be non-compliant with SOA information security policies to the SSO for exception handling in accordance with information security policies.

SOA Internal

7. Policy Framework

7.1. Framework Diagram

Executive Management must implement support of the ISMS policy established in section 6 above, and further information security policies, standards, procedures, and practices to ensure that safeguards are applied to all SOA information assets, consistent with the framework illustrated in Figure 2 – State of Alaska Framework Diagram.

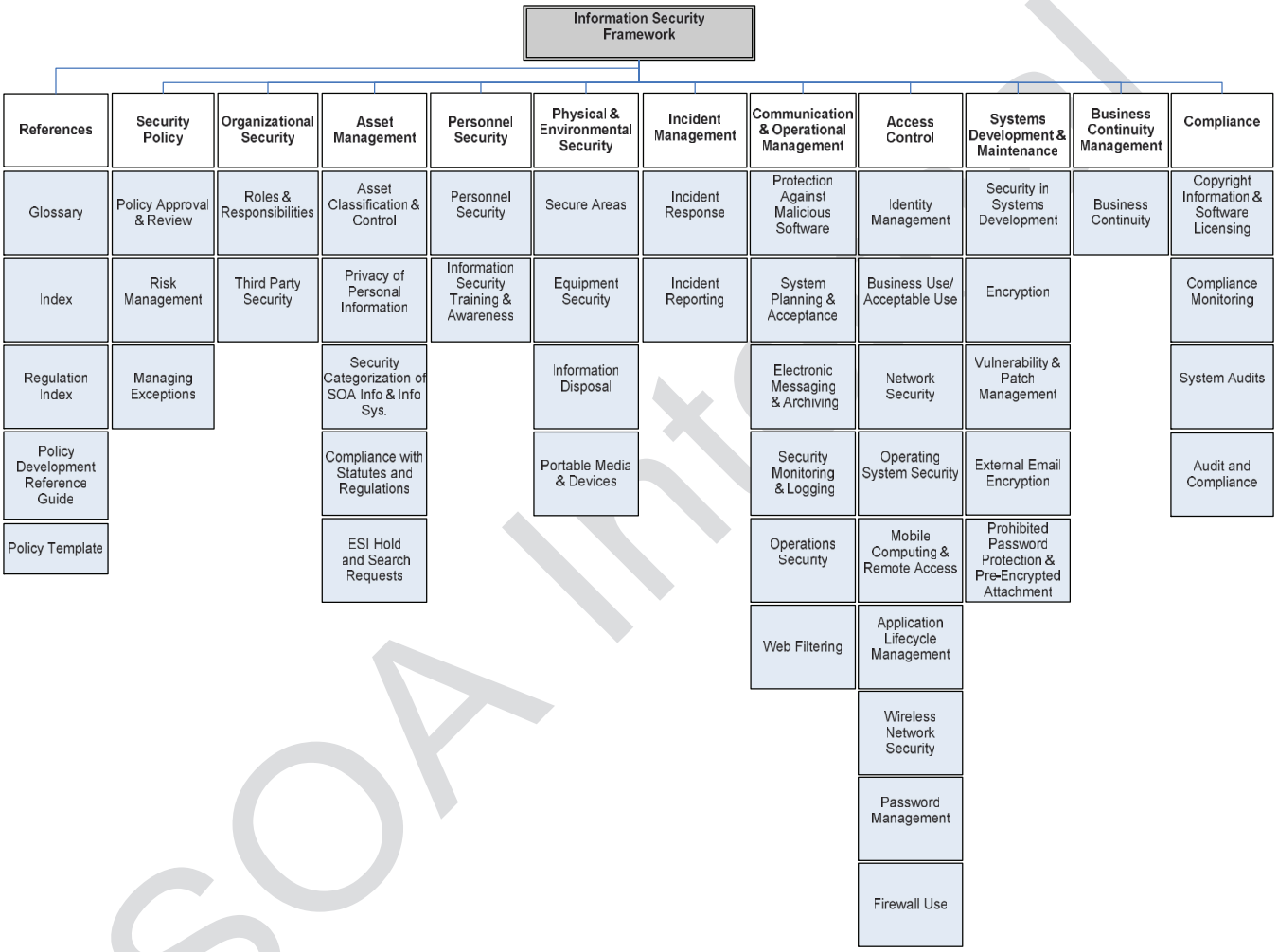

Figure 2 – State of Alaska Framework Diagram

SOA Internal

7.2. Reference Standard(s)

The primary reference standard employed in the SOA Information Security Framework is the international standard ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*, published by the International Organization for Standardization (ISO) in October 2005. Secondary reference standards include the National Institute of Standards and Technology (NIST) Special Publication 800 series and the international standard ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*, published by the ISO in June 2005.

8. Security Governance Organization Structure

The SOA CIO has established the following security organization responsible for ensuring that SOA ISMS is implemented in accordance with this framework.

8.1. State of Alaska Chief Information Officer (CIO)

Alaska Statute 44.21 designates DOA as the department responsible for the operation and management of telecommunication and information technology data processing resources and activities of the executive branch of State government and the judicial and legislative branches to the extent requested by those branches. DOA is required to provide for periodic review State telecommunication and information technology data processing procedures and mechanisms.

The Commissioner of DOA holds the authority, as the CIO, for the executive branch agencies, corporations, and commissions. The CIO has maintained various governance boards and work groups to provide recommendations and assist in the fulfillment of statutory requirements. These groups include the Enterprise Investment Board (EIB), the Technology Management Council (TMC), the Incident Response Team (IRT), and the SSO. Responsibilities of the CIO include:

- Determining policy requirements consistent with the needs of the SOA and approving information security policies developed by the SSO;
- Ensuring adequate funding and staffing of the SSO and other roles of the SOA security organization; and
- Reviewing any exceptions to information security policies recommended by the SSO.

8.2. State of Alaska Security Office (SSO)

The SSO, led by the CSO under authority delegated by the CIO, is responsible for establishing, implementing, monitoring, auditing, improving and enforcing the SOA ISMS. Specific responsibilities must include:

- Developing, coordinating approval, enforcing and communicating information security strategic plans, policies and implementing procedures, standards and solutions in support of the plans and policies;
- Supporting the CIO, EIB, TMC, Functional Work Groups (FWGs), and other SOA organizations as necessary to further the security objectives of the SOA;
- Presenting information security issues, policy changes and exceptions, and recommendations to the CIO or EIB;
- Providing the management, leadership, coordination and support for the security activities of the executive branch department Information Security Officers (ISOs) and department Computer Security Designees (CSDs);
- Providing coordination and support for the activities of the security liaisons of the legislative and judicial branches;

SOA Internal

- Approving, coordinating and overseeing security related investments, improvements, solutions and services for the SOA, audits, incident response analysis and best practices;
- Providing technical assistance to the Division of Personnel and Labor Relations on employee related matters;
- Acting as the single point of contact for the executive branch departments, agencies, divisions, corporations or commissions for the collection and delivery of electronic data for public record requests, email holds and legal discoveries;
- Acting as a point of contact for executive branch on non-criminal related information security issues with special interest groups and entities, including U.S Federal Government, US-CERT(Computer Emergency Readiness Team), Federal Bureau of Investigations (FBI), Secret Service, Alaska State Troopers, Multi-State Information Sharing and Analysis Center (MS-ISAC), InfraGard, National Emergency Numbering Association (NENA), State or local government, private industry, or others;
- Coordinating and conducting independent risk assessment activities for the ISMS;
- Coordinating and conducting training and awareness activities for the ISMS;
- Planning and implementing controls, evaluating, recommending and implementing the selection of solutions, and participating in the development of the information technology strategies of the SOA to ensure consistency with SOA information security policies, procedures and standards and the goals and objectives of the State;
- Coordinating the activities and provide Incident Command (IC) for the incident response team and the SOA forensic investigation team;
- Monitoring information security, performing independent audits of the operation of the ISMS, and reporting on the State of information security to SOA Executive Management;
- Reviewing the results of risk assessments, monitoring activities, audits, incident response, and investigations;
- Directing corrective and preventative actions for all information security policies; and
- Assisting in the performance of risk assessments.

8.3. Enterprise Investment Board (EIB)

The EIB serves as the governance board for the SOA, which is responsible for assisting the CIO in IT governance and setting information security policy and reviewing the ISMS. It is comprised of the Governor's Chief of Staff, the director of the Office of Management and Budget, the Commissioner of DOA (CIO), a representative from the administrative services directors, and the director of ETS. The EIB meets as deemed necessary. Security related responsibilities include:

- Ensuring consistency of departments' IT;
- Managing on an enterprise model in accordance with SOA standards; and
- Approving information security policies developed by the SSO and presented by the CIO.

8.4. Technology Management Council (TMC)

The TMC is chaired by the director of ETS. The SSO makes presentations and recommendations to the TMC on security related matters on an "as needed" basis. Security related responsibilities for the TMC include:

- Recommending enterprise class technology standards to meet the ISMS;
- Providing subject matter expertise in the form of functional workgroups (FWG) to the CIO, EIB and the SSO;
- Participating in supporting the CIO, EIB, and the SSO activities for the ISMS; and

SOA Internal

- Monitoring and reporting on the implementation of technology standards and the operation of controls that ensure executive branch agencies, corporations and commissions are adhering to the standards established by ISMS information security policies.

8.5. Incident Response Team (IRT)

The SOA IRT is directed by the SSO and staffed by subject matter experts identified by the SSO. The IRT meets quarterly to plan, review issues and receive domain-specific training. IRT is convened by the SSO in support of incident response activities and planning. Specific responsibilities include:

- Providing subject matter expertise to the SSO and other members of the IRT;
- Assisting in the assessment, investigation, containment, remediation and planning of security or disaster related incidents; and
- Assisting in the development of preventative or corrective actions and continuity of operational activities related to information security.

SOA Internal

1. Purpose

To define the terms used within State of Alaska (SOA) information security policies.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms used throughout the SOA Information Security Policies are defined within this document.

5. Statement Glossary Definitions

This is a list of textual specialized terms used in the Information Security Policies, with the definitions for those terms.

5.1.1 802.11x

A family of wireless networking protocols.

5.1.2 Access Control

The principle of limiting access to information assets only to appropriate individuals. See also: *Information Assets*

5.1.3 Access Rights

The ability granted to personnel authorized for the access to information assets. See also: *Information Assets*

5.1.4 Administrative Account

A specific category of account on an information system characterized by heightened privilege. See also: *Information System*

5.1.5 Administrative Security Controls

A type of security control implemented primarily via administrative mechanisms. See also: *Security Controls*

5.1.6 Advanced Encryption Standard (AES)

An encryption standard adopted by the U.S. government.

5.1.7 Adware

A specific category of malware categorized by unwanted commercial advertising. See also: *Malware*

5.1.8 AES

Advanced Encryption Standard.

5.1.9 Alaska Public Safety Information Network (APSIN)

A collection of system servers, devices or networks which processes, stores and transports regulated law enforcement information.

5.1.10 Application Security

The process of governing the information security aspects of the applications supported by a particular information system. See also: *Information System*

5.1.11 APSIN

Alaska Public Safety Information Network.

5.1.12 Asset

A resource owned, managed, or held in trust by SOA. See also: *Information Asset*

5.1.13 Asset Classification

See Classification

5.1.14 Audit

A formal methodical examination of an organization or individual's accounts or financial situation.

5.1.15 Authentication

The process of validating a user's claimed identity using one or more authentication factors. See also: *Identity Management, Authentication Factors*

5.1.16 Authentication Factor

A piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. A specific category of authentication criteria encompassing a vehicle from one of the following three categories: what you have, what you are, what you know. See also: *Authentication*

5.1.17 Availability

Indicates a property of information assets, information systems, and other resources whereby appropriate personnel, systems, or other entities have the ability to readily access resources without impedance. See also: *Information Asset, Information System*

5.1.18 Backup

The creation of a duplicate or copy of an information asset.

5.1.19 Bastion

A fortified area or position.

5.1.20 Botnet

A specific category of malware characterized by remote control of numerous information systems for illicit (and often illegal) purposes. See also: *Malware*

5.1.21 Business Management

Day-to-day operations and maintenance of service, systems, solution or programs that are provided to the various State departments and directed by the Business Manager and Business Owners.

5.1.22 Business Manager

A person, designated by a Business Owner, who is responsible for the service role of function.

5.1.23 Business Owner

Normally a Director level position, which holds the accountability and responsibility for the delivery and day-to-day operations and maintenance of a service, system, solution or program that the State provides.

5.1.24 CED

See Department of Commerce, Community and Economic Development.

5.1.25 Chain of Custody

Refers to the chronological documentation, and/or paper trail, that show the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. May help establish that the alleged evidence is related to the alleged crime.

5.1.26 Chief Information Officer (CIO)

The executive branch authority for information technology and telecommunications solutions and services within the SOA Government. The Commissioner of the Department of Administration holds this authority, responsibility, role, and function under AS 44.21.

5.1.27 Chief Security Officer (CSO)

The executive branch authority, delegated by the CIO, responsible for establishing, implementing, monitoring, auditing, improving and enforcing the SOA ISMS.

5.1.28 CIO

Chief Information Officer.

5.1.29 CJIS

Criminal Justice Information System (CJIS).

5.1.30 Classification

The process of segregating assets into groups according to priority, risk, or information assets processed. See also: *Risk, Information Asset, Asset*

5.1.31 Compensating Control

Compensating controls give organizations an alternative to security requirements that cannot be met "due to legitimate and documented technical or business constraints." Compensating controls must sufficiently mitigate the risk associated with the original control requirements.

5.1.32 Compliance

The process that ensures adherence to governing regulation, legislation, contractual requirements, or industry best practice.

5.1.33 Compromise

A violation of the confidentiality, integrity and availability of an information system or information asset. See also: *Confidentiality, Integrity and Availability, Information System, Information Asset*

5.1.34 Confidential

The classification level ascribed to the most sensitive of information assets containing information whereby unauthorized disclosure could be prejudicial to SOA, its employees, personnel and citizens. See also: *Classification and SOA Internal*

5.1.35 Confidentiality

A property of information assets, information systems, and other resources whereby access is limited only to personnel and entities authorized to view the information or access the resource. See also: *Information Asset, Information System*

5.1.36 Continuity of Operation Plan (COOP)

The creation of the documentation and process which allows for the continuation of the essential functions of government departments or agencies during any incident or emergency that may disrupt normal operations.

5.1.37 COOP

Continuity of Operation Plan.

5.1.38 Corrective Action

A plan or process (usually consisting of one more security controls) designed to address a specific vulnerability, threat, or area of risk to an information asset. See also: *Information Asset, Security Control, Vulnerability, Threat, Risk.*

5.1.39 Courtroom Admissibility

The ability for evidence to be presented within a court of law by the support of digital forensics refers to the requirement that the chain of custody be maintained and appropriate procedures are followed to preserve evidence integrity. See also: *Forensics*

5.1.40 Cryptographic Key

A confidential data value used as input to a cryptographic operation. See also: *Encryption*

5.1.41 CSO

Chief Security Officer.

5.1.42 Data

Numerical or other information represented in a form suitable for processing by computer.

5.1.43 Data Wipe

The process to render information assets unreadable through erasure and subsequent multiple overwrites. See also: *Information Disposal*

5.1.44 DEC

See Department of Environmental Conservation.

5.1.45 Defense Information Systems Agency (DISA)

Department of Defense (DoD) combat support agency with the goal of providing real-time information technology (IT) and communications. DISA plans, engineers, acquires, and supports IT products and services for the US president, vice president, secretary of defense, and all DoD agencies. Specifically, it provides communications networks, hardware, software, databases, applications, and other IT capabilities to meet the information processing and communication transport needs of the DoD.

5.1.46 Degaussing

The process to render information assets unreadable via exposure to a sufficiently-strong magnetic field or pulse. See also: *Information Disposal*

5.1.47 Department(s)

All SOA branches, departments, divisions, corporations, commissions or other related entities.

5.1.48 Department of Administration (DOA)

State of Alaska Department of Administration.

5.1.49 Department of Commerce, Community & Economic Development (CED)

State of Alaska Department of Commerce, Community & Economic Development.

5.1.50 Department of Corrections (DOC)

State of Alaska Department of Corrections.

5.1.51 Department of Education & Early Development (EED)

State of Alaska Department of Education & Early Development.

5.1.52 Department of Environmental Conservation (DEC)

State of Alaska Department of Environmental Conservation.

5.1.53 Department of Fish and Game (DFG)

State of Alaska Department of Fish and Game.

5.1.54 Department of Health & Social Services (HSS)
State of Alaska Department of Health & Social Services.

5.1.55 Department of Labor & Workforce Development (DOL)
State of Alaska Department of Labor & Workforce Development.

5.1.56 Department of Law (LAW)
State of Alaska Department of Law.

5.1.57 Department of Military & Veteran's Affairs (DMVA)
State of Alaska Department of Military & Veteran's Affairs.

5.1.58 Department of Natural Resources (DNR)
State of Alaska Department of Natural Resources.

5.1.59 Department of Public Safety (DPS)
State of Alaska Department of Public Safety.

5.1.60 Department of Revenue (DOR)
State of Alaska Department of Revenue.

5.1.61 Department of Transportation & Public Facilities (DOT)
State of Alaska Department of Transportation & Public Facilities.

5.1.62 DFG
See Department of Fish and Game.

5.1.63 DISA
Defense Information Systems Agency.

5.1.64 DMVA
See Department of Military & Veteran's Affairs.

5.1.65 DNR
See Department of Natural Resources.

5.1.66 DNS
Domain Name System.

5.1.67 DOA
See Department of Administration.

5.1.68 DOC
See Department of Corrections.

5.1.69 DoD 5220-22.0
The Federal Department of Defense (DoD) guidelines for disposal of electronic equipment and data. ftp://ftpguest:ftpguest@transfer.state.ak.us/diskcleaner/dban

5.1.70 DOL

See Department of Labor & Workforce Development.

5.1.71 Domain Name System (DNS)

A system that translates names into the numerical (binary) identifiers associated with network equipment for the purpose of locating and addressing these devices world-wide.
See also: *Network Address*

5.1.72 DOR

See Department of Revenue.

5.1.73 DOT

See Department of Transportation & Public Facilities.

5.1.74 DPS

See Department of Public Safety.

5.1.75 EED

See Department of Education & Early Development.

5.1.76 Electronic Mail (commonly referred to as Email/E-mail)

A method of exchanging two-way high-speed electronic information communications across the Internet or other computer networks.
See also: *Electronic Messaging System*

5.1.77 Electronic Messaging System

A communication system whose purpose is to provide efficient means for two-way high-speed electronic information communications.

5.1.78 Electronically Stored Information (ESI)

Information that is stored electronically, regardless of the media or format.

5.1.79 Encryption

A technical security control used to protect the confidentiality of an information asset.
See also: *Information Asset, Confidentiality, Technical Security Control*

5.1.80 Environmental Threat

A type of threat associated with the environment in which an asset, facility, or resource is located and may be compromised or exposed to a security violation. See also: *Threat*

5.1.81 EPHI

Electronically Protected Health Information (EPHI).

5.1.82 ESI

Electronically Stored Information.

5.1.83 ESI Hold

An ESI hold preserves electronically stored information related to the criteria selected until released. ESI holds can be placed for a variety of reasons. For example, an ESI hold may be placed to assist in fulfilling a public records request, legal discovery, or an investigation.

5.1.84 Event Log

Chronological records produced by a telecommunication or information technology system concerning the access, attempted access, operational changes, or other internal operating system or application functionality to include changes and access occurring to the data that resides on, or facilitated by, the system.

5.1.85 Executive Employee

The following persons are executive employees: (1) the Executive Branch employees defined as "public officials" in AS 39.50.200(a)(9); and (2) the persons employed in the following job classifications:

- Assistant Commissioner
- Executive Director
- Assistant Director
- Labor Relations Manager
- State Accountant
- State Leasing and Facilities Manager
- Department of Public Safety Liaison
- Chief, Worker's Compensation Adjudication
- Veterans Affairs Administrator
- Administrator, Violent Crimes Compensation Board
- Administrator, Highway Safety Planning Agency
- Marine Highway Transportation Services Manager

Positions placed in the partially exempt service under AS 39.25.130(a) (1) or (2) will be added to this list.

5.1.86 Executive Management

Senior or top-level management, with statutory authority to make business, financial, and operational decisions and changes within an SOA department, corporation or commission. These are generally exempt commissioner office positions that hold the liability for department functions, service programs or other activity of department staff.

5.1.87 Externally-Facing Systems

Information systems characterized by their accessibility by users on the public Internet or on non-SOA networks. See also: *Information System*

5.1.88 Fair Use

Doctrine in United States copyright law that allows limited use of copyrighted material without requiring permission from the rights holders 17 USC § 107.

5.1.89 Federal Information Processing Standard (FIPS)

The current standard of conformance for modules implementing cryptographic algorithms and security functions. Conformance is managed through the Cryptographic Module Validation Program under NIST Computer Security Resource Center.

5.1.90 Financial Account Number

A numeric or alphanumeric group of identifiers where potential financial harm could occur to an owner if it is disclosed to an unauthorized person.

5.1.91 FIPS

Federal Information Processing Standard.

5.1.92 Firewall

Software deployed on an information system for the purpose of limiting network connectivity to that asset. See also: *Information System*

5.1.93 Forensics

The application of scientific examination of evidence to determine information about a crime or other event.

5.1.94 Flaw

An imperfection, defect or unaccountable inconstancy capable of jeopardizing the integrity of a system.

5.1.95 Geopolitical Threat

A type of threat associated with the politics of a region in which an asset, facility, or resource is located (for example, civil unrest). See also: *Threat*

5.1.96 GOV

See Office of the Governor.

5.1.97 HIPS

Host-Based Intrusion Prevention System.

5.1.98 Host-Based Intrusion Prevention System (HIPS)

A software package, network application, or other system designed to proactively detect and prevent intrusions.

5.1.99 HSS

See Department of Health & Social Services.

5.1.100 Identity Management

A formalized process for identifying, governing, and maintaining the user identifiers assigned to individuals and the rights associated with those identifiers. See also: *User Identifier*

5.1.101 IDS

Intrusion Detection System

5.1.102 Incident Reporting

The specific process of informing appropriate personnel in response to a security incident. See also: *Security Incident*

5.1.103 Incident Response

The process of taking appropriate action to a security incident. See also: *Security Incident*

5.1.104 Information

The communication or reception of knowledge or intelligence in written, electronic or oral communication form.

5.1.105 Information Asset

Information owned, held in trust, stewarded or otherwise maintained by the SOA for any purpose. See also: *Information System, Information Owner*

5.1.106 Information Custodians

A person, as prescribed by their information owner, who must implement and maintain appropriate safeguards to protect those information assets.

5.1.107 Information Disposal

The process of appropriately decommissioning information assets in a manner that preserves confidentiality as required. See also: *Information System, Information Asset, Confidentiality*

5.1.108 Information Owner

A person, as prescribed by their Business Manager, who must define the protective requirements for the information assets for which they are responsible, in accordance with SOA policies and applicable legal and regulatory requirements, and must ensure these requirements are clearly communicated to the Information Custodian.

5.1.109 Information Processing Facility

A physical location, (e.g. data center, or specially designated area) that is used for the purpose of housing information systems and/or storing, processing, or transmitting information assets. See *Information Asset, Information System*

5.1.110 Information Security

The protection of information assets and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

5.1.111 Information Security Management System (ISMS)

A formalized methodology for managing information security processes, oversight, and governance within an organization.

5.1.112 Information System

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

5.1.113 Information Technology (IT)

Any equipment or interconnected system or sub system of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

5.1.114 Information Type

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

5.1.115 Ingress/Egress

- Ingress: Network traffic that originates from outside of the network's routers and proceeds toward a destination inside of the network; or

- Egress: Network traffic that begins inside of a network and proceeds through its routers to a destination somewhere outside of the network.

5.1.116 Integrity

The property of information assets, information systems, and other resources, whereby the reliability of the asset is ensured of its adherence to a code of ethical truth, through the implementation of protections against unauthorized tampering, modification, or corruption. See also: *Information Asset, Information System.*

5.1.117 Intrusion Detection System (IDS)

Software or hardware designed to detect unauthorized attempts at accessing, manipulating, or disabling computer systems, mainly through a network, such as the Internet.

5.1.118 Intrusion Prevention System (IPS)

A network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. This technology is considered by some to be an extension of intrusion detection (IDS) technology.

5.1.119 IPS

Intrusion Prevention System

5.1.120 ISMS

Information Security Management System. See also: *Information Security Management System*.

5.1.121 IT

Information Technology.

5.1.122 Kazaa

A peer-to-peer data sharing package. See also: *Peer-to-Peer Network*

5.1.123 Kludge or Kludgy

A system, especially a computer system, that is constituted of poorly matched elements or of elements originally intended for other applications; or a clumsy or inelegant solution to a problem.

5.1.124 Labeling

The process of attaching, associating or designating data classification to a container, system, or information asset. See also: *Classification, Information System, Information Asset*

5.1.125 LAN

Local Area Network

5.1.126 LAW

See Department of Law.

5.1.127 Least Privilege

An access control methodology characterized by granting the minimum required privilege to users to accomplish their duties. See also: *Access Control*

5.1.128 Limewire

A peer-to-peer data sharing package. See also: *Peer-to-Peer Network*

5.1.129 Local Area Network (LAN)

A communications network connecting various hardware devices together within a building by means of a continuous cable or an in-house voice-data telephone system.

5.1.130 MAC Address

A network-unique hardware identifier used by layer-2 communication protocols.

5.1.131 Major Revision

Process of a product upgrade which could involve a software version improvement or service pack advancement on software from any security flaws.

5.1.132 Malicious Software

Software designed to circumvent one or more security controls and/or create damage that would compromise security.

5.1.133 Malware

Software designed to interfere with a computer's normal function. See also: *Malicious Software*

5.1.134 Malware Prevention Software

Software deployed for the purposes of finding and removing malicious software. See also: *Malicious Software*

5.1.135 Minor Revision

Process of a product update to keep pace with the most recent software effectiveness, which could involve security patches to fix a flaw in the software.

5.1.136 Mobile Code

Software characterized by the ability to transmit itself across network boundaries for remote execution.

5.1.137 NAT

Network Address Translation.

5.1.138 Need to Know

"Need-to-know" means an individual has a business reason to access or share information.

5.1.139 Network Address

A unique identifier assigned to a device for the purpose of routing network packets. See also: *Unique Identifier*

5.1.140 Network Address Translation (NAT)

NAT (Network Address Translation or Network Address Translator) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

5.1.141 Network Security

A process of governing information security aspects of wired and wireless network, transport, and data communications pathways.

5.1.142 Network Sniffer

A software utility or a device used to passively eavesdrop, collect or analyze information packets on a network.

5.1.143 Network Time Protocol (NTP)

A TCP/IP protocol used to synchronize the real-time clock in computers, network devices and other electronic equipment that is time sensitive. It is also used to maintain the correct time in NTP-based wall and desk clocks.

5.1.144 Non-repudiation

A concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract. Although this concept can be applied to any transmission, including television and radio, the most common application is in the verification and trust of signatures.

5.1.145 NTP

Network Time Protocol.

5.1.146 Office of the Governor (GOV)

State of Alaska Office of the Governor.

5.1.147 Open Web Application Security Project (OWASP)

OWASP is an open-source application security project. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. OWASP advocates approaching application security by considering the people, process, and technology dimensions.

5.1.148 Operating System Security

The process of governing the information security aspects of the operating system installed on a particular information system. See also: *Information System*

5.1.149 OWASP

Open Web Application Security Project

5.1.150 Password Cracker

A software utility or a device used for the purpose of obtaining passwords – usually via brute force. See also: *Authentication*

5.1.151 Payment Card Industry Data Security Standard (PCI DSS)

Industry self-regulation governing the information security aspects of storing, processing, or transmitting information related to payment processing.

5.1.152 PCI DSS

Payment Card Industry Data Security Standard. See also: *Payment Card Industry Data Security Standard*

5.1.153 Peer-to-Peer Network

A distributed data sharing network often times used to share copyrighted music, software, and movies.

5.1.154 Personally Identifiable Information (PII)

An "individual's name", which means a combination of an individual's first name or first initial; and last name; and one or more of the following information elements:

- The individual's social security number;
- The individual's driver's license number
- State identification card number;
- The individual's account number;
- Credit card account number;
- Debit card account number; or
- Financial account passwords or access codes.

5.1.155 Personnel

Employees, partners, contractors, consultants, temporaries, other SOA workers and workers affiliated with third parties or anyone having access to SOA information that is not directly accessible to the general public from a non-SOA network (e.g. Internet).

5.1.156 Physical Security Controls

A type of security control implemented primarily via physical mechanisms. See also: *Security Controls*

5.1.157 Physical Threat

A type of threat associated with the physical parameters of an asset, facility, or resource. See also: *Threat*

5.1.158 PII

Personal Identifiable Information.

5.1.159 PKI

Public Key Infrastructure Cryptographic Algorithm.

5.1.160 Policy Exception

A formalized written statement granting one or more processes, information systems, personnel, or other entities the license to continue performing activities on behalf of the

organization for a defined period of time despite known areas of noncompliance with defined information security policy. See also: *Information System*

5.1.161 Policy Statement

A formalized statement detailing the requirements, mandates, and strictures to be used within the organization.

5.1.162 Post Mortem Report

A report created after a security incident violation detailing all specific events related to the security incident. See also: *Security Incident*

5.1.163 Privacy

The property of confidentiality ascribed to a particular information asset. See also: *Confidentiality, Information Asset*

5.1.164 Private Key

The portion of a cryptographic key within a public key cryptosystem that must be kept secret and not shared with others. See also: *Public Key Cryptosystem, Cryptographic Key, Public Key*

5.1.165 Prohibited

To forbid, by authority, access to any established list, objective or action; such as in reference to forbidden sites – e.g. pornographic, gambling, etc.

5.1.166 Proxy Server

Is a computer within the networks system that acts as an intermediary for requests from users seeking resources from other servers. A user connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. If the request is validated by the filter, the proxy server provides the resource by connecting to the relevant server and requesting the service on behalf of the user.

5.1.167 Public

The classification level ascribed to assets that have been specifically approved for access to the general public. See also: *Classification*

5.1.168 Public Key

The portion of a cryptographic key within a public key cryptographic algorithm that may be shared with other parties. See also: *Public Key Cryptosystem, Cryptographic Key, Private Key*

5.1.169 Public Key Infrastructure Cryptographic Algorithm (PKI)

A cryptographic technique in which two key values – one public and one private – are required for proper operation. See also: *Encryption, Cryptographic Key*

5.1.170 Record Retention

The act of preserving records such as information assets, documents, or other artifacts for a defined period of time prescribed by a fully authorized SOA records retention schedule under AS 40.21. See also: *Information Asset*

5.1.171 Recovery

The restoration of a stolen, lost, or corrupted information asset with a backup. See also: *Backup*

5.1.172 Recovery Key

A key used within many commercial cryptographic systems to enable data recovery. See also: *Encryption, Cryptographic Key*

5.1.173 Remote Authentication Dial-In User Service

A technical security control that consists of a protocol to identify and assign access to remote-access entities. See also: *Technical Security Control, Access Control*

5.1.174 Restricted

Indicates restriction to a specific subject or object that in general is not accessible and may only be authorized for limited use and time based on business needs of the individual user or business agency.

5.1.175 Risk

The threat or probability that an action or event will adversely or beneficially affect an organization's ability to achieve its objectives. See also: *Threat*

5.1.176 Risk Assessment

Formalized methodology for evaluation of risks presented by one or more threats against an information asset. See also: *Information Asset, Risk, Threat*

5.1.177 Risk Management

The identification, assessment, and prioritization of threats followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unforeseeable events or exposed unauthorized disclosure.

5.1.178 Risk Treatment

A formalized methodology for the mitigation and management of risks. See also: *Risk*

5.1.179 Role Based Access Control

An access control methodology characterized by the grouping of users into defined roles and assigning privileges to those roles, in accordance with the duties and function of the role. See also: *Access Control*

5.1.180 Rootkit

A specific type of malware categorized by remote control of a single information system. See also: *Malware*

5.1.181 Secure Area

A physical location that has been audited or certified by SSO as having met security controls for a specific purpose.

5.1.182 Secure Shell (SSH)

A command-line oriented remote access protocol, characterized by confidential and authenticated communications. See also: *Confidentiality, Authentication*

5.1.183 Security Category

The characterization of information or an information system based on an assessment of the potential impact that loss of confidentiality, integrity and availability of such information or information system would have on an organization's operation, assets or individuals.

5.1.184 Security Controls

Technical, administrative, or procedural safeguards deployed to ensure the continued confidentiality, integrity and availability of Information Assets and Information Systems. See also: *Information System, Information Asset, Confidentiality, Integrity and Availability*

5.1.185 Security Event

A specific event, either intentionally or unintentionally instigated or occurring by environmental impact that may have an undesirable affect on the confidentiality, integrity and availability of an information asset. See also: *Security Incident, Confidentiality, Integrity and Availability, Information Asset*

5.1.186 Security Incident

A security event that has been identified and formally assigned incident status within the security incident management process. See also: *Security Event*

5.1.187 Security Objective

The approach to maintain confidentiality, integrity and availability.

5.1.188 Segregation of Duties

An administrative control approach consisting of separation of critical security tasks among different personnel in order to prevent collusion and ensure security task integrity.

5.1.189 Sensitive Information/Data

Information and data that might result in the loss of a level of security if revealed or disclosed to a person with an unknown trustability or hostile intentions.

5.1.190 Service Set Identifier (SSID)

A human-readable identifier assigned to a wireless (802.11x) network. See also: *802.11x*

5.1.191 SOA

State of Alaska.

5.1.192 SOA Internal

The State of Alaska classification level ascribed to assets that are not defined as confidential but are not immediately accessible to the general public. See also: *Classification*

5.1.193 Social Engineering

The process of gaining access to a resource through subterfuge which usually occurs through misrepresenting oneself to organizational personnel.

5.1.194 Software Vulnerability

The vulnerability extant due to the software base installed on a deployed Information System. See also: *Information System, Vulnerability*

5.1.195 SPI

Stateful Packet Inspection

5.1.196 Spyware

A specific category of malware categorized by dissemination of personal information to others. See also: *Malware*

5.1.197 SSC

State Service Center.

5.1.198 SSH

Secure Shell. See *Secure Shell*

5.1.199 SSID

Service Set Identifier. See *Service Set Identifier*

5.1.200 SSO

State Security Office.

5.1.201 State Information System

Information processing systems owned, managed, or otherwise used by the SOA for the processing, storage, or transmission of Information assets. See also: *Information Asset.*

5.1.202 State Security Office (SSO)

The lead authority for information security within the SOA executive branch.

5.1.203 State Service Center (SSC)

The support center for SOA customers to report problems, request service, or asks questions regarding SOA information technology and telecommunications.

5.1.204 Stateful Packet Inspection (SPI)

A firewall technology which ensures that all inbound packets are the result of an outbound request. Designed to prevent harmful or unrequested packets from entering the computer.

5.1.205 TACACS+

Terminal Access Controller Access-Control System Plus.

5.1.206 Technical Security Controls

A type of security control implemented primarily via technological mechanisms. See also: *Security Controls*

5.1.207 Technology Management Council (TMC)

The Technology Management Council (TMC) membership of seven consists of the Director of the Division of Enterprise Technology Services (ETS) and one IT Manager (ITM) representing each of the six service areas:

i. HSS IT Manager
ii. DOT IT Manager
iii. General 1 (LAW, GOV, DOA)
iv. General 2 (DED, EED, DOL, DOR)

v. Public Protection (DOC, DMVA, DPS)
vi. Resources (DEC, DRG, DNR)

5.1.208 Terminal Access Control Access-Control System Plus (TACACS+)

A technical security control consisting of a protocol for identifying and assigning access to entities on a network. See also: *Technical Security Control, Access Control*

5.1.209 Third Party

A person or group of people who perform contract service for the State of Alaska.

5.1.210 Threat

A condition of intentional expression to inflict damage, which, should it occur, would negatively impact the security of the SOA organizations and businesses. See also: *Risk*

5.1.211 Threat Mitigation

The process to neutralize or counteract the activity or affect of a threat. See also: *Threat*

5.1.212 TMC

Technology Management Council.

5.1.213 Trojan Horse

A specific category of malware disguised as a useful computer program that contains concealed instructions which, when activated, performs an illicit or malicious action (e.g.as destroying data files). See also: *Malware*

5.1.214 Two-Factor Authentication

A strong authentication strategy utilizing two distinct substantiated verification factors. See also: *Authentication, Authentication Factors*

5.1.215 Unauthorized Disclosure

Access without explicit permission from a Business Manager, statute, regulation or job responsibility.

5.1.216 Unique Identifier

A unique index assigned to an entity for the purpose of granting access to resources and identification. See also: *Authentication, User Identifier*

5.1.217 Unsolicited Email

E-mail spam, also known as junk e-mail, is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. A common synonym for spam is unsolicited bulk e-mail (UBE). Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. "UCE" refers specifically to unsolicited commercial e-mail. Notifications sent by Executive Management or Business Owners regarding problems, programs, functions or other related topics sent to SOA personnel is NOT considered SPAM or UBE.

5.1.218 User Identifier

An index assigned to a user for the purpose of granting access to resources and identification of the user within a population. See also: *Authentication*

5.1.219 Violation

A breach, infringement, or transgression of policy, procedure, statute, regulation, or an executive or administrative order.

5.1.220 Virtual Private Network (VPN)

A technical security control designed to ensure confidentiality, integrity, and availability of information transmitted between two points across a public network. See also: *Confidentiality, Integrity, and Availability*

5.1.221 Virus

A specific malware category of a computer program that is usually hidden within another seemingly innocuous program which produces copies of itself and inserts them into other programs and usually performs a malicious action such as destroying data. See also: *Malware*

5.1.222 VPN

Virtual Private Network. See *Virtual Private Network*

5.1.223 Vulnerability

The vector by which a threat of an attack or an intention to do damage is realized. See also: *Threat*

5.1.224 Vulnerability Management

A formalized process for identifying, evaluating, tracking, and remediating vulnerabilities. See also: *Vulnerability*

5.1.225 Vulnerability Scanner

A software package or device used for the purpose of enumerating software vulnerabilities on a given host. See also: *Software Vulnerability*

5.1.226 WAN

Wide Area Network

5.1.227 Web Filtering

The process that monitors SOA Internet usage and restricts access to known harmful (viruses, spyware and malware) websites, websites with excess bandwidth utilization, and/or websites where there are no apparent SOA business requirements to access the website.

5.1.228 Wide Area Network (WAN)

A system consisting of a set of nodes that are interconnected by a set of links, and generally covers a large geographic area, usually on the order of hundreds of miles.

5.1.229 Worm

A specific category of malware categorized by self-replication using means other than file infection. It usually performs a malicious action such as destroying data. See also: *Malware*

5.1.230 Written Consent/Approval

A written document authorizing a release or use of information or an object; usually contains a summarization of purpose, risks, benefits, confidentiality, details of rights or information about the consent, a signature and a date.

5.1.231 Zero-day Exploit

A computer threat (attack or vulnerability) that tries to exploit computer application vulnerabilities that are unknown to others, undisclosed to the software developer, or where no security fix is available. This attack uses heuristic methodology techniques to enhance the attack, which challenges detections and solutions.

5.1.232 Zero-day Protection

A tool that provides the ability to protection against zero-day exploits, without updates.

Title:	Information Security Policy Index	Effective:	12/19/2025
		Last Review:	12/19/2025
		Review Frequency:	Annually
Number:	ISP-003		
Version:	1.04	Approved by:	CIO
Pages	8	Distribution:	SOA

1. Purpose

To provide a summary of the requirements outlined within State of Alaska (SOA) Information Security Policies (ISP).

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy is:

- An Information Security Policy (ISP) Index; and
- A brief description of the SOA ISP policies.

5.1. Policy Framework

5.1.1 ISP-001: ISP Framework

This policy:

- Provides the framework that defines SOA scope and policy responsibilities for SOA information assets; and
- Establishes the Information Security Management System (ISMS);

5.2. References

5.2.1 ISP-002: ISP Glossary

This policy defines:

SOA Internal

- The terms used within the ISPs.

5.2.2 ISP-003: Information Security Policy (ISP) Index

This policy is:

- An ISP Index; and
- A brief description of the SOA ISP policies

5.2.3 ISP-004: ISP Policy Regulatory Index

This policy is:

- A cross-referencing regulations map of SOA statutes, regulations, AAM, industry best practices and the State Information Security Office (SSO) ISPs.

5.2.4 ISP-005: ISP Policy Development Reference Guide

This guide:

- Provides the layout and directions to define and develop department specific security policies; and
- Outlines the methodology and customized approach to modification and finalization.

5.2.5 ISP-006: ISP Policy Template

This template is formatted to assist in the physical process of writing a policy.

5.3. Security Policy

5.3.1 ISP-101: Policy Approval and Review

This policy stipulates requirements for:

- Policy approval
- Policy review

5.3.2 ISP-102: Risk Management

This policy stipulates the process for:

- Risk management
- Risk response
- Risk evaluation

5.3.3 ISP-103: Managing Exceptions

This policy stipulates requirements for:

- Exception evaluations
- Exception requests
- Exception reviews

5.4. Organizational Security

5.4.1 ISP-111: Roles and Responsibilities

This policy stipulates:

- Executive Management responsibilities;
- Allocation of responsibilities;
- Department Information Security Officer (ISO) responsibilities;
- Department Computer Security Designee (CSD) responsibilities; and
- Personal responsibilities.

5.4.2 ISP-112: Third Party Security

This policy stipulates requirements for:

SOA Internal

- Risk management;
- Third party access;
- Third party agreement; and
- Third party management.

5.5. Asset Management

5.5.1 ISP-121: Asset Classification and Control

This policy defines:

- Inventory assets;
- Information classification;
- Information handling and labeling; and
- Information classification reference table guideline.

5.5.2 ISP-122: Privacy of Personal Information

This policy stipulates requirements for:

- Safeguarding confidential information;
- Public communication and notification following loss of personally identifiable information; and
- Personally identifiable information retention.

5.5.3 ISP-123: Security Categorization of SOA Information & Information Systems

This policy defines:

- Categorization of information and information system standards;
- Categorization of information and information system security objectives;
- Potential impact on organizations & individuals guidelines for risk levels;
- Security categorization applied to information types;
- Security categorization applied to information system;
- Table indicating risk level of disclosure; and
- Table specifying SOA examples of information risk levels.

5.5.4 ISP-124 Compliance with Statutes and Regulations

This policy defines:

- SOA compliance with statutes and regulations;
- Compliance with regulatory agencies standards; and
- Proper crediting of source information.

5.5.5 ISP-125 ESI Hold and Search Requests

This policy stipulates the requirements for:

- All ESI holds and searches that are authorized by the CIO or CIO's designee.

5.6. Personnel Security

5.6.1 ISP-131: Personnel Security

This policy stipulates requirements for:

- Personnel security responsibilities;
- Appropriate access to information;
- Personnel safeguards, access and termination;
- Personnel training and awareness; and

SOA Internal

- Personnel security background checks.

5.6.2 ISP-132: Security Awareness and Training

This policy stipulates appropriate:

- Program design;
- Program material; and
- Program implementation.

5.7. Physical & Environmental Security

5.7.1 ISP-141: Secure Areas

This policy defines:

- Secure areas.

5.7.2 ISP-142: Equipment Security

This policy stipulates:

- Equipment must be secure and protected; and
- Access controls must be implemented.

5.7.3 ISP-143: Information Disposal

This policy stipulates requirements for:

- Secure disposal; and
- Information disposal.

5.7.4 ISP-144: Portable Media and Devices

This policy stipulates proper:

- Use of portable data devices.

5.8. Incident Management

5.8.1 ISP-151: Incident Response

This policy stipulates:

- Incident response authority;
- Incident response management;
- Incident assessment and escalation;
- Incident response;
- Incident resolution; and
- Incident response reporting.

5.8.2 ISP-152: Incident Reporting

This policy stipulates the process for:

- Incident reporting.

5.9. Communication & Operational Management

5.9.1 ISP-161: Protection against Malicious Software

This policy stipulates requirements for:

- Protection against malicious code (pre/post introduction to the network environment); and
- Remediation of systems.

SOA Internal

5.9.2 ISP-162: System Planning and Acceptance

This policy stipulates requirements for:

- System planning and acceptance;
- System criteria and testing;
- Implementation training;
- Information system documentation; and
- Security planning.

5.9.3 ISP-163: Electronic Messaging

This policy stipulates requirements for:

- System ownership and email account management;
- Use of messaging systems;
- Message protection;
- Electronic messaging administration, archive and retention; and
- Safeguards.

5.9.4 ISP-164: Security Monitoring

This policy stipulates requirements for:

- System logging;
- Protection of logging and auditing information;
- System monitoring; and
- Configuring network time protocol (NTP).

5.9.5 ISP-165: Operations Security

This policy stipulates:

- Operational responsibilities;
- System recovery requirements; and
- Requirements for electronic commerce protections.

5.9.6 ISP-166: Web Filtering

This policy stipulates:

- Prohibited website categories;
- Website filtering waiver form requirements; and
- Website waiver form example.

5.10. Access Control

5.10.1 ISP-171: Identity Management

This policy stipulates requirements for:

- User accounts;
- User account controls;
- Authentication;
- Account management; and
- Account and access management.

5.10.2 ISP-172: Business Use and Access Control

This policy stipulates:

- User Access.

5.10.3 ISP-173: Network Security

This policy stipulates requirements for:

SOA Internal

- Network management;
- Network systems;
- Network audits;
- Network design; and
- Network security.

5.10.4 ISP-174: Operating System Security

This policy stipulates requirements for:

- Configuration and deployment;
- User authentication and access control;
- Systems utilities;
- Connection time; and
- Configuration of Network Time Protocol (NTP).

5.10.5 ISP-175: Mobile Computing and Remote Access

This policy defines requirements for:

- Mobile computing devices;
- Remote access; and
- Secure configuration.

5.10.6 ISP-176: Application Lifecycle Management

This policy stipulates requirements for:

- Security review; and
- Application planning and acceptance.

5.10.7 ISP-177: Wireless Network Security

This policy stipulates requirements for:

- Wireless connections;
- Secure configuration of wireless devices;
- Secure configuration of wireless networks; and
- Secure monitoring.

5.10.8 ISP-178: Password Management

This policy stipulates:

- Requirements for setting passwords;
- Protections from disclosure; and
- Proper administration of passwords.

5.10.9 ISP-179: Firewalls

This policy stipulates:

- SOA firewall requirements; and
- Department firewall requirements.

5.11. Systems Development & Maintenance

5.11.1 ISP-191: Security in System Development

This policy stipulates requirements for:

- System planning;
- Software development and implementation;
- System awareness;
- System testing;
- System acceptance; and

SOA Internal

- Secure system build.

5.11.2 ISP-192: Encryption

This policy stipulates the requirements for:

- Use of encryption;
- Implementation of encryption services; and
- Sufficient encryption.

5.11.3 ISP-193: Vulnerability Management

This policy stipulates requirements for:

- Vulnerability management; and
- Patch management.

5.11.4 ISP-194: External Email Encryption

This policy defines:

- Encryption mechanism implementation; and
- Encryption availability for all SOA emailed information assets.

5.11.5 ISP-195: Prohibited Use of Password Protected Content & Pre-Encrypted Attachments

This policy defines requirements for:

- Local password protection and attachment encryption;
- Image format text based documents; and
- SOA system-wide encryption.

5.11.6 ISP-196: Cloud and Offsite Hosting

This policy stipulates:

- Cloud and Offsite Hosting.

5.12. Business Continuity Management

5.12.1 ISP-201: Business Continuity

This policy stipulates:

- Establishment of COOP;
- COOP infrastructure; and
- COOP planning.

5.13. Compliance

5.13.1 ISP-211: Copyright Information and Unauthorized Software

This policy stipulates:

- Proper use of copyright material;
- Software guidelines; and
- Preservation of intellectual property rights.

5.13.2 ISP-212: Compliance Monitoring

This policy stipulates requirements for:

- Implementing and reviewing controls; and
- Methods for assessing compliance.

SOA Internal

5.13.3 ISP-213: System Audit

This policy stipulates requirements for:

- Information system audits;
- CIO notification requirement of external electronic and IT audits; and
- Audit tools authorization.

5.13.4 ISP-214: Auditing and Compliance

This policy stipulates requirements for:

- Independent information system auditing and compliance monitoring; and
- Authorizations for auditing and compliance monitoring.

SOA Internal

1.1. A Cross-Regulatory Map

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
001	8.5		13.1.1	IR-4	164.314(b)(2)(iv)	
001	6.1.1	AAM 100.060, AAM 230.010	6.1.1			
001	6.1.2		4.2.2.c			
001	6.2.1		4.2.1.i		164.308(a)(1)	
001	6.2.2	AAM 38.335	6.1.3		164.308(a)(3)	
001	6.2.2	AAM 100.060, AAM 230.010	6.1.1		164.308(a)(3)	
001	6.2.3	AAM 38.335	6.1.3		164.308(a)(3)	
001	6.2.4	AAM 38.335	6.1.3		164.308(a)(3)	
001	6.3.1		5.1.1, 8.2.2	AT-1, AT-2		13403(a)
001	6.3.2	AAM 38.335	7.1.3	PL-4		
001	6.3.3	AAM 38.335	7.2.2	AC-14	164.312(c)(2)	

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.2		3.4e, 3.5c, 5.2.2. 5.4, 5.5	45.48.010, 45.48.040, 45.48.180		5.6.8	DS8.2, PO9.5, PO9.6
			3.1c, 3.2e			1.2, 4.7.3	
							PO6.2
	4.1						PO6.7
	4.3	1.1.4, 12.5	3.1a, 3.1d, 3.2c			1.2, 2.5	PO4.2
	4.3		3.1c, 3.2e			1.2, 4.7.3	PO4.7, PO6.8
	4.3	1.1.4, 12.5	3.1a, 3.1d, 3.2c			1.2, 2.5	PO4.7
	4.3	1.1.4, 12.5	3.1a, 3.1d, 3.2c			1.2, 2.5	PO4.4,
			2, 3.5e, 4.3			4.7.3, 5.6.3, 5.6.11, 5.62, 6.1	PO6.1
		12.3.5				2.2	ME2.5,ME4.7
	4.16	9.7, 9.7.1, 9.7.2	7.1			5.1, 5.3	DS5.8

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
001	6.3.4	AAM 90.020, AAM 200.040, AAM 38.335	11.1.1, 11.2.2	AC-6, AC-2, AC-1		
001	6.3.5		15.1.1	PS-1		13421
001	6.4.1	AAM 38.335	7.1.1		164.312(e)(2)(i)	
001	6.4.2	AAM 38.160	7.2.1, 7.2.2		164.312(c)(2)	
001	6.5.1	AAM10.050	13.1.1	IR-1	164.308(a)(6), 164.314(b)(2)(iv)	13402
001	6.5.2	AAM 38.335	13.2.1, 13.2.2	IR-1, IR-4, IR-5, IR-6		13402(i)(2)
001	6.6.1		4.2.1.c-e	RA-1	164.308(a)(1)(ii)(A)	
001	6.6.2		4.2.1.f-g, 14.1.2	RA-1, RA-3	164.308(a)(1)(ii)(B)	
001	6.7.2		8.2.3	PS-8	164.308(a)(1)(ii)(C)	
101	5.1.1	AAM 90.010	5.1.1		164.308(a)(1)	
101	5.1.2		5.1.2	AT-1, AT-2	164.316(a)	
101	5.1.3		5.1.1		164.316(b)(1), 164.316(b)(2)(ii)	
101	5.2.1	AAM 38.335	5.1.2		164.316(a), 164.316(b)(2)(iii)	
102	5.1.1		4.2.1	RA-1		
102	5.1.2		4.2.1	RA-1		
102	5.1.2		4.2.1	RA-5		
Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		7.1, 7.1.1, 7.2.2	3.2d, 3.4a, 7.3.2.1, 8.2			2.1, 5.6.1, 5.6.7	
			2.1				ME3.2
	4.18	12.3.3, 12.10.1					PO8.6
	4.16		7.1			5.1, 5.3	PO2.3
	4.3, 4.20		3.3d, 3.4e, 3.5c, 5.2.2, 5.4, 5.5	45.48.010, 45.48.040, 45.48.180		5.6.8	PO9.5, PO9.6, DS8.2
		12.5.2, 12.9.1, 12.9.6	3.3d, 5.5			5.6.8	PO9.5, PO9.6, DS8.2, DS8.4 DS5.6, PC-5
	4.1	12.1.1					PO9.1, PC-5
	4.1						PO9.3, PO9.4, PO9.5
	4.1		3.2a, 4.2			5.6.11	
	4.1		2.0			5.6.2	PO6.1, PO4.14
	4.21		2.3			5.63	PO6.2
	4.22		2.0			5.6.2	PO2.3
	4.21, 4.22	12.1.3	2.3			5.63	PO6.2
		12.1.2					PO9.3
		12.1.2					PO9.3
		12.1.2					PO9.3,
	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)

Internal

102	5.2.1		4.2.1	RA-3		
102	5.3.1		4.2.1	RA-3, RA-4		
103	5.1.1		4.2.1	RA-1		
103	5.1.2		4.2.1	RA-1, RA-3		
103	5.2.1		4.2.1	RA-1, RA-3		
103	5.2.2		4.2.1	RA-1, RA-3		
103	5.3.1		4.2.1	RA-1, RA-3		
103	5.3.2		4.2.1	RA-1, RA-3		
111	5.2		6.1.4	PE-17	164.308(a)(4)	
111	5.2	AAM 38.335	6.1.3			
111	5.2		6.1.3	PC-4		
111	5.1.1	AAM 100.060, AAM 230.010	6.1.1		164.308(a)(3)	
111	5.1.2		6.1.2		164.308(a)(3)	
111	5.2.1	AAM 38.195	6.1.5	PS-6	164.308(b)(1), 164.308(b)(4), 164.314(a)	
111	5.5.1		6.1.7	SI-5		
111	5.5.1		11.3.3	PE-5		
111	5.5.1		11.3.2	AC-11, AC-12		
111	5.5.1		6.1.6	IR-4		

SOA Internal

							PO9.3, PO9.4,
		12.1.3					DS5.1
							M2.3
							M2.2
							M2.3
							M2.3
	4.4		3.1c			2.1	
		1.1.4, 12.5	3.1a, 3.1d, 3.2c			1.2, 2.5	PO4.7
		12.4				4.7.3	PO4.4,
	4.3	12.4	3.1c, 3.2e			1.2, 4.7.3	PO4.6, PO7.3
	4.3	12.4	3.1a, 3.5b, 5.4			2.5, 4.7.3,	
	4.9, 4.19						DS5.4,
							DS10, DS11, DS12, DS13
		12.4				4.7.3	DS5, PO4.6
		12.4				4.7.3 5.6.17.5	DS5
			3.1c, 5.2.2				DS8.2, PO9.5, PO9.6

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
112	5.1.1	AAM 100.120, AAM 38.335	6.2.1, 8.1.3			
112	5.2.1	AAM 38.335	6.2.2			13404(b)
112	5.3.1	AAM 38.335	6.2.3	PS-6		13404(a)
112	5.3.2	AAM 38.335	6.2.3, 10.2.1	PS-6		
112	5.3.3	AAM 38.335	6.2.3	PS-6		13402(b)
112	5.3.4		6.2.3	PS-6		
112	5.3.5	AAM 38.335	10.8.2, 10.2.2	SC-9, SA-9		13402(b), 13404(a), 13408
112	5.4.1	AAM 38. 335	10.2.3	CM-3, SA-9		13407(b)
121	5.37	AAM 38.335	9.2.6	MP-6, MP-7		
121	5.1.1	AAM 38.335	7.1.1	CM-2		
121	5.2.1	AAM 55.060	7.1.2			
121	5.2.2	AAM 38.160	7.2.1			
121	5.2.3	AAM 38.160	7.2.1			
121	5.2.4	AAM 38.335	7.2.2	AC-15		
121	5.2.5	AAM 38.335	7.1.3			

SOA I

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		12.8, 12.10.2	3.1a, 3.2a, 6.3	45.48.520		3.3, 5.3, 5.2, 5.6.11	DS2.4
		12.10.2	6.3	45.48.520			DS2.7
		12.8, 12.10.2, 12.10.3	6.3, 6.7	45.48.520		3.3, 5.3, 5.5.2, 5.5.3	M3.2
		12.8, 12.10.2, 12.10.3	6.3, 6.7	45.48.520		3.3, 5.3, 5.5.2, 5.5.3	M1-1
		12.8, 12.10.2, 12.10.3	6.3, 6.7	45.48.520		3.3, 5.3, 5.5.2, 5.5.3	M3.2
			6.3, 6.7	45.48.520		3.3, 5.3, 5.5.2, 5.5.3	M3.2
			6.2, 6.3, 6.6	45.48.520		5.4, 5.6.14	ME3.1
		12.8, 12.10.4	6.3	45.48.520		5.6.14	DS2
		9.1, 9.10.1, 9.10.2	3.4d, 4.6, 4.7, 7.9			8.4	DS11.4,
		12.3.3, 12.10.1					PO8.6
		12.3.4					PO4.7, PO4.8
						5.1	PO2.3, PO2.4
						5.1	PO2.3
		9.7, 9.7.1, 9.7.2	7.1			5.1, 5.3	PO2.3, DS11.6, AC2
		12.3.5				2.2	PO6.5

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
121	5.3.1	AAM 38.335	7.2.2	AC-15, AC-16		
121	5.3.2	AAM 38.335	7.2.2	AC-16		
121	5.3.3	AAM 38.335	7.2.2	AC-16		
121	5.3.4	AAM 38.335	7.2.2, 11.3.3	AC-16		
121	5.3.5	AAM 38.335	7.2.2	AC-16		
121	5.3.6	AAM 90.020	11.6.1	CM-5	164.312(a)(2)(iv)	
122	5.32	AAM 38.335	9.2.6	MP-6, MP-7	164.310(d)(1)	
122	5.1.1	AAM 10.035, AAM 50.140, AAM 38.335	10.7.3	MP Family, SI-12	164.316(a)	
122	5.1.2		15.1.1	AC-1		
122	5.1.3		15.1.1	AC-1		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		9.7, 9.7.1, 9.7.2	7.1			5.1, 5.3	DS5.8
		9.7, 9.7.1, 9.7.2	7.1			5.1, 5.3	DS5.8
		9.7, 9.7.1, 9.7.2	7.1			5.1, 5.3	DS5.8
		9.7, 9.7.1, 9.7.2, 8.5.15	7.1			5.1, 5.3	PO2.3
		9.7, 9.7.1, 9.7.2	7.1			5.1, 5.3	DS5.8
	4.14	12.3.10	6.3			4.7.2, 5.6.7, 5.6.15	DS11
	4.13	9.1, 9.10.1, 9.10.2	3.4d, 4.6, 4.7, 7.9	45.48.500		8.4	DS11.4,
	4.21	3.4, 9.6, 9.7, 9.7.1, 9.7.2, 9.8	8.6		99.31,(a)(1), 99.31(a)(2)	4.3.6,4.3.74.3.8, 4.7.2, 5.6.10, 6.3.2, 6.3.3	DS11.1, DS11.2, DS11.4, DS11.5, DS11.6, PC5, AC6
			2.1	45.48.400, 45.48.410, 45.48.420, 45.48.430	99.37(d)		DS11.17, DS11.18
		PCI-DSS V1.2	2.1	45.48.750	99.31(a)(1)		DS11

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
122	5.2.1	AAM 90.020, AAM 200.040, AAM 38.335	6.1.7, 11.1.1, 13.1.2	IR-6, MP-1	164.308(a)(6), 164.314(b)(2)(iv)	13402(a)
122	5.2.2					
122	5.3.1	AAM 38.335	7.2.2	AC-15, AC-16, AC-17	164.312(c)(1), 164.312(e)(2)(ii), 164.313 (c)	
123	5.2	AAM 38.335	7.2.1	AC-15, AC-16, AC-17		
123	5.3	AAM 38.335	7.2.2	AC-15, AC-16, AC-17		
123	5.4	AAM 38.335	7.2.2	AC-15, AC-16, AC-17		
124	5.1.1	AAM 38.335	15.1.1, 15.1.2, 15.1.3, 15.1.4, 15.1.6, 15.2.1			13421
125						
131	5.3		8.1.2, 8.3.1,	Ps-4, PS-5	164.312(a)(1)	
131	5.1.1	AAM 38.335	8.1.1	PS-1	164.308(a)(5)	
131	5.2.1	AAM 90.020, AAM 38.335	11.1.1	AC-1	164.308(a)(4)(ii)(B)	13401(a)

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.6, 4.20	7.1, 7.1.1		45.48.010	99.5		DS10
					99.5		
	4.12, 4.14	9.7, 9.7.1, 9.7.2	7.1	45.48.500	99.31(a) (1)	5.1, 5.3	DS5.21
	4.16	9.7, 9.7.1, 9.7.2	7.1		99.31(a) (1)	5.1, 5.3	PO2.3
	4.16	9.7, 9.7.1, 9.7.2	7.1		99.31(a) (1)	5.1, 5.3	PO2.3, DS11.6, AC2
	4.16	9.7, 9.7.1, 9.7.2	7.1		99.31(a) (1)	5.1, 5.3	PO2.3
		3.2, 3.2.1, 3.2.2	7.1	45.48.750		2.5, 3.1, 4.7.3, 5.6.7, 6.3.5	ME3.2, PO3.2
	4.14	12.7	4.5			5.2, 5.6.11	PO7.8
	4.4	12.9.3	3.1a, 3.4c, 5.2.2			5.6.3	PO4.6, PO7.3, PC5
	4.4	7.1, 7.2	3.2d, 7.3.2.1, 8.2			2.1	DS5.2

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
131	5.2.1	AAM 38. 335	10.10.2	MA-05(b), MA-05(c), PE-6, PE-8, SI-4	164.308(a)(3)(ii)(A)	13401(a)
131	5.3.1	AAM 100.120, AAM 38.335	8.1.2	PS-2	164.308(a)(3)(ii)(B)	
131	5.3.2		8.3.1	PS-5		
131	5.3.3		8.3.1, 8.3.2	PS-4	164.308(a)(3)(ii)(C)	
131	5.4.1		8.2.2	AT-3	164.308(a)(5)	13403
132	5.1.3	AAM 38.335	8.2.2	AT-1, AT-2	164.308(a)(5)(ii)(A)	
132	5.1.1	AAM 38.335	6.1.3		164.308(a)(2)	
132	5.2.1		8.2.2	AT-1, AT-2		
132	5.2.1	AAM 38.335	8.2.2	AT-3, AT-4		
132	5.2.2	AAM 38.335	8.2.2	AT-3	164.308(a)(4)(ii)(C)	13403(a)
132	5.3.1	AAM 38.335	8.2.2	AT-1, AT-4		
132	5.3.2	AAM 38.335	8.2.2, 8.2.1	AT-3		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.3	10.6, 11.4, 11.5, 12.5.5, 12.9.5	6.3, 7.8, 7.14			3.2, 5.6.2	DS5.5
	4.1	12.7	3.1a, 3.5e, 4.5.1, 6.3			5.2, 5.6.11	PO4.13, PO7.3
						5.6.11	PO7.8
	4.3		8.2.3			5.6.11	PO7.8
	4.5		3.5e, 4.3, 6.3			4.7.3, 5.6.3, 5.6.11, 6.1	PO7.4, DS7.2,
	4.5	12.6, 12.6.1, 12.9.4	3.5e, 4.3, 6.3			4.7.3, 5.6.3, 5.6.11, 6.1	DS7.1, PC5, PO7.4, DS7.2
	4.2	1.1.4, 12.5	3.1a, 3.1d, 3.2c			1.2, 2.5	PO4.7, PO6.11
			3.5e, 4.3, 6.3			4.7.3, 5.6.3, 5.6.11, 6.1	DS7.1, PC5, PO7.4, DS7.2
		12.6, 12.6.1, 12.9.4	3.5e, 4.3, 6.3			4.7.3, 5.6.3, 5.6.11, 6.1	PO7.4, DS7.2
	4.4	12.6, 12.6.1, 12.9.4	3.5e, 4.3, 6.3			4.7.3, 5.6.3, 5.6.11, 6.1	PO7.4, DS7.2
		12.6, 12.6.1, 12.9.4	3.5e, 4.3, 6.3			4.7.3, 5.6.3, 5.6.11, 6.1	DS7.1, DS7.2
		12.6, 12.6.1, 12.9.4	3.2a, 3.5e, 6.3			4.7.3, 5.6.3, 5.6.11, 6.1	PO7.4, DS7.2

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
141	5.1.1	AAM 50.150, AAM 100.060, AAM 38.335	9.1.3	PE-1	164.310(a)(2)(iii)	
141	5.1.2	AAM 38.335	9.1.1	PE-3	164.310(a)(1)	
141	5.1.3	AAM 50.150, AAM 38.335	9.1.5	PE-1	164.308(a)(3)	
141	5.1.4		9.1.6	PE-16		
141	5.1.6			MA-05		
141	5.1.7			MA-05		
142	5.1.1		9.2.1, 9.1.4	PE-1, PE-7	164.310(a)(1)	
142	5.1.2		9.2.3	PE-9		
142	5.1.3		9.2.4	PE-9		
142	5.2.1	AAM 50.150, AAM 38.335	9.1.2	PE-3	164.310(a)(1)	

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.1	9.1, 9.1.1, 9.1.2, 9.1.3	4.4.1			4.1, 4.2, 4.3.1, 4.3.3, 4.3.4, 4.3.9, 4.3.10, 4.3.11, 4.7.1	DS12.5, DS12.1
	4.1	9.1, 9.1.1, 9.1.2, 9.1.3, 9.2, 9.3, 9.3.1, 9.3.2, 9.3.3, 9.4	4.4.1			4.1, 4.3, 4.3.1, 4.3.3, 4.3.4, 4.3.12	DS12.2
	4.3	9.1, 9.1.1, 9.1.2, 9.1.3				4.1, 4.2, 4.3.1, 4.3.9, 4.7, 4.7.1,	DS12.5, DS12.1
						4.2	DS12.1
	4.10		3.4d			4.3.12	DS12.1, DS12.5,
			3.4d			5.6.9	DS12.1
			3.4d			5.6.9	DS12.1
	4.10	9.1, 9.1.1, 9.1.2, 9.1.3	4.4.1			4.1, 4.2, 4.3, 4.3, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.9, 4.3.10, 4.3.11	DS12.2, DS12.2

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
142	5.2.2	AAM 200.040, AAM 38.335	11.2.2	AC-2, AC-6	164.308(a)(4)(ii)(B), 164.312(a)(1)	
143	5.1.1	AAM 38.335	9.2.6	MP-6, MP-7		
143	5.1.2	AAM 38.335	9.2.6	MP-7		
143	5.1.3			MA-02		
143	5.1.4	AAM 50.140, AAM 100.060	10.7.2	MP-6, MP-7	164.310(d)(2)(i)	
143	5.1.5	AAM 50.140, AAM 100.060	10.7.2	MP-7	164.310(d)(2)(i)	
143	5.2.1	AAM 100.060	10.7.2, 9.2.7		164.310(d)(1)	
143	5.2.2	AAM 50.140, AAM 100.060, AAM 38.335	10.7.2	MP-7	164.310(d)(1), 164.310(d)(2)(ii)	

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		2.1, 2.2.2, 2.2.4, 2.3, 7.1, 7.2	3.4a			5.6.1, 5.6.7	DS5.2
		9.1, 9.10.1, 9.10.2	3.4d, 4.6, 4.7, 7.9	45.48.500, 45.48.540		8.4	DS11.4,
		9.1, 9.10.1, 9.10.2	3.4d, 4.6, 4.7, 7.9			8.4	DS11.4,
	4.13		4.6	45.48.500, 45.48.510, 45.48.530		3.2, 5.6.10, 5.6.15, 6.3.4, 8..3	DS11.18
			4.6	45.48.500, 45.48.510, 45.48.530		3.2, 5.6.10, 5.6.15, 6.3.4, 8..3	DS11.18
	4.13		3.4d, 4.6	45.48.500, 45.48.510, 45.48.530		3.2, 5.6.10, 5.6.15, 6.3.4, 8..3	DS11.18
	4.13	9.1, 9.10.1, 9.10.2	4.6	45.48.500, 45.48.510, 45.48.530		3.2, 5.6.10, 5.6.15, 6.3.4, 8..3	DS11.18

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
143	5.2.3	AAM 100.060, AAM 38.335	10.7.2, 10.7.1	MP-7	164.310(d)(1), 164.310(d)(2)(ii)	
144	5.1.1	AAM 38.335	11.2.1	AC-4	164.308(a)(4)	
144	5.1.2		10.7.1	MP-1		
144	5.1.3		10.7.1, 11.7.1, 12.3.1	MP-1		
144	5.1.4		9.2.6	MP-1, MP-6		
144	5.1.5	AAM 100.060	10.8.3	SC-9	164.310(d)(2)(iii)	
151	5.1.1		13.2.1			
151	5.2.1		14.1.5	AT-3	164.308(a)(5)(iii)	
151	5.2.2	AAM 38.335	13.1.1	IR-1	164.308(a)(6)	13402(a, b, c, d)

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.13	9.1, 9.5, 9.7, 9.7.1, 9.7.2, 9.8, 9.9, 9.9.1, 9.10.1, 9.10.2	4.6	45.48.500, 45.48.510, 45.48.530		3.2, 4.6, 5.6.10, 5.6.15, 6.3.4, 8..3	DS11.18
	4.4	2.1, 7.1, 7.2, 8.1, 8.2, 8.3, 12.3.1, 12.5.4	7.13.1			5.6.1, 5.6.7	DS5.10
						3.2, 4.6, 5.6.10, 5.6.15	
			4.4.2, 7.12			3.2, 4.6, 4.7,4.7.1, 4.7.2, 5.6.4, 5.6.10, 5.6.15, 6.15	DS11.27
			3.4d, 4.6, 4.7, 7.9			8.4	DS11.4, DS11.6
	4.13	9.7, 9.7.1, 9.7.2				4.4, 4.5	DS11.22
			3.3d, 5.5			5.6.8	
	4.5					5.6.6	PO7.3, PO7.4
	4.6	12.9	3.4e, 3.5c, 5.2.2, 5.4, 5.5	45.48.010, 45.48.040, 45.48.180		5.6.8	PO9.5, PO9.6, DS8.2, DS5.6, PC-5

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
151	5.2.3	AAM 38.335	13.1.2	IR-5		
151	5.3.1		13.2.3	IR-1		
151	5.3.2		13.2.1	IR-1		13402(i)(2)
151	5.3.3	AAM 38.335	13.2.1	IR-1		13402(f)
151	5.4.1		13.2.3	IR-1	164.308(a)(6)(ii)	
151	5.4.1	AAM 38.335	13.2.1	IR-1	164.308(a)(6)(ii)	
151	5.4.3	AAM 38.335	13.2.3	IR-1		
151	5.4.4	AAM 38.335	13.2.3	IR-4		
151	5.4.5	AAM 38.335	13.2.3	IR-4		
151	5.4.6	AAM 38.335	13.2.2	IR-7	164.308(a)(6)(iii)	13402(f)
151	5.5.1	AAM 38.335	13.2.3	IR-4		
151	5.5.2	AAM 38.335	13.2.3	IR-4, IR-6		
151	5.6.1	AAM 38.335	13.2.3	IR-5	164.308(a)(5)(ii)	

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		12.9	3.3d, 5.2, 3.5d, 5.4, 5.5			5.6.8, 5.6.16	DS8.2, DS8.4
			5.5				DS5, DS10.1, DS5.11
			3.3d, 5.5			5.6.8	DS8.2, DS5.6, , DS5.11
		12.5.3, 12.9.1	3.3d, 5.5	45.48.040		5.6.8	PO9.5, PO9.6, DS8.2, DS5.6, PC-5
	4.6		5.5				DS8.2, DS5.6, PC5, DS5.11
	4.6	12.5.3, 12.9.1	3.3d, 5.5			5.6.8	PO9.5, PO9.6, DS8.2, DS5.6, PC-5
		12.9.1	5.5	45.48.040			DS8.2, DS5.6,DS5.11, DS10.1
		12.9.1	5.5				DS5.11
		12.9.1	5.5				DS8.2, PO9.5, PO9.6
	4.6	12.5.2, 12.9.1, 12.9.6	5.5	45.48.200		5.6.8	DS8.1
		12.9.1	5.5				DS8.2, PO9.5, PO9.6
		12.9.1	5.5				DS8.2, PO9.5, PO9.6
	4.5	12.9.1	5.5				DS8.2, DS8.4

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
151	5.6.2	AAM 38.335	13.2.2	IR-4, IR-6	164.308(a)(6)(ii)	13402(f)
152	5.1.1	AAM 38.335	13.2.2	IR-1	164.308(a)(6) (iii)	13402
161	5.1.1	AAM 38. 335	10.4.1	SI-3	164.308(a)(5)(ii)B	
161	5.1.2	AAM 38. 335	10.4.1	IR-1		
161	5.1.3		12.4.1	CM-1		
161	5.1.4	AAM 38. 335	10.4.1	SI-4		
161	5.1.5	AAM 38. 335	10.4.2	SC-18	164.308(a)(5)(ii)(B)	
162	5.1.1		10.3.1	SA-2		
162	5.1.2	AAM 230.190	10.3.2	SA-4		
162	5.1.3	AAM 230.190	10.3.2	CA-6		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.6	12.5.2, 12.9.1, 12.9.6	5.5			5.6.8	DS8.2, DS5.11
	4.6	12.9.1	5.5	45.48.010		5.6.8	PO9.5, PO9.6, DS8.2, DS5.6, PC-5
	4.5	5.1, 5.1.1, 5.2, 6.2, 6.6	7.8, 7.15			5.6.16	DS5
		5.1, 5.1.1, 5.2, 6.2, 6.6	7.8, 7.15			5.6.16	DS5
							AI3.6
		5.1, 5.1.1, 5.2, 6.2, 6.6	7.8, 7.15			5.6.16	DS5.10
	4.5	5.1, 5.1.1, 5.2				5.6.15	DS5
							DS3.2
						5.6.5	PO3
						5.6.5	PO3

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
162	5.2.1	AAM 38. 335	10.3.2			
162	5.2.2	AAM 230.190	12.5.2	SA-11		
162	5.3.1		8.2.2	AT-3		
162	5.4.1		10.7.4	MP-4		
162	5.5.1	AAM 38.335	10.1.1		164.308(a)(7)(ii)(E)	
162	5.5.2					
163	5.1.1		7.1.3			
163	5.2.1	AAM 38.335	11.4.3	AC-13		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		2.2, 6.3.1, 6.3.7, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10, 12.3.7				5.6.5	PO3
						5.6.14	AI7.2, AI7.4
			3.5e, 4.3			4.7.3, 5.6.3, 5.6.11, 6.1	PO7.4, DS7.2
			7.1			5.6.10	PO6.3, PO6.4, PO6.5
	4.7	12.2, 1.1.5	7.1				DS5.17
							DS5.1
						2.2	PO6.3,PO6.4, PO6.5
		1.1.6, 1.1.7	3.4b, 7.2.3, 7.7, 7.13.1			5.6.1	DS5.1

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
163	5.2.2					
163	5.2.3					
163	5.2.4		6.2.3			
163	5.3.1	AAM 38.335	10.8.1	AC-4, AC-20, PS-6		
163	5.4.1		10.8.4	AC-8		
163	5.4.2	AAM 38. 335	10.2.2	SA-9	164.314(b)(2)(iii)	13401(a)
163	5.5.1	AAM 38. 335	10.4.1	SI-3	164.308(a)(5)(ii)(B)	
163	5.5.2		10.10.2			
164	5.1.1	AAM 38. 335	10.10.1	AU-2, AU-3, AU-4, AU-11	164.308(a)(1)(ii)(D), 164.312(b)	

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
							DS5.3
			6.3, 6.7			3.3, 5.3, 5.5.2, 5.5.3	
			3.1b, 6.2, 6.3, 7.9, 8.5			5.4, 5.6.15, 5.6.16	PO6.3, PO6.4, PO6.5
						4.4, 4.5	
	4.2	12.8.4	6.3				DS2.7
	4.5	5.1, 5.1.1, 5.2, 6.2, 6.6	7.8, 7.15			5.6.16	DS5.10
			7.8, 7.14			3.2, 5.6.2	M2.1
	4.1, 4.15	10.1, 10.2, 10.2.3, 10.2.4, 10.2.7, 10.3, 10.3.4, 10.3.5, 10.3.6	6.3, 7.8, 7.14, 8.4				M2.1

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
164	5.1.5	AAM 38. 335	10.10.4	AU-1	164.308(a)(1)	
164	5.2.1	AAM 38. 335	10.10.3	AU-9		
164	5.3.1	AAM 38. 335	10.10.2	AU-6	164.308(a)(1)	
164	5.4.1	AAM 38. 335	10.10.6	AU-8		
165	5.1.1	AAM 38. 335	10.1.1	SA-5	164.308(a)(1)	

SOA I

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.1	10.2, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 12.5.5	6.3, 7.8			5.6.2	DS5.7
		10.5, 10.5.1, 10.5.2, 10.5.3, 10.5.4, 10.5.5	6.3, 7.8, 7.14, 8.4			3.2, 5.6.2	DS5.7
	4.1	10.6, 11.4, 11.5, 12.5.5, 12.9.5	6.3, 7.8, 7.14			3.2, 5.6.2	DS5.5
		10.4				5.6.2	
	4.1	1.3.6, 12.2, 12.5.1	7.1				DS5.7

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
165	5.1.2	AAM 38. 335	10.1.2	CM-1		
165	5.1.3	AAM 50.080, AAM 50.170, AAM 38.335	10.1.3	PS-1, PS-2, AC-5	164.308(a)(4)(ii)	
165	5.1.4	AAM 38. 335	10.1.4	SC-2, SC-3, CM-2	164.314(b)(2)(ii)	
165	5.1.5		9.2.2	PE-9		
165	5.1.6	AAM 38.335	9.2.5	PE-17		
165	5.1.7	AAM 230.190	10.8.5	SC-7	164.310(d)(2)(iii)	
165	5.2.1	AAM 38. 335	10.5.1	CP-4, CP-5, CP-9	164.308(a)(7)(ii)(B), 164.310(d)(2)(iv)	
165	5.3.1	AAM 38.335	10.9.1	AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14		
165	5.3.2	AAM 38.225	10.9.2	SC-3, SC-7, SC-8, SC-9, SC-14		
165	5.3.3		10.9.3	SC-14		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		1.1.1, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4				5.6.5	AI3.6
	4.4	6.3.3					PO4.11
	4.2	6.3.2					AI5.7
			3.4d				DS12.4
		9.9, 9.9.1	3.4d, 7.8			5.6.9	
			3.1b			4.4, 4.5	ME3.1
	4.7,4.13	9.5	7.1			5.6.6	DS11.5, DS4.9, DS11.3, DS11.2
		ALL PCI DSS		45.48.750			ME3.1
		3.2, 3.3, 3.4, 4.1, 4.2	7.1	45.48.750			ME3.1
							ME3.1

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
171	5.1.1	AAM 38.335	11.4.1	AC-1	164.308(a)(4)(ii)(B)	
171	5.1.1		11.2.1	IA-4	164.312(a)(2)(i)	
171	5.1.2	AAM 200.040, AAM 38.335	11.2.2	AC-1		
171	5.2.1	AAM 90.020	11.1.1	AC-1	164.308(a)(5)(ii)(C)	
171	5.2.2	AAM 91.030	11.5.1	IA-1		
171	5.2.3		10.10.5	AU-2	164.308(a)(5)(ii)(C)	
171	5.4.1	AAM 200.040	11.2.1, 11.2.2	IA-1		
171	5.4.2	AAM 38.335	8.3.3	PS-5		
171	5.4.3	AAM 38.335	8.3.3	PS-5		
171	5.4.4		11.2.1	IA-1		5.5.2
171	5.4.5	AAM 200.040	11.2.2	AC-1		
171	5.5.2		6.2.3	PS-7	164.308(b)(1)	
172	5.1.1		11.1.1, 7.1.3	PL-4		
Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.1, 4.3, 4.4	1.1, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.4, 1.4.1, 1.4.2	7.13.1			5.6.1	DS5.2
	4.14		3.4a, 7.13.1			5.6.1, 5.6.7	DS5.3, DS5.4
		10.2.5	3.4a			5.6.1, 5.6.7	DS5.3
	4.1		3.2d, 7.3.2.1, 8.2			2.1	DS5.2
			7.7			4.7.2, 5.6.1, 5.6.7	DS5.1
	4.1		6.3, 7.8, 7.14			5.6.2	DS5.7
			3.4a, 7.13.1			5.6.1, 5.6.7	DS5.2
		8.5.4					PO7.8
		8.5.4					PO7.8
			7.13.1			5.6.1, 5.6.7	DS5.3,
			3.4a			5.6.1, 5.6.7	DS5.2
	4.9		6.3, 6.7			3.3, 5.3, 5.5.2, 5.5.3	DS2
			7.2.4a, 7.3.2.1, 7.7, 8.2			2.1, 2.2	DS5.2
	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)

Internal

172	5.1.10	AAM 38.335	11.4.1	AC-1		
172	5.1.6	AAM 10.100, AAM 15.060, AAM 38.225, AAM 90.020	11.5.2	IA-2, IA-4		
172	5.1.7			IA-2, IA-4		
173	5.1.1	AAM 38. 335	10.6.1	SC-9	164.312(a)(1)(i)	
173	5.1.2	AAM 230.100	12.5.1	SC-1		
173	5.1.3		7.1.3	SC-1		
173	5.1.4		10.6.2			
173	5.1.5		11.4.2	IA-1		

SOA I

		1.1, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.4, 1.4.1, 1.4.2	7.13.1			5.6.1	DS5.5
			6.1, 7.2.3, 7.2.4a, 7.2.4b, 7.3.1, 7.7		99.31(c)	4.7.2, 5.6.1, 5.6.7	DS5.2
							DS5.3
	4.14	1.4	7.9, 7.13.1			5.6.5, 5.6.15, 5.6.16, 5.6.17.1	DS11.27
						2.2	PO6.3,PO6.4, PO6.5
			3.1b, 6.3			5.6.5, 5.6.15	
			3.4b, 6.1, 7.2.3, 7.2.4a, 7.2.4b, 7.31, 7.7, 7.9, 7.11.4			5.6.5, 5.6.15	DS5.3

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
173	5.2.1	AAM 38.335	11.4.6	AC-4		
173	5.2.2		7.1.3			
173	5.2.3	AAM 38.335	11.7.1	AC-19		
173	5.3.1		15.2.1	CA-2		
173	5.3.2	AAM 38.335	15.2.2	CA-2		
173	5.4.1		11.4.6	SC-7		

SOA In

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		1.1.1, 1.1.2, 1.1.3, 1.1.5, 1.1.6, 1.1.7, 1.2, 1.3.8, 1.4, 1.4.1, 1.4.2, 1.5	3.4b, 7.7, 7.13.1			5.6.1	DS5.20
						2.2	PO6.3,PO6.4, PO6.5
		1.3.8, 1.3.9, 2.1.1, 4.1.1	4.4.2			4.7, 5.6.4	PO6
			3.2b, 3.3.c, 3.4e, 9.1, 9.2			2.5, 4.7.3, 6.3.5	M2.4
		11.1	3.3b, 3.5b, 6.2, 9.3			3.2, 5.6.4, 5.6.16, 6.3.5	M3.1
			3.4b, 7.7, 7.13.1			5.6.1	DS5.10

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
173	5.4.3	AAM 38.335	11.4.7	AC-4		
173	5.4.4	AAM 38.335	11.4.5	AC-3, SC-3		
173	5.4.5	AAM 38.335	11.4.5	SC-3		
173	5.4.6	AAM 38.335	10.6.1	AC-18		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		1.1.2, 1.1.8, 1.1.9, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 1.4, 1.4.1, 1.4.2	7.13.1			5.6.1	DS5.16
		1.1.3, 1.3, 1.4.1, 1.4.2	3.4b, 7.13			5.6.1	DS5.10, DS5.20
		1.1.3, 1.3, 1.3.1, 1.3.2	3.4b, 7.13.1			5.6.1	DS5.7, DS5.1
		1.3.8	7.9, 7.13.1			5.6.5, 5.6.15, 5.6.16, 5.6.17.1	DS11.27

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
173	5.4.7	AAM 38.225, AAM 38.335	11.4.2	IA-2, IA-4	164.308(a)(4)(iiii)	
173	5.4.8		11.4.4	MA-1		
173	5.4.9	AAM 38.335	11.5.6	SC-10	164.312(a)(1)(viii)	
173	5.5.1		10.6.1	SC-7		
173	5.5.2	AAM 38.335	11.4.6	AC-4		
173	5.5.3		11.4.6	SC-7		
173	5.5.4		11.4.2	SC-7		
173	5.5.5		11.4.1	AC-17		
174	5.2	AAM 10.100, AAM 15.060, AAM 38.225, AAM 90.020, AAM 91.030, AAM 38.335	11.1.1, 11.5.2	AC-1	164.308(a)(4)(ii)(C), 164.312(d)	

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.4	1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7, 12.3.2	3.4b, 6.1, 7.2.3, 7.2.4a, 7.2.4b, 7.31, 7.7, 7.9, 7.11.4			5.6.1, 5.6.15	DS5.3
			3.4b, 7.13.1			5.6.1	DS5.2
	4.14	12.3.9				5.6.1, 5.6.15	
			7.9, 7.13.1			5.6.5, 5.6.15, 5.6.16, 5.6.17.1	DS5.10
		1.1, 1.1.1	3.4b, 7.7, 7.13.1			5.6.1	DS5.20
						5.6.1	DS5.10
			3.4b, 6.1, 7.2.3, 7.2.4a, 7.2.4b, 7.31, 7.7, 7.9, 7.11.4			5.6.1, 5.6.15	DS5.3
			7.13.1			5.6.1	DS5.2
	4.4	10.3.1, 10.3.2, 10.3.3, 10.3.4	3.2d, 3.4a, 6.1, 7.2.3, 7.2.4a, 7.3.2.1, 7.2.4b, 7.3.1, 7.7, 8.2	45.48.170	99.31(c)	2.1, 4.7.2, 5.6.1, 5.6.7	DS5.2

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
174	5.1.1	AAM 38.335	10.1.1	CM-2, CM-3	164.310(b)	
174	5.1.2	AAM 38.335	10.1.1	CM-2	164.310(a)(2)(iv)	
174	5.1.3			CM-2	164.308(a)(8)	
174	5.2.1	AAM 91.030, AAM 38.335	11.5.1	IA-1		
174	5.3.1	AAM 38.335	11.5.4	MA-3		
174	5.4.1	AAM 38.335	11.5.5	AC-12	164.312(a)(2)(iii)	
175	5.1.1	AAM 38.335	11.7.1	AC-19, AC-20		
175	5.1.2	AAM 38.335	11.7.1	AC-19	164.312(a)(2)(iv)	
175	5.1.3	AAM 38.335	11.7.1	AC-19, AC-20	164.310(b)(iii)	
175	5.1.4	AAM 38.335	11.7.1	AC-19		
175	5.2.1	AAM 38.335	11.7.2	AC-17		
Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
175	5.2.2	AAM 38.335	11.7.2	AC-17		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.11	1.1.9, 1.2	7.1				DS9.7
	4.1	1.1.9, 1.2	7.1				DS9
	4.8						DS9
		8.5.16	7.7			4.7.2, 5.6.1, 5.6.7	DS5.4
		2.2.2, 2.2.4				5.6.1	DS5
	4.14	8.5.15, 12.3.8	7.8			5.6.1, 5.6.15	
		1.3.8, 1.3.9, 2.1.1, 4.1.1	4.4.2			4.7, 5.6.4	PO6
	4.14	1.3.8, 1.3.9, 2.1.1, 4.1.1				4.7, 5.6.4	PO2.1
	4.11	1.3.8, 1.3.9, 2.1.1, 4.1.1				4.7, 5.6.4	DS5.2
		1.3.8, 1.3.9, 2.1.1, 4.1.1				4.7, 5.6.4	DS5.1
		1.3.8, 1.3.9, 2.1.1				4.7, 5.6.4	
	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		1.3.8, 1.3.9, 2.1.1				4.7, 5.6.4	

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
175	5.2.3	AAM 38.335	11.7.2	AC-17, AC-19, AC-20		
175	5.2.4	AAM 38.335	11.7.2	AC-19		
175	5.3.1	AAM 38.335	11.7.2	CM-2	164.308(a)(5)(ii)(B)	
175	5.3.2		11.7.2	AC-17		
176	5.1.1	AAM 230.190	12.5.2	CA-2	164.312(b)	
176	5.1.2	AAM 230.190	12.5.2	CA-2		
176	5.2.1	AAM 230.190	12.5.2		164.314(b)(2)(i)	
177	5.31		11.4.2	AC-18		
177	5.1.1		11.4.1	AC-18	164.308(a)(4)	
177	5.1.2		10.6.1, 12.3.1	AC-18	164.312(e)(1)	
177	5.1.3		11.4.1			
177	5.2.1		11.4.1	AC-18		
177	5.2.2		11.4.1	AC-18		
177	5.3.2		11.4.3	AC-18		
177	5.3.3	AAM 38.335	11.4.3	IA-3		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		1.3.8, 1.3.9, 2.1.1				4.7, 5.6.4	DS11
		1.3.8, 1.3.9, 2.1.1				4.7, 5.6.4	DS11
	4.5	1.3.9				4.7, 5.6.4	DS11
						4.7, 5.6.4	DS5.3
	4.15					5.6.14	DS5.1
						5.6.14	AI7.7
	4.2					5.6.14	DS5.1
			3.4b, 6.2, 7.2.3, 7.2.4a, 7.2.4b, 7.31, 7.7, 7.9, 7.11.4			5.6.1, 5.6.15	DS5.3
	4.4		7.13.1			5.6.1	
	4.18		4.4.2, 7.9, 7.12, 7.13.1			4.7.1, 4.7.2, 5.6.5, 5.6.15, 5.6.16, 5.6.17.1, 6.15	DS11.27
			7.13.1			5.6.1	
			7.13.1			5.6.1	
			7.13.1			5.6.1	
			3.4b, 7.7, 7.13.1			5.6.1	
		1.1.5	3.4b, 7.7, 7.13.1			5.6.1	

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
177	5.3.5		9.1.6, 10.6.1	AC-18		
177	5.4.1	AAM 38.335	11.4.6	AC-4		
177	5.4.1		10.6.1	AC-18		
177	5.4.2		11.4.1	AC-18		
178	5.1.1	AAM 10.100	11.2.3	IA-2	164.308(a)(5)(ii)(D)	
178	5.1.2	AAM 10.100, AAM 15.060, AAM 100.060, AAM 200.040	11.2.3, 11.3.1	IA-2		
178	5.1.3	AAM10.100, AAM15.060, AAM 100.060, AAM 200.040	11.2.3, 11.3.1	IA-2		
178	5.2.1	AAM 10.100	11.2.3		164.308(a)(5)(ii)(D)	
178	5.2.2	AAM 10.100, AAM 15.060, AAM 100.060, AAM 200.040	11.3.1	IA-2	164.308(a)(5)(ii)(D)	
178	5.2.2	AAM 10.100	11.2.3	IA-2	164.308(a)(5)(ii)(D)	
178	5.2.4	AAM 10.100	11.2.3	IR-6		
178	5.3.1	AAM10.100	11.2.3, 11.5.3	IA-5		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
			7.9, 7.13.1			4.2, 5.6.5, 5.6.15, 5.6.16, 5.6.17.1	
		1.3.4	3.4b, 7.7, 7.13.1			5.6.1	DS5.10
			7.9, 7.13.1			5.6.5, 5.6.15, 5.6.16, 5.6.17.1	DS5.3
			7.13.1			5.6.1	
	4.5					5.6.1, 5.6.7	DS5.3
			7.2.4b, 7.3.3			4.7.2, 5.6.1, 5.6.7	DS5.3
			7.2.4b, 7.3.3			4.7.2, 5.6.1, 5.6.7	DS5.3
	4.5					5.6.1, 5.6.7	DS5.3
	4.5		7.2.4b, 7.3.3			4.7.2	DS5.4, DS5.5
	4.5					5.6.1, 5.6.7	DS5.3
						5.6.1, 5.6.7	DS10.1
			7.2.4b			5.6.1, 5.6.7, 4.7.2	DS5.3, DS5.4

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
178	5.3.2	AAM 10.100, AAM 38.335	11.2.3	IA-5		
178	5.3.3	AAM 10.100, AAM 38.335	11.2.3	IA-3		
178	5.3.4	AAM 10.100, AAM 38.335	11.2.3	IA-1		
178	5.3.5	AAM10.100	11.2.3	IA-2		
178	5.3.6	AAM10.100	11.2.3	SA-1		
178	5.3.7	AAM 38.335	11.2.4	AC-13	164.312(a)(1)(vii)	
179	5.1.2		10.10.2	SI-4		
179	5.1.7		15.2.1	AC-1		
179	5.2.1		11.4.1	AC-3		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		2.1, 7.1, 7.2, 8.1, 8.2, 8.3, 8.4, 8.5.1, 8.5.2, 8.5.3				5.6.1, 5.6.7	DS5.3
		2.1, 7.1, 7.2, 8.1, 8.2, 8.3, 8.4, 8.5.1, 8.5.2, 8.5.3				5.6.1, 5.6.7	DS5.3
		2.1, 7.1, 7.2, 8.1, 8.2, 8.3, 8.4, 8.5.1, 8.5.2, 8.5.3				5.6.1, 5.6.7	DS5.3,
						5.6.1, 5.6.7	DS5.2
						5.6.1, 5.6.7	DS5.2
	4.14	2.1, 7.1, 7.2, 8.5.5, 12.3.3	3.4a, 7.13.1			5.6.1, 5.6.7	DS5.4
		10.10.4				3.2, 5.6.2	DS5.5, DS5.10
		12.1.1					DS5.10
		12.3.6, 12.3.5, 12.3.7				5.6.1	DS5.10

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
191	5.1.1	AAM10.030, AAM 230.100, AAM 38.335	12.2.2	SA-8		
191	5.1.2	AAM 38.335	12.5.1	SA-10		
191	5.1.3			PL-2		
191	5.1.4	AAM10.030, AAM 230.100, AAM 38.335	12.5.1	CM-1, SA-5		
191	5.1.5		11.6.2	SC-2, SC-3, SC-7	164.314(b)(2)(ii)	
191	5.2.1	AAM 38.335	12.2.2, 12.2.3, 12.2.4	SA-13		
191	5.2.2	AAM 38.160	12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.5.4	SI-6, SI-7, SI-8, SI-10		
191	5.2.2	AAM 38.335	12.1.1	SA-13		
191	5.2.3	AAM 230.190	12.5.1, 12.5.2	CM-3		
191	5.2.3	AAM 38.160	12.2.2	SA-1		
191	5.2.4	AAM 38.335	12.4.3	SA-14		
191	5.2.5		12.5.5	SA-1, SA-9, SA-13		

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4					AI2.4
		12.9.1				5.6.14	AI3.6
		1.1.2					DS11, PO11.11
	4.15					5.6.1, 5.6.15	AI5.11
		6.3, 6.3.1, 6.3.1.2	5.6			5.6.6	
						5.6.17, 5.6.14	DS5.1
		6.3.1	5.6			5.6.6	
						5.6.14	
		6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4					AI6.1, AI7.3
		6.3	5.6			5.6.6	AI3.6
			5.6			5.6.6	AI6.1, DS2.3, DS2.7, DS5.4

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
191	5.3.1	AAM 38.160	12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.5.4	SA-8, , SA-13, SI-4, SI-7		
191	5.4.1	AAM 38.160	12.2.2	SA-8		
191	5.4.2	AAM 38.335	12.1.1, 12.4.2, 12.5.1	SA-10		
192	5.1.1		12.3.1		164.312(a)(1)(viii)	4.14
192	5.1.2		12.3.1	SC-8, SC-9	164.312(a)(1)(viii)	164.312(a)(1)(viii)

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4				5.6.17, 5.6.14	DS5.5, DS5.10, PO2.4, DS5.9, PO2.4, AI2.4
		6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4					AI2.4
		6.3, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10, 12.3.7	3.1d			5.6.13	AI3
			4.4.2, 7.12			4.7.1, 4.7.2, .6.15	DS5.3
			4.4.2, 7.12			4.7.1, 4.7.2, .6.15	DS5.11

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
192	5.1.3	AAM 38.335	12.3.1	MP-4	164.312(a)(1)(viii)	4.14
192	5.2.2		12.3.1	PM-11		
192	5.2.3	AAM 38.335	12.3.2	SC-12		

SOA In

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		2.3, 3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 4.1, 4.2	4.4.2, 7.12			4.7.1, 4.7.2, .6.15	DS5.18
			4.4.2, 7.12			4.7.1, 4.7.2, .6.15	
		3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 4.1, 4.2	4.4.2,7.3, 7.9, 7.12			4.7.2, 5.6.15	DS5.18

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
192	5.2.4	AAM 38.335	12.3.2	SC-12		
192	5.3.1		12.3.2	SC-13		
192	5.3.2		12.3.2	SC-13		
193	5.1.1		12.6.1	RA-5	164.310(a)(1)(i)	
193	5.1.2		6.1.8	CA-2	164.314(a), 164.314(a)(2)(i)	
193	5.1.3		12.6.1	RA-5		
193	5.2.1		12.6.1	CM-5		
193	5.2.2		12.5.1	CM-9		

SOA In

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		2.3, 3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 4.1, 4.2	4.4.2, 7.3, 7.9, 7.12			4.7.2, 5.6.15	DS5.18
			4.4.2, 7.3, 7.9, 7.12			4.7.2, 5.6.15	DS5.18
			4.4.2, 7.3, 7.12			4.7.2, 5.6.15	DS5.18
	4.1		3.3d, 3.5d, 5.5			5.6.13	M2.1
	4.19					2.5, 2.6, 2.7, 5.6.4	DS5.1
			3.3d, 3.5d, 5.5			5.6.13	M2.3
			7.8, 7.15			6.1, 6.2	AI2.12
						1.1.2, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4	AI3.6

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
193	5.2.3		12.5.1	RA-5		
193	5.2.5	AAM 38.335	10.5.1	CP-9	164.308(a)(7)(ii)(A)	
194	5.1.1	AAM 38.335	15.1.6			

SOA In

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
						1.1.2, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4	AI3.6
	4.7	12.9.1	5.6			5.6.6	DS11.5,
		3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 4.1	4.4.2, 7.2.3, 7.2.4a, 7.9, 7.11.4, 7.12			5.6.7	DS5.16

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
194	5.2.1	AAM 38.335	15.1.6	PL-4		
195	5.1.1	AAM 38.335	15.1.6, 15.2.2			
201	5.1.3	AAM 38.335	14.1.3	CP-2, MA-06		
201	5.2.2	AAM 38.335	14.1.3	CP-1	164.308(a)(7)(i)	
201	5.3.1			MA-06		
211	5.1.2		15.1.2	SA-6		
211	5.2.1		15.1.5	PL-4		
211	5.2.2		15.1.5	PL-4		
211	5.3.1		15.1.2	SA-6		

SOA In

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
		3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 4.1	4.4.2, 7.2.3, 7.2.4a, 7.9, 7.11.4, 7.12			5.6.7	DS5.8
		3.6	3.3b, 3.5b, 6.2			3.2, 5.6.4, 5.6.16, 6.3.5	DS5.16
		12.9.1	5.6			5.6.6	PO3.3
		12.9.1	5.6			5.6.6	PO3.3
							DS9.3
						5.6.16	AI1.14
						5.6.16	AI1.14
							ME3.2, PO6.9

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
212	5.1.1		15.3.1			
212	5.1.2		15.3.1			
212	5.1.3	AAM 38.335	15.2.2	CA-1		
212	5.1.4	AAM 38.335	15.1.3	AU-9	164.316(b)(2)(i)	
212	5.1.5	AAM 38.335	15.1.6			
212	5.2.1		15.3.2	AU-9		

SOA In

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
			3.5d, 6.3			5.6.13	M2.4
			3.5d, 6.3			5.6.13	M2.4
		11.1	3.3b, 3.5b, 6.2			3.2, 5.6.4, 5.6.16, 6.3.5	M2.3
	4.22	3.1, 10.7				3.1	DS11.3
		3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 4.1	4.4.2, 7.2.3, 7.2.4a, 7.9, 7.11.4, 7.12			5.67	DS5.8
			7.1			3.2, 5.6.1	M2.4

Internal

Policy	Clause	AAM	ISO-27001 Clause	NIST 800-53	HIPAA	HI-TECH
212	5.2.1		15.2.2	AU-6, AU-7, CA-7, SI-4	164.308(a)(1)(ii)(D	
212	5.2.2		15.2.2, 15.3.1, 6.1.8	AU-2, AU-6		
213	5.1.1	AM 38.335	12.6.1	RA-3	164.308(a)(1)(ii)(A)	
213	5.1.2		15.2.1, 15.2.2	CA-2		
213	5.1.3		15.3.1	AU-1		
213	5.2.1		15.3.2	AU-9		
214	5.1.1		15.3.1			
214	5.1.1		15.3.1	AU-1		
215						

SOA Internal

	NIST 800-66	PCI DSS	CJIS	HB 65	FERPA	IRS PUB 1075	COBIT (SoX)
	4.1		3.3b, 3.5b, 6.2			3.2, 5.6.4, 5.6.16, 6.3.5	M2.3
			3.5d, 6.3, 7.14			2.5, 2.6, 2.7, 5.6.4, 5.6.13	M3.5
	4.10	11.1, 11.2, 11.3				5.6.13	PO9.3, PO9.4, AI1.1
						3.2, 5.6.4, 5.6.16, 6.3, 6.3.5	DS5.5
						5.6.13	
						3.2, 5.6.1	
			3.5d, 6.3			5.6.13	

Internal

Title:	Policy Development Reference Guide	Effective:	2/12/2025
		Last Review:	2/12/2025
		Review Frequency:	Tri-annually
Number:	ISP-005		
Version:	1.02	Approved by:	CIO
Pages	8	Distribution:	SOA

1. Purpose

The State of Alaska (SOA) has created a policy template that allows extensive customization for use throughout the SOA, including local governments, with minimal modification. This document describes the approach to customization and detailed instructions on modification of the policy documents for use within other areas of the SOA.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

This is the layout and directions to define and develop a policy. This subtopic "Definitions" must include the following statement: Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Customization Approach

The SOA policy template is designed to facilitate customization by other branches of government and the departments throughout the SOA; specifically, the policy template was created with the view in mind that departments may wish to make use of the policy template and adapt it to their own specific environment.

To accomplish this, the SOA Security Office (SSO) has created "Policy Templates" that allow rapid substitution of policy specifics with relatively minor effort. These templates provide a framework or container of "boilerplate" policy text, and a list of a number of customizable "variables" that can be set by agencies for customization.

SOA Internal

This document describes the process for modifying a policy template for customization by departments, as well as an index of customizable fields for each of the policy template documentations created by SOA.

6. Template Modification Method

The steps involved in the modification of a policy are as follows:

1. Copy the blank template in ISP-006 or an existing policy to modify as an additional policy for your department.
2. Name or re-name policy document(s) to establish or change policy name.
3. Determine applicable template variables.
4. Change template variables.
5. Update document references.
6. Perform manual editing steps.

The following subsections describe each of these steps in detail.

6.1. Step 1: Select Blank Template or Policy Document to Change

The first step in the policy modification or development process is to decide which policy needs to be established or requires modification. Typically, this will be all or a majority of the policy document. The organization should make a list of the documentation they wish to modify and obtain an electronic copy of the policy template or documents which they must subsequently modify.

6.2. Step 2: Determine Applicable Template Variables

Once a list of polices that need to be established or that require changes has been compiled, appropriate customizable variables within the template need to be determined. A full list of the customizable variables for each of the policy documents supplied is located below in "Appendix A: List of Policy Variables". The department should read and understand the policy template, review the variables that may be changed within that template, and understand what effect the template variables have on the text within the template, prior to making changes. Template variables can be set up to affect the entire document globally. Changes are made to global variables by selecting *properties* under the file tab menu in the open document and selecting the custom tab.

The following illustrates a customizable template variable prior to a change within the context of a policy document. In this example, the variable "Department" is populated, throughout the document with the value "State of Alaska" and the variable "Glossary Title" is populated throughout the document, with the value "Information Security Glossary."

SOA Internal

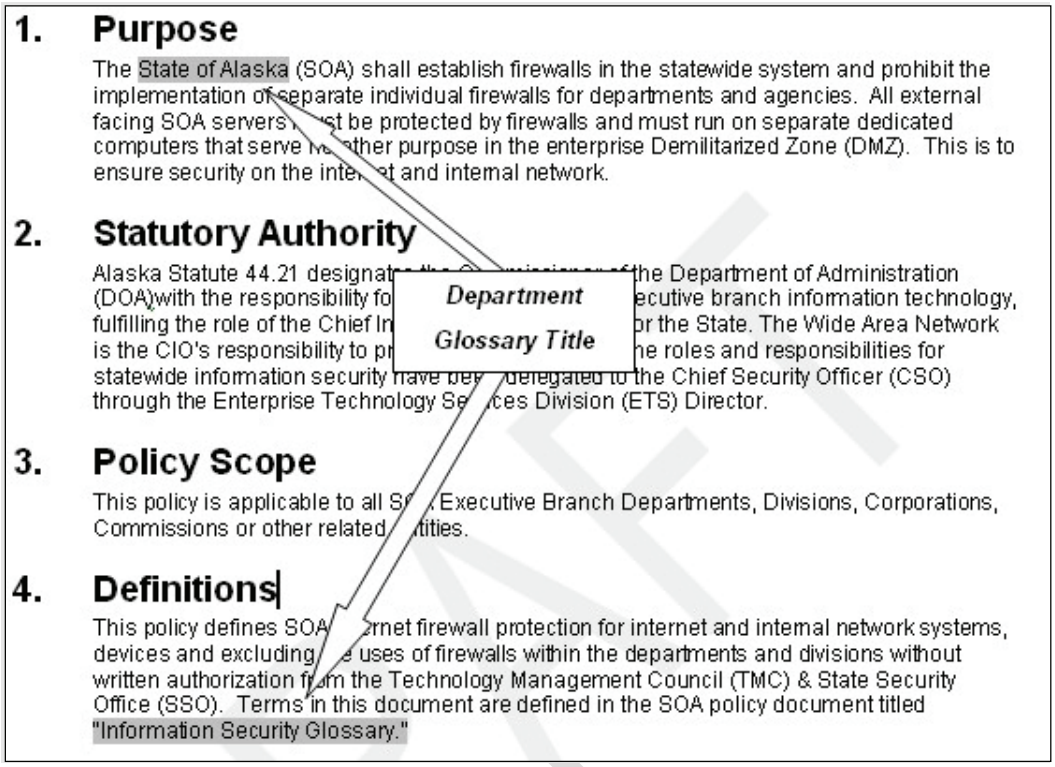

Figure 1 - Variable in the Context of a Policy Template

6.3. Step 3: Change Template Variables

Once the department has decided which variables it must change, it needs to create a modification to that variable and propagate that change throughout the document. The following are the steps to accomplish this.

6.3.1 Change the Variable Property Value

The customizable variables within the template are stored as properties associated with the template file and are located on the file tab menu. To change the variables, click on the file from the Microsoft Word™ document and select “Properties” from the drop-down list:

SOA Internal DRAFT

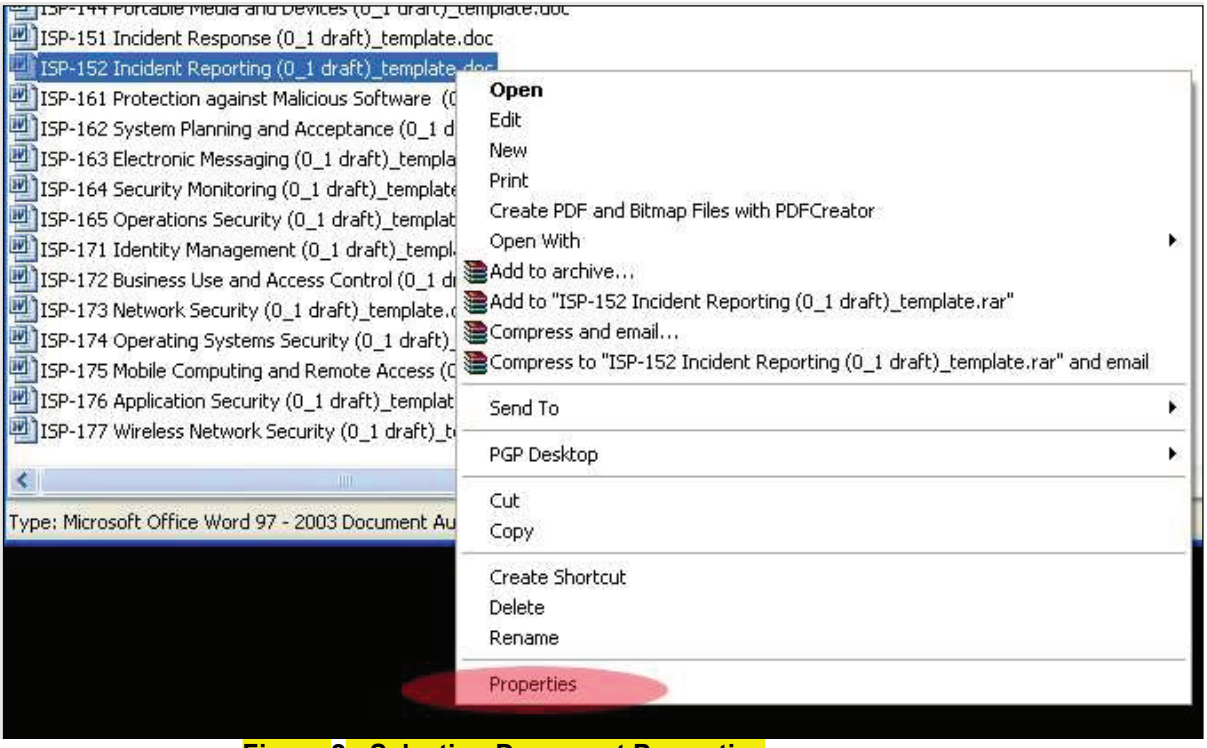

Figure 2 - Selecting Document Properties

SOA Internal

Within the document properties dialogue, select the “Custom” tab, and select the appropriate values from the list of custom properties associated with the document:

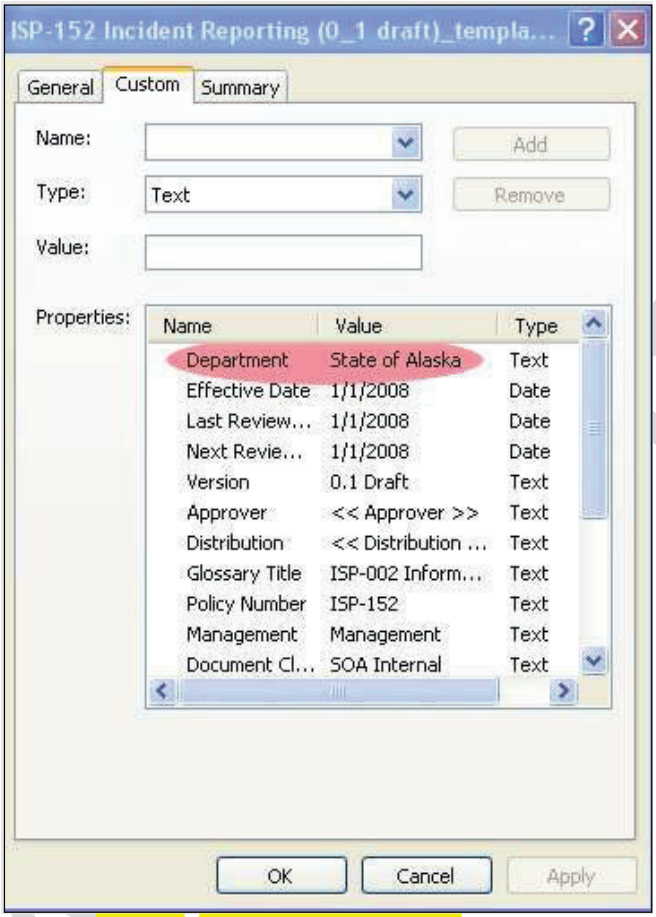

Figure 3 - Custom Properties

The appropriate value should be selected, and the new value entered into the “Value” edit box. Once the completions of the modifications are made, click the “modify” button to update the value.

SOA Internal

Figure 4 - Value Modification

Select "OK" to close the properties window once the changes are complete.

6.4. Step 4: Update Document References

Once the document properties are modified, check to be sure the changes are propagated throughout the text of the document.

To accomplish this, open the document using Microsoft Word™, right click one or more instances where the value appears, and select "Update Field" from the context menu. Note that more than one value can be altered at one time by highlighting multiple instances of the variable when "Update Field" is selected.

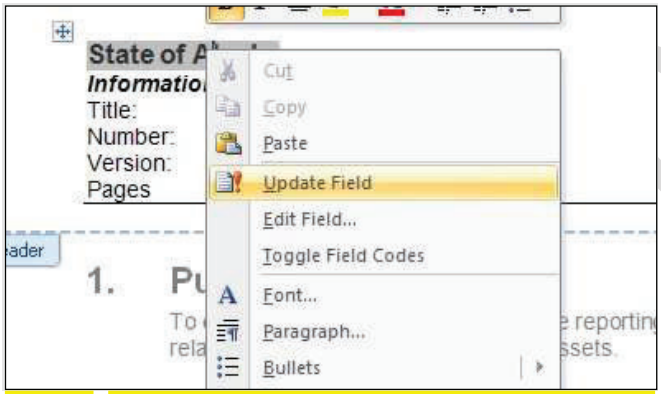

Figure 5 - Updating Values within Microsoft Word™

Once the values are updated, the text should reflect the modification:

1. Purpose

To ensure the effective and appropriate reporting of known or suspected security incidents related to Department of Agriculture information assets.

2. Definitions

Terms in this document are defined in the Department of Agriculture policy document entitled "ISP-002 Information Security Glossary."

3. Policy Statement

3.1. Incident Reporting

Figure 6 - Modified Policy Template

6.5. Step 5: Perform Manual Editing

The policy templates were designed to minimize manual editing. However, manual editing may be required to achieve the desired effect and to make the statement(s) appropriate for the department. It is important to re-read the policy text to determine if any manual modification of the policy is required prior to publication.

Appendix A: List of Policy Variables

The full list of variables within each of the templates included in the body of documentation is provided for reference:

Globally Used Variables

The following values are used in all policy documents:

- **Approver** – individual, office, or role of the party responsible for approving the policy.
- **Department** – department, organization, or entity issuing the policy statement(s).
- **Department Short Name** – a "nickname" or "short name" for the department, if applicable.
- **Distribution** – intended audience for the policy or a statement of the scope of distribution.
- **Document Classification** – classification level associated with policy documentation.
- **Effective Date** – date upon which the policy takes effect.
- **Executive Management** – designation of the employees responsible for management of the organization.
- **Glossary** – name of the document or source containing the definitions of the terms used within the policy.
- **Last Review** – date of last review by Executive Management.
- **Managing Authority** – "short name" (such as an acronym) of the personnel responsible for policy issuance and managerial authority.
- **Managing Authority Full Name** – "long name" of the personnel responsible for policy issuance and managerial authority.
- **Next Review** – date at which the policy is scheduled for review.
- **Policy Number** – numerical value associated with the policy document.
- **Version** – version number of the document.

Locally Used Variables

The following values are used in specific policy documents, but are not required for every policy document:

- **Advisory Authority** – personnel responsible for oversight of third-party services such as outsourcing, vendors, and third-parties.
- **Advisory Authority Short Name** – short name of the Advisory Authority, if applicable.
- **Compromise Report Personnel** – personnel responsible for receiving reports of potential compromise such as data compromise or compromise of an information asset.
- **Data Owner** – personnel responsible for data classification and data governance.
- **Incident Response Team Long Name** – long name of the incident response team convened to oversee security incidents.
- **Incident Response Team Short Name** – short name of the incident response team, if applicable.
- **Information Owners** – personnel responsible for management and governance of non-data information assets.
- **Monitoring Party** – personnel to whom the incident response team must report progress and status.
- **Network Maintainer** – personnel tasked with maintenance of the network.
- **Notification Party** – personnel to be notified in the event an incident is suspected.

SOA Internal

- **Notification Timeline** – maximum amount of time before notification of an incident to the appropriate personnel.
- **Patch Timeline** – maximum amount of time before issuance of security patches.
- **Report Form** – specific document used to file an incident report.
- **Requirement Authority** – personnel responsible for evaluating security requirements and approving those requirements.
- **Requirement Authority Short Name** – "short name" for the requirement authority if applicable.
- **Response Decision Timeline** – maximum amount of time before an incident response decision is issued**.**

SOA Internal

Title:	Policy Template	Effective:	7/1/2017
Number:	ISP-006	Last Review:	7/1/2017
Version:	1.01	Next Review:	Annually
Pages	2	Approved by:	CIO
		Distribution:	SOA

1. Purpose

The State of Alaska (SOA) shall prohibit… or The State of Alaska shall ensure… *these are the beginning of statements that will be used to create a policy statement to support a policy that is being developed. As a user, you would add the language here to develop the policy you want to create.*

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to all SOA branches, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary. *If necessary, ensure that any new language or definitions that are not in the glossary have been added before publication of this new policy.*

5. Policy Statement *This is the space where summarized subtopics will be listed, in bullet point format, any and all subtopics that support the main topic being developed; this is not limited to any particular number of bullets.*

This policy defines:

- Subtopic;
- Subtopic; and
- Final subtopic.

5.1. Policy Subtopic (from 1st single bullet point)

5.1.1 Details to Sub topic *(details that support the subtopic)*

Create a statement that has substantive information supporting the 1st specific subtopic (1st bullet point) to the main topic of the new policy being developed.

SOA Internal

5.2. Policy Subtopic *(from 2nd single bullet point)*

5.2.1 Details to Sub topic *(details that support the subtopic)*

Create a statement that has substantive information supporting the 2nd specific subtopic (2nd bullet point) to the main topic of the new policy being developed.

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Policy Approval and Review	Next Review:	Per policy
Number:	ISP-101		
Version:	1.04	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

This policy is to ensure that State of Alaska (SOA) information security policies are approved by Executive Management and periodically reviewed for accuracy, risk, and continued applicability. Policies must reflect statutory requirements and prevailing operational circumstances.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Policy approval; and
- Policy review.

5.1. Policy Approval

5.1.1 Security Policy Requirements

The State Security Office (SSO) must determine statewide security policy requirements consistent with the needs of the SOA and must communicate those requirements to the CIO.

Executive Management for each department must determine regulatory compliance requirements specific to the business and ensure inclusion of applicable information security requirements from those regulations in department security policy. Departmental information security policies may not conflict with SOA ISP's.

SOA Internal

5.1.2 Formal Policy Authorization

The SSO must prepare statewide information security policies and must submit such policies to the CIO for authorization.

The department Information Security Officers (ISO) must prepare department specific information security policies and must submit department specific policies to the SSO for review and approval prior to submission to the department's Executive Management for authorization..

5.1.3 Publication, Notification, and Awareness Training

Upon approval by the CIO, the SSO must publish the statewide information security policies and provide notification, education, and awareness training to the departments for application.

Upon approval by the department's Executive Management, the ISO must publish the department specific information security policies, notify the SSO, and provide department specific notification, education, and awareness training to department users for application.

Information security policies must be published in a known and advertised internal network location accessible by all personnel to whom the policies apply.

5.2. Policy Review

5.2.1 Review

The CIO and SSO must review approved policies at least every three years to ensure they remain consistent with the needs of the SOA and align with current regulatory, technological, operational, organizational, or environmental changes.

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Risk Management	Next Review:	Per policy
Number:	ISP-102		
Version:	1.2	Approved by:	CIO
Pages	4	Distribution:	SOA

1. Purpose

To define practices established to manage and identify mitigation strategies to address risks and threats to the confidentiality, integrity and availability of the State of Alaska (SOA) information system and information assets. To ensure the SOA is protected from those risks of significant likelihood and consequence in the pursuit of the SOA's stated strategic goals and objectives to be pro-active rather than re-active management as well as fulfillment of Legal and statutory requirements.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates the process for:

- Risk management;
- Risk response; and
- Risk evaluation.

5.1. Risk Management

5.1.1 Assessment Analysis

In collaboration with the State Security Office (SSO) and the Division of Risk Management (DRM), Business Owners must implement a formal risk assessment and management process. This risk management must identify and address potential threats that may expose

SOA Internal

the SOA network, resources, assets, information systems and information to unauthorized disclosure, service disruption, or any adverse condition.

Department Information Security Officers must ensure that risk assessment activities are performed annually and whenever significant changes are made to the administrative, technical or physical environment.

5.1.2 Vulnerability Identification

SSO personnel tasked with risk assessment management of the enterprise must identify potential vulnerabilities for the department during the risk assessment process. Vulnerability identification in support of risk assessment may include activities such as technical vulnerability assessment and scanning, review of the configuration of computer systems and network devices and evaluation of operating system or application patch levels and non-technical analysis.

5.1.3 Adverse Impact

The adverse impact of a security event can be described in terms of the loss or degradation of one or a combination of any of the following: confidentiality, integrity and availability to SOA networks, systems, services or information.

5.2. Risk Response

5.2.1 Risk Mitigation

Business Owners are accountable for documenting the risks identified in the course of risk assessments. Business Owners, with guidance of the SSO and DRM, are accountable for documenting and implementing a plan for risk treatment including specific mitigation measures for unacceptable risks.

5.3. Risk Evaluation

5.3.1 Periodic Review

The SSO and DRM must review the results of Department risk assessments determined by security testing and evaluation on a periodic basis, not less than annually, and must monitor the progress of risk treatment plans and take corrective actions as necessary.

5.3.2 Security Criteria

The SSO and DRM risk assessment personnel must determine whether the security requirements stipulated for the information, IT system and collected during evaluation, are being met by existing or planned security controls. Typically, information and system security requirements can be presented in table format, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy the security control requirements.

A security requirements check list contains the basic security standards that can be used to systematically evaluate and identify vulnerabilities of the assets (personnel, hardware, software, and information), non-automated procedures, processes and information transfers associated with a given IT system in the following security areas:

- Management
- Operational

SOA Internal

- Technical

SOA Internal

5.3.2.1 Security Criteria Table

This table defines the minimum assessment criteria in identifying an IT system's vulnerabilities in each security area.

Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigation • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan • Statute, regulatory, policy and industry standards compliance
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Information, media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office space, filing cabinets) • Humidity control • Temperature control • Workstations, laptops and stand-alone personal computers and work areas
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Access control (electronic and physical) • Identification and authentication • Threat detection • Object reuse • System and Application Hardening • Audit • Logging (operational, and technical) • Monitoring and reporting (operational and technical)

SOA Internal

		Effective:	5/16/2025
		Last Review:	5/16/2025
Title:	Managing Exceptions	Next Review:	Tri-annually
Number:	ISP-103		
Version:	1.04	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To establish a process to monitor and manage exceptions to State of Alaska (SOA) information security policies due to operational constraints, technical limitations, legal requirements or other case-by-case issues.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Exception requests;
- Exception evaluations; and
- Exception reviews.

5.1. Exception Requests

5.1.1 Written Exception Requests

When a policy exception requirement is identified, the department Information Security Officer (ISO) must submit a written policy exception request, which includes the ISO signed authorization, to the State Security Office (SSO).

SOA Internal

5.1.2 Content of Exception Requests

When submitting a policy exception request, personnel must provide an authorized written description of the proposed exception through the exception request form and any supplemental information requested by the SSO.

5.2. Exception Evaluations

5.2.1 Coordination of Exception Requests

The SSO must evaluate exception requests and provide a recommendation to the CIO. The SSO must provide, in writing, the CIO decision and additional guidance to the requestor, as appropriate.

5.2.2 Approval of Exception Requests

The CIO must review policy exception requests presented by departments through the SSO with the SSO recommendations and must determine whether or not to approve the exception in accordance with the needs of the SOA enterprise and executive branch.

5.3. Exceptions Reviews

5.3.1 Regular Review of Approved Exceptions

The department must review and evaluate information security policy exceptions every 6 months to determine if the exception is still required and if the risk assessment and compensating controls continue to be adequate and appropriate. Upon review, the department must re-submit the exception for authorization. The department's failure to re-submit will result in the termination of the exception.

5.3.2 Exception Tracking

For each exception, Executive Management must maintain a written record of the exception and the business case for the exception. The SSO will review waiver related compensating controls subsequent to approval.

SOA Internal

		Effective:	5/16/2025
		Last Review:	5/16/2025
Title:	Departmental Roles and Responsibilities	Next Review:	Bi-annually
Number:	ISP-111		
Version:	1.02	Approved by:	CIO
Pages	4	Distribution:	SOA

1. Purpose

To establish functional roles and responsibilities related to State of Alaska (SOA) information assets in accordance with defined information security management system (ISMS) policies, procedures and directives.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Executive Management responsibilities;
- Allocation of responsibilities;
- Department information security officer (ISO) responsibilities;
- Department computer security designee (CSD) responsibilities; and
- Personal responsibilities.

5.1. Executive Management Responsibilities

5.1.1 Commitment to Information Security

Executive Management must actively support, maintain, and govern the department's information security management through:

- Allocation of appropriate funding and/or resources for implementation of the requirements defined by SOA policies;
- Supporting education and training of appropriate personnel;

SOA Internal

- Supervising and governing contact with external authorities where appropriate;
- Providing ongoing acknowledgement and support of information security responsibility to all personnel; and
- Oversight of policy and other department security programs or artifacts.

5.1.2 Information Security Coordination

Executive Management must ensure that information security responsibility is coordinated throughout all areas of the organization with input and participation from personnel with relevant job roles, responsibilities and duties.

5.2. Allocation of Responsibilities

Executive Management must formally assign authority and responsibility for information security functions in a clear and unambiguous manner.

- Information security responsibilities listed within this policy are designated to all Department Commissioners. The Department Commissioner may formally delegate, in a clear and unambiguous manner, the business roles and responsibilities, as defined within section 5.3 Department Information Security Officer (ISO) Responsibilities, to a business leader within the department, such as a Division Director, Deputy Director, Business Manager, or similar.
- Personnel assigned or delegated the responsibilities listed within section 5.3 Department Information Security Officer of this policy may formally delegate, in a clear and unambiguous manner, the technical roles and responsibilities as defined within section 5.4 Department Computer Security Designee (CSD) Responsibilities to a technical lead within the department, such as a department IT Manager, a Technical Manager, or similar.
- Personnel with the responsibilities listed within this policy must work directly with the SSO to ensure security compliance (confidentiality, integrity and availability) is properly maintained and the department is compliant with the SOA Information Framework and Policies. Formal delegations must be forwarded to the CISO, which maintains a record of security accountability within each department.

5.3. Department Information Security Officer (ISO) Responsibilities

5.3.1 Commitment to Information Security

All department ISOs must actively support, maintain, and manage information security within their departments through:

- Having sufficient knowledge of agency business processes and the underlying applications supporting those processes;
- Having or accumulating knowledge about the technologies and asset identification methodologies within the department to identify organizational assets;
- Providing responsible and accurate documentation on the existing business processes;
- Assisting in preparing an inventory of assets, allowing understanding of the extent of the SOA's systems, networks, applications and information to achieve an effective security program;
- Acting as the single point of contact for the SSO on all administrative, technical and physical security controls and solutions;

SOA Internal

- Coordinating and communicating with the SSO on enterprise and department security related projects, solutions, services, systems, or other security related matters;
- Facilitating the delivery of pertinent security information to all appropriate department personnel;
- Providing security explicit assignments to department personnel;
- Ensuring confidentiality agreements or non-disclosure agreements are in place for all employees and contractors with potential access to SOA restricted information and/or assets;
- Communicating information security responsibilities to all personnel within the department on an on-going basis;
- Building on the enterprise security policies, procedures and processes by developing agency policies, procedures and processes that ensure the department's essential business functions, legal and financial obligations are met;
- Ensuring department personnel, contractors, vendors, partners, visitors, and others with authorized access to SOA information and information assets are aware of and educated about all security policies, procedures, and processes, within the department and the SOA, as necessary;
- Coordinating risk assessments and mitigation of security risks;
- Coordinating system and data classification efforts;
- Coordinating threat and vulnerability analysis efforts;
- Coordinating security plans and obtaining the appropriate department and SSO approvals for the plans;
- Ensuring a coordinated effort is maintained with the SSO on the development and implementation of a department wide security architecture, systems, services, or solutions that meet the State's information security requirements;
- Providing coordination with and assistance to the SSO for periodic security audits within the departments.

5.4. Department Computer Security Designee (CSD) Responsibilities

5.4.1 Commitment to Information Security

Department CSDs must actively support the department's ISO with technical assistance in maintaining information security within the department through:

- Having sufficient technical knowledge of agency business processes and the underlying applications supporting those processes;
- Providing technical assistance in preparing an inventory of assets, indicating a clear understanding of the breadth of the department's systems, networks, applications and information to achieve an effective security program;
- Providing technical assistance to the ISO on department security policies, procedures and processes;
- Assisting the ISO in coordinating risk assessments and mitigation of security risks within the department;
- Assisting the ISO in coordinating system and data classification efforts within the department;
- Assisting the ISO in coordinating threat and vulnerability analysis efforts within the department;
- Assisting the ISO in coordinating and securing department level security plans;
- Assisting the ISO in periodic security audits within the department; and

SOA Internal

- Participating in security technical work groups as assigned.

5.5. Personal Responsibilities

5.5.1 Commitment to Information Security

Personnel must actively support and maintain the information security within their departments through:

- Maintaining appropriate levels of contact with relevant internal information security and incident response authorities (such as the SSO, ISO, CSD and regulatory bodies);
- Ensuring that unattended filing cabinets, workspace, other related work areas and work stations use appropriate controls that prevent unauthorized access to confidential information;
- Ensuring that work areas and workstations remain clear of confidential information when the information is not actively being used for defined business purposes;
- Ensuring compliance with legal, regulatory, policy, procedure, standards and directive requirements; and
- Complying with the destruction of confidential information assets procedures and retention policies.

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Third Party Security	Next Review:	Per policy
Number:	ISP-112		
Version:	1.2	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To define the information security expectations of the State of Alaska (SOA) when conducting business with vendors, contractors, business partners, and other third party entities with authorized access to SOA information and information assets operating within or on behalf of the SOA.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Risk management;
- Third party access;
- Third party agreement; and
- Third party management.

5.1. Risk Management

5.1.1 Risk Assessment and Third Parties

Executive Management must ensure that risks related to a third party accessing, processing, communicating, or managing SOA information or information processing facilities are identified and appropriately addressed.

SOA Internal

5.2. Third Party Access

5.2.1 Security of Information

Executive Management must ensure that the information security requirements of SOA information systems are identified, and that appropriate controls are implemented to safeguard such information systems, prior to granting access to third parties.

5.3. Third Party Agreements

5.3.1 Security Requirements in Third Party Agreements

Executive Management must ensure that an agreement covering relevant security requirements is in place for any third parties providing services involving accessing, processing, communicating, or managing SOA information or information processing facilities. Such an agreement must include non-disclosure definition, ownership of information, systems and services, confidentiality requirements, information retention and/or destruction during and post-mortem of agreement, service definitions, delivery levels, service management aspects, or other applicable security controls expected of the third party, or of the SOA, as appropriate to the service, agreement or contract.

5.3.2 Monitoring Compliance with Third Party Agreements

Executive Management must ensure that services of third parties are monitored to verify compliance with the security requirements of agreements. Such monitoring must include review of reports or records generated regarding the service or other criteria appropriate to the service.

Executive Management must ensure appropriate performance audits are conducted to respond to information security incidents or in accordance with the terms of service agreements. The State Security Office (SSO) or the Department of Law must provide guidance to Executive Management, as necessary, in support of issues of security or contract compliance and enforcement.

5.3.3 Updating Third Party Agreements

Executive Management must periodically review changes to the organization, its policies, and its systems to identify changes to the security requirements of third parties. When security requirements change, Executive Management must determine, whether modification of third party agreements is necessary and, if needed, must coordinate with internal or external counsel and DOA Division of General Services as well as with the applicable third parties to address the proposed changes to agreements.

Executive Management must immediately notify the DOA Division of General Services and the SSO of any material change in the SOA relationship with a third party service provider, including but not limited to:

- enhancements to the services offered;
- development of new applications and systems;
- modifications to SOA policies and procedures;
- termination of services; and
- loss of personal or sensitive information.

SOA Internal

5.3.4 Maintenance of Third Party Agreements

Executive Management and/or internal counsel must maintain an original copy of each executed third party agreement in accordance with SOA record retention policies.

5.3.5 Exchange Agreements

Executive Management must establish agreements for the exchange of information and/or software between the SOA and external parties. These agreements must include assurances for the security of SOA information throughout the agreement's life cycle and the return or certified disposal of SOA information upon termination of agreements.

5.4. Third Party Management

5.4.1 Changes to Third Party Services

Executive Management must manage changes to services, products, processes, procedures, or controls that impact the security and information assets of the SOA and ensure changes are accurately documented and communicated to DOA Division of General Services.

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Information Asset Classification and Control	Next Review:	Per policy
Number:	ISP-121		
Version:	1.2	Approved by:	CIO
Pages	4	Distribution:	SOA

1. Purpose

To ensure accountability and appropriate controls for State of Alaska (SOA) information assets are in place to classify and manage hardware, software and information within the SOA by providing overall guidance to information protection and a conceptual model for classifying SOA information based on its sensitivity level. The SOA data classification is based on the concept of "*need to know"*. Information is only disclosed to a person with a legitimate and demonstrable business need. Each SOA employee with access to SOA information assets or information systems has a security role in handling this information and is responsible to protect SOA information from unauthorized disclosure, use, modification and deletion.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy defines:

- Inventory assets;
- Information classification;
- Information handling and labeling; and
- Information classification reference table guideline.

5.1. Inventory of Assets

5.1.1 Information Asset Inventory

Executive Management must ensure that an inventory of information systems is established and maintained detailing all hardware, software, communications links, and information assets within a department.

SOA Internal

5.2. Information Classification

5.2.1 Information Ownership

Executive Management must assign a Information Owner for all information assets. Information Owners must determine the classifications of the information assets assigned to them, and must periodically review the classifications to ensure they are accurate.

5.2.2 Information Classification

Information Owners must assign one or more of the following designations to the information assets for which they are responsible:

Life Safety: Information that, in the event of loss, interruption, unauthorized disclosure, modification, damage or if otherwise unavailable, has the potential to bring about loss of life or serious harm to a person. This is the most critical and highest classification. Examples of life safety systems and information include the following:

- Systems and/or information governed by federal, State, or local law as emergency communications or critically sensitive information in support of first responders, military, other State or national defense, security, medical, emergency services, or law enforcement entities (e.g., specific federal and State acts and regulations for critically sensitive information or emergency communication solutions related to telecommunications, RF, microwave, satellite, homeland security, State and national security or defense, nuclear, transportation, critical infrastructure, bio and chemical agents, and/or weapons of mass destruction, personal protection services, law enforcement confidential informant, undercover operational information, other information or systems as deemed appropriate in protection of life safety services, systems and processes).

Confidential: Information that, in the event of loss or unauthorized disclosure, has the potential to bring about a moderate to significant financial or operational impact and/or cause a medium to long term loss of credibility or reputation. Examples of confidential information include information that is:

- Governed by federal, State, or local law (e.g., federal information regulated under Federal Information Security Management Act (FISMA) or protected health information (PHI) regulated under the Health Insurance Portability and Accountability Act (HIPAA));
- Governed under industry regulation, contract, or other agreement for which a financial penalty is associated with loss or misuse (e.g., credit card or bank account information);
- Personally identifiable information (PII), electronic protected health information (EPHI), non-public information (e.g., social security numbers); and
- Potentially damaging to the operation of SOA information systems, such as authentication information (i.e., usernames and passwords).

- **SOA Internal**: Information for which access is authorized to all State employees or authorized third party. Loss, misuse, or unauthorized disclosure of this information has the potential to result in a minimal adverse impact, operational impairment, or short-term loss of credibility or reputation.

- **Public**: Any information that is not classified as Life Safety, Confidential or SOA Internal and is readily available to the general public (public domain).

SOA Internal

5.2.3 Personally Identifiable Information (PII)

Information Owners must classify personally identifiable information (PII), including an individual's financial and medical information, as confidential. Reference SOA policy ISP-122 Privacy of Personally Identifiable Information and Alaska Personal Information Protection Act, AS 45.48, for further clarification of confidential classification for personally identifiable information.

5.2.4 Combining Classifications

When information of multiple classifications is combined, Information Owners must classify the aggregate information according to the most restrictive classification level of the source information.

5.2.5 Handling Externally Provided Information

Information Owners must assign an appropriate classification to all externally provided information that is not clearly in the public domain.

5.3. Information Handling and Labeling

5.3.1 Comprehensive Classification and Labeling

Information Owners must ensure information is labeled appropriately to indicate classification level. Any information that is not labeled must be handled as SOA confidential, except information which is indisputably, by its form and function, public domain information (e.g., a press release, an external job posting, marketing materials, unrestricted website content).

5.3.2 Labeling Printed Documents

Information Owners must ensure that printed confidential information is labeled, or that the information enclosure (e.g., envelope, folder, binder) is appropriately labeled, to indicate the information's sensitivity level.

5.3.3 Labeling Electronic Media

Information Owners must ensure that magnetic tapes, floppy disks, and other computer storage media containing confidential information, or the enclosures for such media, are externally labeled to indicate the level of sensitivity of the contained information.

5.3.4 Displayed Information

When confidential information is displayed on a computer screen or is accessible by the user, the user must ensure that the display is not viewable by personnel who are not authorized to view the information being displayed. Personnel must immediately lock their workstation when their display screen is unattended for any reason.

5.3.5 Information Life Cycle Labeling

From the time the information is created until it is destroyed, Information Owners must ensure that information is labeled appropriately according to its classification and in compliance with SOA record retention policies.

5.3.6 Protecting Sensitive Information

Information Owners must ensure that all sensitive information, including life safety, confidential and SOA internal information, is protected from unauthorized disclosure, misuse, or loss according to approved methods and policies.

SOA Internal

5.3.7 Disposal of Confidential Information

Information Owners must ensure that all sensitive information, including life safety, confidential and SOA internal information in printed or electronic form, is disposed of in accordance with approved destruction/disposal SOA policy ISP-143 Information Disposal and in compliance with SOA record retention policies (AS 40.21).

5.4. Information Classification Reference Table Guideline

The table below is a conceptual model for classifying SOA information assets according to sensitivity level. The SOA asset classification is based on the concept of *"need to know"*. Information is only disclosed to personnel with a legitimate and demonstrable business need to receive the information. This table is NOT comprehensive and is intended as a guideline only. Executive Managers for each department must determine and authorize all security levels.

Action	**Requirement if…**			
	Life Safety	**Confidential**	**SOA Internal**	**Public**
Storage on fixed Media	• Duplication required; • Encryption recommended	Encryption or physical access control	Encryption optional	Encryption not advised
Storage on Exchangeable Media	• Duplication required; • Encryption recommended	Encryption	Encryption optional	Encryption not advised
Copying	Permission of owner required	Permission of owner required	Copies for SOA employee only	No restriction
Faxing	Encrypted link plus password protected recipient mailbox or attended receipt	Password protection recipient mail or attended receipt.	Copies for SOA employee only	No restriction
Sending by Public Network	Encryption required	Encryption required	Encryption recommended	Encryption not advised.
Disposal	Shredding (cross cut required) or secure disposal boxes	Shredding (cross cut recommended) or secure disposal boxes	Shredding	Ordinary trash can
Release to Third Party	Owner approval and non-disclosure agreement	Owner approval and non-disclosure agreement	Non-Disclosure agreement	No restriction
Electronic Media Labeling Required	External and internal labels	External and internal labels	External and internal labels	No restriction
Hardcopy Labeling Required	• Each page if loose; • Front & back covers, and title page if bound	• Each page if loose; • Front & back covers, and title page if bound	• Each page if loose; • Front & back covers, and title page if bound	No restriction
Internal & External Mail Packaging	Address to specific person and label only on the inside of the envelope Certified Mail	Address to specific person and label only on the inside of the envelope Certified Mail	Envelope/Specific person label required	Envelope markings not required
Granting Access Rights	Owner ONLY	Owner ONLY	Business Owner or Manager to determine	No restrictions
Tracking Process by Log	Recipients, copies made, locations, addresses, those who viewed and destruction	Recipients, copies made, locations, addresses, those who viewed and destruction	Business Owner or Manager must determine process of tracking information	Not necessary

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Privacy of Personally Identifiable Information	Next Review:	Per policy
Number:	ISP-122		
Version:	1.2	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure that adequate and appropriate safeguards are implemented for the protection of personally identifiable information (PII) or sensitive information stored, processed, or transmitted by the State of Alaska (SOA).

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Safeguarding confidential information;
- Public communication and notification to personally identifiable information; and
- Personally identifiable information retention.

5.1. Safeguarding Confidential Information

5.1.1 Personally Identifiable Information (PII)

Executive Management must ensure that PII is stored, processed, or transmitted for approved purposes only and in accordance with applicable legal, regulatory, and contractual requirements.

SOA Internal

5.1.2 Social Security Numbers (SSN)

SSN are highly confidential and legally protected information. SSN can only be collected if no other method of identification is available or a department has statute, or regulation that allows the collection. Personnel must ensure that SSN are collected only when absolutely necessary and held with the strictest of confidence.

5.1.3 Financial Information

Financial information is highly confidential and legally protected information. Financial account numbers, passwords, and access codes must be held with the strictest of confidence and must be physically or logically secured to ensure the information is not disclosed to unauthorized personnel.

Payment card data, including credit card numbers and associated information, defined by Payment Card Industry Data Security Standard (PCI DSS), are highly confidential and protected information. Personnel must ensure that payment card electrical information is collected only when absolutely necessary and is handled in accordance with the PCI DSS.

5.2. Public Communication and Notification to Personally Identifiable Information

5.2.1 Public Communication and Notification

Executive Management must ensure, subject to applicable laws and regulations, that an SOA individual is informed of the unauthorized disclosure of the individual's PII, notwithstanding AS.45.48.010.

Personnel must obtain approval from the Department of Law prior to sending a public communication or notification of unauthorized or suspected unauthorized disclosure.

Personnel must not provide public disclosure of any unauthorized or suspected unauthorized electronic access without obtaining approval for said notification from the Department of Law.

5.2.2 Individual Access

In accordance with Personal Information Protection Act, AS 45.48; SOA citizens must be provided access to their PII upon request.

5.3. Personally Identifiable Information Retention

5.3.1 Storage

Executive Management must ensure that stored PII is protected from unauthorized access or disclosure. Executive Management must implement, wherever operationally feasible, encryption as a safeguard of electronically stored or transmitted PII. Executive Management must ensure that adequate physical controls (e.g., locked file cabinets, locked offices, data centers areas, computer equipment racks, etc.) are applied to safeguard the information.

5.3.2 Disposal

Information Owners must ensure that all sensitive information, including life safety, confidential and SOA internal information in printed or electronic form, is disposed of in accordance with approved destruction/disposal SOA policy ISP-143 Information Disposal and in compliance with SOA record disposal policies (AS 45.48).

SOA Internal

1. Purpose

To ensure all departments provide a categorization for all information and information systems collected or maintained by, or on behalf of, each department.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy defines:

- Categorization of information and information system standards;
- Categorization of information and information system security objectives;
- Potential impact on organizations & individuals guidelines for risk levels;
- Security categorization applied to information types;
- Security categorization applied to information system;
- Table indicating risk level of disclosure; and
- Table specifying SOA examples of information risk levels.

5.1. Categorization of Information and Information System Standards

5.1.1 Categorization Standards

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that promotes effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities. Established categorization standards provide consistent reporting to the Enterprise Investment Board (EIB) on the adequacy and effectiveness of

SOA Internal

information security policies, procedures, and practices. Subsequent security standards and guidelines must address the second and third tasks cited.

5.1.2 Applicability of Standards

These standards must apply to all information within the SOA government including information that has been determined pursuant to Alaska State Statute. Business Owners must use the security categorizations described in this document to provide a categorization of information or information systems. Additional security designators may be developed and used at department discretion. Departments as well as private sector organizations using the infrastructure of the SOA must use these standards and follow the standards process.

5.2. Categorization of Information and Information System Security Objectives

The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain day-to-day functions and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. SOA defines three security objectives for information and information systems:

CONFIDENTIALITY

A property of information assets, information systems, and other resources whereby access is limited to personnel and entities authorized to view the information or access the resource.

As further defined in 44 USC, § 3542, confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information; in conjunction with integrity and availability.

A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

The property of information assets, information systems, and other resources, whereby the reliability of the asset is ensured of its adherence to a code of ethical truth, through the implementation of protections against unauthorized tampering, modification, or corruption.

As further defined in 44 USC, § 3542, integrity is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; in conjunction with confidentiality and availability.

A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

Indicates a property of information assets, information systems, and other resources whereby appropriate personnel, systems, or other entities have the ability to readily access resources without impedance.

As further defined in 44 USC, § 3542, availability is ensuring timely and reliable access to and use of information; in conjunction with confidentiality and integrity.

A loss of *availability* is the disruption of access to or use of information or information system.

5.3. Potential Impact on Organizations & Individual Guidelines for Risk

There are three areas of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity and availability). The application of the following

SOA Internal

classifications to each of the areas for information and information systems must take place within the context of each organization and the overall SOA interests.

The potential impact is **LOW** and considered **Limited** if:

The loss of confidentiality, integrity and availability could be expected to have a **limited** adverse effect on organizational operations, assets, or individuals. Adverse effects on individuals must include, but are not limited to, loss of privacy to which individuals are entitled under law.

AMPLIFICATION: A limited adverse effect means that the loss of confidentiality, integrity and availability might:

- cause a degradation in mission capability to an extent and duration that the organization is still able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to organizational assets;
- result in minor financial loss; or
- result in minor harm to individuals.

The potential impact is **MODERATE** and considered **Serious** if:

The loss of confidentiality, integrity and availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that the loss of confidentiality, integrity and availability might:

- cause a significant degradation in mission capability to an extent and duration that the organization is still able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to organizational assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is **HIGH** and considered **Severe or Catastrophic** if:

The loss of confidentiality, integrity and availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that the loss of confidentiality, integrity and availability might:

- cause a severe degradation in or loss of mission capability to an extent and duration that the organization is NOT able to perform one or more of its primary functions;
- result in major damage to organizational assets;
- result in major financial loss; or
- result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

5.4. Security Categorization Applied to Information Types

The security category of an information type can be associated with both user and system information.

Information can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system (see description of security categories for information systems below). Establishing an appropriate security category of an information type requires determining the *potential impact* for each security objective associated with the particular information type. System information (e.g.,

SOA Internal

network routing tables, password files, and cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed, stored, or transmitted by the information system to ensure confidentiality, integrity, and availability.

The generalized format for expressing the security category (SC) of an information type is:

> **SC** information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE. The potential impact value of *not applicable* only applies to the security objective of confidentiality.

EXAMPLE 1: An organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category (SC) of this information type is expressed as:

> **SC** public information = {(**confidentiality**, NA), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 2: Law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category (SC) of this information type is expressed as:

> **SC** investigative information = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}.

EXAMPLE 3: Financial organization managing routine administrative information (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security category (SC) of this information type is expressed as:

> **SC** administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

5.5. Security Categorization Applied to Information Systems

Determination of the security category of an information system requires analysis and must consider the security categories of all information types that reside on the information system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity and availability) must be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system. It is recognized that information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate *worst case* potential impact for the overall information system, thereby obviating the need to consider the system processes in the security categorization of the information system.

The generalized format for expressing the security category (SC) of an information system is:

> **SC** information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

SOA Internal

Note that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

EXAMPLE 4: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that:

- the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and
- the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories (SC) of these information types are expressed as:

SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},
and
SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is expressed as:

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

EXAMPLE 5: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that:

- for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and
- for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories (SC) of these information types are expressed as:

SC sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)},
and
SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is initially expressed as:

SC SCADA system = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a

SOA Internal

security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as:

SC SCADA system = {(**confidentiality**, MODERATE), (**integrity**, HIGH), (**availability**, HIGH)}.

SOA Internal

5.6. Table of Risk Level for Disclosure

Table 1
This table summarizes the potential risk impact definitions for each security objective—confidentiality, integrity and availability.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have **a severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

SOA Internal

5.7. Table of Specific SOA Examples

Table 2
This table indicates specific examples of SOA information and information system security objectives — confidentiality, integrity and availability. These are ONLY examples as each department and independent entities are responsible for the risk level categorization.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	• Public inform web server	• Short term marketing plan	• Personally Identifiable Information (PII) • Prosecutor evidence
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	• Non-Privacy related administrative file server	• Public web server compromise • Changes to access data base	• SCADA sensor data • MyAlaska
Availability Ensuring timely and reliable access to and use of information.	• Brochures • Flyers • Public "How to's" memos	• Public web server compromise	• Ingress/Egress router failure • DDoss on Alaska.gov

SOA Internal

1. Purpose

To ensure that State of Alaska (SOA) information security systems comply with all relevant legal, regulatory, and contractual requirements.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy defines:

- SOA compliance with statutes and regulations;
- Compliance with regulatory agency standards; and
- Proper crediting of source information.

5.1. SOA Compliance with Statutes and Regulations

5.1.1 SOA must comply with Statutes and Regulations Information

SOA must ensure all departments comply with all State and Federal information statutes and regulations, as well as SOA Information Security Policies.

5.1.2 Departmental Information Security Policy Compliance

Departments that create customized policies for their individual department needs must ensure that those policies are reviewed by the SSO. Policies should be created with consultation of legal counsel, relevant laws, regulations and mandates. ISO will work with the

SOA Internal

SSO to edit, copy, publish, and distribute department information security policies. The CISO and State CIO retain the authority to require changes in department policies that do not meet minimum SOA statewide ISP requirements.

5.2. Compliance with Regulatory Agency's Standards

5.2.1 List of Relevant Information Security Standards Organizations

Departments must ensure that all policy development is compliant with State ISP and leverage applicable security standards and requirements based on applicable laws, statutes, and legally binding agreements. References are as follows:

- SOA Information Security Policies (ISP) Office of Information Technology (https://oit-int.alaska.gov/policy/information-security-policies/);
- National Institute of Standards and Technology (NIST) http://www.nist.gov/index.html;
- Center for Internet Security (CIS) CIS Center for Internet Security
- International Organization for Standardization (ISO) ISO - International Organization for Standardization;
- Payment Card Identity Data Security Standard (PCI DSS) PCI Security Standards Council – Protect Payment Data with Industry-driven Security Standards, Training, and Programs;
- Or others as necessary.

5.3. Proper Crediting of Source Information

5.3.1 Proper Crediting of Source Information

SOA personnel must ensure the source of all Information Security Policies or regulatory requirements is properly credited to the appropriate information reference source when establishing department policies. Departments must provide the SSO with the detailed information necessary to ensure SOA policy ISP-004 Regulatory Matrix remains current with all statutory or regulatory requirements.

SOA Internal

		Effective:	7/1/2017
		Last Review:	7/1/2017
Title:	ESI Hold and Search Requests	Next Review:	Annually
Number:	ISP-125		
Version:	1.12	Approved by:	CIO
Pages:	1	Distribution:	SOA

1. Purpose

To ensure that all holds of electronically stored information (ESI) (including email) and searches for ESI that are requested to be implemented by the State Security Office (SSO) are authorized.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy applies to all SOA branches, departments, divisions, corporations, commissions or other related entities which are referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

- This policy stipulates the requirements for all ESI holds and searches that are authorized by the CIO or CIO's designee.

5.1. ESI Holds and Searches

The SSO may be asked to hold or search for ESI. ESI holds and searches that are requested to be implemented by the SSO must be authorized by the CIO or CIO's designee. Only at the request of the CIO or CIO's designee shall the SSO prevent the deletion of or coordinate the search for and collection and production of ESI.

The SSO will prevent the deletion of or coordinate the search for and collection and production of ESI from the SOA network, users' computers, workstations, servers, other electronic devices, or email system, as requested. Analyses may be performed by the SSO as part of the search and collection process to ensure that the process is thoroughly conducted and that the information preserved or produced is covered by the ESI hold or search request. Such analyses must be authorized by the CIO or CIO's designee. The SSO will provide detailed reports on its activities under this policy to the CIO or CIO's designee.

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Personnel Security	Next Review:	Per Policy
Number:	ISP-131		
Version:	1.2	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To establish the information security requirements associated with the hiring, management, and training of State of Alaska (SOA) personnel who will access or handle confidential/sensitive information or activities, in the course of performing their job responsibilities.

Note: This policy is supplemental to the personnel policies of the SOA and does not replace other SOA policies with respect to the employment, management, training, or termination of SOA personnel.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Personnel security responsibilities;
- Appropriate access to information;
- Personnel safeguards, access and termination;
- Personnel training and awareness; and
- Personnel security background checks.

5.1. Personnel Security Responsibilities

5.1.1 Security Roles and Responsibilities

Executive Management must establish the information security roles and responsibilities for all SOA personnel.

SOA Internal

5.2. Appropriate Access to Information

5.2.1 Appropriate Access

Business Managers must ensure that personnel are granted appropriate access to sensitive and regulated information and information assets consistent with their work responsibilities, throughout the duration of their employment. Business Managers must ensure that such access is limited to the minimum amount necessary to perform job specific responsibilities.

Executive Management must ensure that personnel, contractors, vendors, partners, visitors, and others with authorized access to SOA information and information assets are appropriately supervised when handling sensitive and regulated data, that such handling is for purposes of performing SOA work responsibilities only, and that those individuals handling such information are authorized.

5.3. Personnel Safeguards, Access and Termination

5.3.1 Hiring

Business Owners must ensure that adequate safeguards (e.g., screening and background checks, including applicable Federal Bureau of Investigation (FBI) fingerprint based background checks) are in accordance with requirements of potential access to FBI and Criminal Justice Information Security (CJIS) data.

5.3.2 Changes in Position

Business Managers must ensure that the allocation of access by personnel is reviewed and updated when personnel change positions within the SOA. Personnel tasked with managing access controls must promptly update access to reflect changes in position, must maintain a record of all such changes, and must regularly review that such changes have been appropriately made.

5.3.3 Termination

Information Security Officers (ISO) must establish a formal process, covering personnel and third parties, to ensure that the access rights of terminated individuals are promptly disabled and removed. Personnel tasked with managing access controls must promptly change access rights to reflect the termination, maintain a record of the changes, and regularly review that such changes have been appropriately made.

5.4. Personnel Training and Awareness

5.4.1 Information Security Training

ISO must ensure that all personnel, contractors, vendors, partners, visitors, and others with access or potential access to SOA information and information assets receive appropriate information security training and/or awareness and are provided with information security awareness materials on a regular basis. This includes regular security training requirements as defined by legal or regulatory requirements (e.g., HIPAA, CJIS, PCI DSS, IRS, or others).

5.5. Personnel Security Background Check

Any personnel who will have the potential to access CJIS data must successfully obtain an Alaska Public Safety Information Network (APSIN) security clearance and have authorization for APSIN data access by the Department of Public Safety's APSIN Security Office.

SOA Internal

5.5.1 Background Check

The clearance and authorization process requires a criminal background and national records check to be conducted by the Department of Public Safety's APSIN Security Office and the FBI. As part of this process applicants will be required to submit to fingerprinting.

SOA Internal

		Effective:	12/19/2025
		Last Review:	12/19/2025
Title:	Security Awareness and Training	Next Review:	Tri-annually
Number:	ISP-132		
Version:	1.03	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To establish information security training and awareness processes to ensure that personnel understand State of Alaska (SOA) information security requirements, roles, and responsibilities.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates appropriate:

- Security Awareness Program design;
- Security Awareness Program material; and
- Security Awareness Program implementation.

5.1. Program Design

5.1.1 Roles and Responsibilities

The State Security Office (SSO) is responsible for developing, executing, and monitoring enterprise information security training programs.

Information Security Officers (ISO) are responsible for executing information security training programs, activities and materials for line of business compliance requirements within their Departments.

SOA Internal

5.1.2 Alignment with Policy

The SSO must ensure that SOA training and awareness materials are consistent and aligned with SOA legal and regulatory requirements, SOA Information Security Management System (ISMS), policies, procedures, and directives.

ISOs are responsible for assuring the training and awareness materials provided meet all specific regulatory and compliance requirements for their Departments and are in alignment with SOA legal, regulatory and ISMS requirements.

5.1.3 Requirements

The SSO must establish this training policy and statewide requirements for SOA personnel.

ISOs are responsible for ensuring department specific requirements for information security training and compliance are reviewed annually. Examples include but are not limited to HIPAA, CJIS, FTI, and PCI.

5.1.4 Program Management

SSO manages the statewide training program including development and presentation of training and educational materials. Program management includes assigning training campaigns, monitoring completion, and reporting metrics to executive management.

ISOs must coordinate with the SSO in the delivery of the statewide training program for SOA personnel within their departments. ISOs must make available any training completion metrics for department specific requirements to the SSO upon request.

5.2. Program Materials

5.2.1 Organization-wide Training

Executive Management must ensure that all personnel without an approved exception, regardless of work duties, receive appropriate information security training with respect to general security requirements and practices including, but not limited to, responsibility for safeguarding information assets, physical access to SOA facilities, internet security practices, social engineering, insider threat, and security event reporting. The SSO must provide oversight to all Departments on awareness programs to regularly communicate information security requirements and practices to all personnel.

5.2.2 Role Specific Material

Executive Management must ensure that personnel to whom additional security requirements apply (e.g., system administrators, network engineers, auditors, personnel with potential access to regulated information), or who handle confidential or personally identifiable information in the course of their work, receive additional training appropriate to their roles with regard to SOA policies ISP-121 Asset Classification & Control and ISP-122 Privacy of Personally Identifiable Information requirements.

5.3. Program Implementation

5.3.1 Implementation Approach

ISOs must coordinate with the SSO to ensure regulatory compliance requirements are mapped to associated ISP's in accordance with ISP-124, 5.3.1. ISOs must develop a formal and documented agency-specific information security training and awareness program for

SOA Internal

personnel to ensure compliance with regulatory requirements and provide audit material for Executive Management and SSO.

5.3.2 Implementation Techniques

Executive Management must ensure that personnel receive the required training and that information security training and awareness activities are documented. ISOs, with the assistance of the SSO, will employ a variety of techniques in implementing security training and security awareness including, but not limited to:

- Training at initial hiring;
- Quarterly end user security training
- Monthly phishing campaigns
- Annual review of Acceptable Use Policy
- Computer-based training for agency specific regulatory requirements; and
- Formal training courses, training in conjunction with employee evaluations and contract reviews; and
- Distribution of awareness information via e-mail, intranet or other written, electronic, or oral publications and communications.
- Implementation of remedial training requirements based on individual security awareness training performance.

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Secure Areas	Next Review:	Per policy
Number:	ISP-141		
Version:	1.02	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

The State of Alaska (SOA) must establish information security requirements for secure confidential information processing areas within SOA facilities.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy defines:

- Secure areas.

5.1. Secure Areas

5.1.1 Designating Secure Areas

Business Owners must ensure that offices, rooms, and facilities where confidential information is handled or stored, including information processing facilities, are designated as "secure areas."

5.1.2 Physical Perimeters

Business Owners must ensure that secure areas are safeguarded by physical controls (e.g., fences, gates, walls, doors, locks, partitions, or occupied reception desk areas) that establish a perimeter that restricts access to unauthorized individuals. Executive Management must

SOA Internal

ensure that access controls are placed at points of ingress to secure areas to limit access to only authorized personnel and escorted visitors.

5.1.3 Supervision in Secure Areas

Business Managers must ensure that personnel receive appropriate supervision with respect to the handling of confidential information when working in secure areas.

5.1.4 Delivery and Loading Areas

Business Owners must ensure that safeguards are applied to delivery and loading areas to protect the information assets that are delivered, stored, or dispatched from unauthorized access.

5.1.5 Documenting Authorization and Controls

Business Managers must ensure that safeguards and authorization processes are documented and communicated to ensure all personnel in the secured area understand their roles and responsibilities for maintaining the security of the area.

5.1.6 Appropriate Use of Facilities

Department Information Security Officers must ensure policies, procedures, and controls are implemented to deter personnel from using information processing facilities for unauthorized purposes.

5.1.7 Establishment of Safeguards

The State Security Office must ensure that safeguards are established and implemented to protect and ensure SOA facilities are properly secured compensatory to levels that meet applicable State and federal statutes, regulatory and contractual requirements.

SOA Internal

Title:	Equipment Security	Effective:	12/19/2025
Number:	ISP-142	Last Review:	12/19/2025
Version:	1.01	Next Review:	Tri-annually
Pages	2	Approved by:	CIO
		Distribution:	SOA

1. Purpose

To ensure that State of Alaska (SOA) information processing systems and SOA information assets are appropriately protected from physical and environmental threats.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Equipment must be secure and protected; and
- Access controls must be implemented.

5.1. Equipment Must be Secure and Protected

5.1.1 Secure Areas

Personnel tasked with information system deployment responsibilities must ensure that SOA information systems are deployed within a secure facility such as a data center, storage cabinet, collocation facility, or other approved area. Business Managers must evaluate the security risks associated with physical, environmental, geopolitical, or other threats and deploy additional security controls as needed to mitigate these threats in a manner commensurate to the classification of the information.

SOA Internal

5.1.2 Public Terminals

Personnel tasked with deployment and administration of publicly provided PC's or kiosk must ensure physical protections are deployed to prohibit theft such as a cable lock on the device.

5.1.3 Cables and Wiring

Personnel tasked with information system deployment responsibilities must:

- Ensure that data communication links such as telephone cables and network cables are appropriately protected to prevent unauthorized access to sensitive information.
- Ensure that power cabling or other cabling required to support information systems is protected from unauthorized tampering or disturbance.
- Not deploy cabling where unencrypted confidential or SOA internal only information must travel (e.g., in public areas, lobbies or commonly shared rooms) in areas outside of SOA control.

5.1.4 Wiring Closets

Personnel must ensure that wiring closets, telecom rooms, or other supporting infrastructures are protected from unauthorized access through the use of physical security controls.

5.2. Access Controls Must be Implemented

5.2.1 Physical Access Controls

Personnel tasked with information security oversight responsibilities must implement controls to ensure that physical access to secure information processing facilities, data centers, wiring closets, and related infrastructure is protected from unauthorized physical access.

5.2.2 Logical Access Controls

Personnel tasked with information security oversight responsibilities must implement administrative and technical controls to ensure that only authorized personnel are provided logical (e.g., administrative console) access to information systems containing sensitive information.

5.2.3 Auditing of Controls

Personnel tasked with information security oversight responsibilities must implement proper auditing controls to identify personnel accessing secured or controlled areas. This would include either automated access control logging or physical "paper" logs which personnel must sign when entering and leaving a controlled area.

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Information Disposal	Next Review:	Per policy
Number:	ISP-143		
Version:	1.03	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To define requirements for the proper disposal of State of Alaska (SOA) information and media that contain sensitive information.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Secure disposal; and
- Information disposal.

5.1. Secure Disposal

5.1.1 Disposal According to Classification and Retention Policy

Personnel must ensure that *Confidential* or *SOA Internal* information is appropriately disposed of when its use is no longer required. Personnel must dispose of or destroy information consistent with the requirements of SOA record retention policies.

5.1.2 Disposal Techniques

The State Security Office (SSO) must establish and communicate a procedure that defines the techniques and solutions that are authorized for the disposal of sensitive information. Disposal techniques must be approved by the State Archivist under 4 AAC 59.030.

SOA Internal

5.1.3 Organizational Control

Personnel must ensure devices or media with confidential or SOA Internal information are maintained within organizational control until information disposal is complete.

5.1.4 Storage Media Disposal

Personnel must utilize a NIST 800-88 compliant wipe process for all *Confidential* or *SOA Internal* information on any workstation, server, portable device, removable device media or other electronic devices or media, to include those found in copiers and printers, prior to the disposal, decommission, or reallocation. Such reallocation includes but is not limited to office or departmental transfers, disposal through standard surplus equipment processes, and donations (e.g., to schools or non-profit organizations).

5.1.5 Disposal Records

Personnel tasked with information disposal responsibilities must ensure that a record of the disposal is created and maintained by their department.

5.2. Information Disposal

5.2.1 Printed Format

A crosscut (hatch) shredder or burning is required for the disposal of all printed information that is classified as *Confidential*, *SOA Internal* or sensitive information.

5.2.2 Electronic Format – Fixed Media

Personnel must utilize a NIST 800-88 compliant wipe process on workstations, servers, network devices, portable devices, or other electronic devices, to include printers and copiers, using an approved technique prior to decommissioning or reassigning the device. If a method of erasure is not possible, personnel must destroy the fixed storage device using an approved technique sufficient to prevent retrieval of information from the device (e.g., drilling, breaking, or destructive level degaussing).

5.2.3 Electronic Format – Removable Media

Personnel must erase sensitive information stored on removable media using an approved technique prior to reassigning the media. If a method of erasure is not possible, or if the media is decommissioned, personnel must destroy the removable media using an approved technique sufficient to prevent retrieval of information from the device (e.g., cutting, breaking, or degaussing).

5.2.4 Disposal and Destruction Form

A Media Disposal Assurance Form must be attached to the physical property and must be signed by a Business Manager or Business Owner. The form will be for Salvage/Surplus or Destruction. There must be a Transfer Authorization Form (TAR) that accompanies the salvaged/surplus device(s), prior to any acceptance by the Property Manager or State warehouses.

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Portable Media and Devices	Next Review:	Per Policy
Number:	ISP-144		
Version:	1.02	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure that safeguards are applied to sensitive or confidential State of Alaska (SOA) information stored on portable data devices.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Proper use of portable data devices.

5.1. Use of Portable Data Devices

5.1.1 No Use without Authorization

Personnel must not store non-encrypted sensitive or confidential SOA information on a portable data device (e.g., flash drive, USB hard drive, memory card or laptop). All encryption must be compliant with SOA policy ISP-192. Exceptions can be administered through the process described in SOA policy ISP-103 Managing Exceptions.

5.1.2 Approved Devices

When personnel are authorized to store sensitive or confidential SOA information on a portable data device, personnel must only use devices supplied by SOA or approved by Executive Management.

SOA Internal

5.1.3 Safeguarding and Sharing

Personnel authorized to store sensitive or confidential SOA information on a portable data device must ensure that the information is protected from unauthorized disclosure by appropriate physical and technical safeguards (e.g., data encryption) and in accordance with applicable SOA policies.

5.1.4 Erase when Information is not Required

Personnel authorized to store sensitive or confidential SOA information on a portable data device must ensure that the information is not retained on the portable data device when it is no longer required for a business purpose.

5.1.5 Physical Media in Transit

Personnel authorized to transport SOA information on a portable data device, beyond the boundaries of SOA facilities, must ensure that controls are in place to ensure the security of that media in transport.

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Protection Against Malicious Software	Next Review:	Per Policy
Number:	ISP-161		
Version:	1.02	Approved by:	CIO
Pages	4	Distribution:	SOA

1. Purpose

To ensure that systems within the State of Alaska (SOA) network are appropriately protected against malicious software such as viruses, Trojan horses, worms, and spyware. Appropriate protection is defined as steps taken to:

- Initially establish protection mechanisms prior to introduction to the SOA network environment and;
- Perform appropriate remediation to systems or devices which have become affected by malicious software.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Protection against malicious code (pre/post introduction to the network environment); and
- Remediation of systems.

5.1. Protection Against Malicious Code

5.1.1 Protective Controls

Personnel tasked with system administration responsibilities must implement both technical countermeasures and operational processes which act together to form a layered "Defense-in Depth" to protect all SOA owned and managed equipment against malicious software such as viruses, Trojan horses, "rootkits", Botnet, spyware and other known malicious software. This protection must be implemented prior to the introduction of a system or device to the

SOA Internal

network environment. Remediation will be required for any host or system found to be compromised.

5.1.1.1 Technical Countermeasures

5.1.1.1.1 Intrusion Prevention

Personnel tasked with system administration responsibilities must deploy State Security Office (SSO) approved "Zero-Day Protection" malware prevention technologies, for example Cisco Security Agent or other SSO approved host-based intrusion prevention software on all servers, systems, and workstations.

5.1.1.1.2 Intrusion Detection

Personnel tasked with system administration responsibilities must deploy SSO approved "Antivirus" malware detection technologies, for example Symantec Anti-Virus or other SSO approved antivirus software on all servers, systems, and workstations. Antivirus signatures must be updated in a manner compliant with the critical software patching timeline.

5.1.1.2 Operational Processes

5.1.1.2.1 System Hardening

Personnel tasked with system administration responsibilities must ensure that all systems and devices are adequately hardened at both the operating system and application level prior to deploying a system or device in its operational environment. Externally facing systems shall be hardened and protected at the highest feasible level.

The purpose of system hardening is to eliminate as many security risks as possible from the operating system and applications. When building new or reimaging existing systems personnel shall remove all non-essential software programs and utilities from the computer. If any software or configuration provides any access (such as "backdoor access") to the system, the software or configuration must be removed unless approved by the SSO. "Best Practice" entities such as Center for Internet Security, Defense Information Systems Agency (DISA), and National Institute of Standards and Technology (NIST) must be used for defining appropriate hardening requirements. Unless otherwise approved by the SSO all SOA infrastructure shall be hardened to STIG or CIS Level 1 standards as provided by Center for Internet Security (cisecurity.org). Exceptions must be noted in documentation, such as security plans and disaster recovery build documentation.

Advanced system hardening may involve reformatting the hard disk and only installing the bare necessities that the computer needs to function. File and print sharing shall be turned off if not absolutely necessary and TCP/IP may be the only protocol installed. The guest account is disabled or removed, the administrator account shall be renamed, root accounts shall be disabled when supportable, and secure passwords shall be created for all user logons. Auditing is enabled to monitor unauthorized access attempts.

5.1.1.2.2 Software Patching

Personnel tasked with system administration responsibilities must ensure that all security patches, at both the operating system and application level are applied on all workstations, servers, network and telecommunication equipment within the specified timeframes defined as:

- Critical - v3.0 CVSS Score 9.0-10.0

SOA Internal

Internally facing Systems shall be patched as soon as operationally possible but no later than 15 days after the vendor release date.

External Facing Systems Shall be patched within 48 hours or protected via compensating controls within 48 hours of vendor release and patched as soon as operationally possible no later than 15 Days.

- High-v3.0 CVSS Score 7.0-8.9

  Internally facing Systems shall be patched as soon as operationally possible but no later than 30 days after the vendor release date.

  External Facing Systems Shall be patched within 48 hours or protected via compensating controls within 48 hours of vendor release and patched as soon as operationally possible no later than 30 Days.

- Moderate-v3.0 CVSS Score 4.0-6.9

  Internally facing Systems shall be patched no later than 30 days after the vendor release date.

  External Facing Systems Shall be patched within 48 or protected via compensating controls within 48 hours of vendor release and patched as soon as operationally possible no later than 30 days.

- All other patches v3.0 CVSS Score 0.0-3.9

  Internal facing shall be patched no later than 120 days after the vendor release date.

  External facing systems shall be patched or protected via other mitigations as soon as operationally possible but no later than 90 days.

Exceptions must be evaluated on a case by case basis (considering custom application and designs) and require written approval from the SSO.

When administering software patch management, personnel must also reference SOA policy ISP-193 Vulnerability and Patch Management for further administrative considerations.

5.1.1.2.3 Log Review

Personnel tasked with system administration responsibilities must regularly review log files from all network resources (e.g., firewalls, routers, servers, appliances and other devices) to identify indications of an intrusion or unauthorized changes in the running configuration of a system. If anomalies are detected, personnel must report the security event according to SOA policy ISP-152 Incident Reporting.

5.1.1.2.4 Backup and Restore

Personnel tasked with system administration responsibilities must regularly perform data backups commensurate with the risk levels determined by the data and system owner. Backup frequency and retention must align with Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

In all cases backups must be verified at the time of creation by a read after write process and should periodically be verified by the performance of an actual recovery process.

SOA Internal

5.1.1.2.5 Mobile Code Protection

Personnel tasked with system administration responsibilities must ensure that protections are deployed to prevent the execution of unauthorized mobile code; should the use of mobile code be authorized, system administration personnel must monitor the use of mobile code and deploy technical countermeasures to prevent unauthorized activity.

5.2. Remediation of Systems

5.2.1 Remediation of Compromised/Exploited Systems

Personnel tasked with system administration responsibilities must ensure that systems or devices which are determined to be compromised by malicious software are remediated appropriately.

- Appropriate remediation must be accomplished in a manner and at a level, consistent with ensuring the malicious software is completely and fully removed and that any impacted system, application, or data files or elements do not contain residue or artifacts of the malicious software.
- Systems or devices compromised by malicious software classified as either a Trojan Horse or any form of malicious software which causes a system or device to participate in a Botnet, must be fully wiped and rebuilt. Wiping must be performed to a degree which will prevent the reconstitution of any Trojan Horse or Botnet software from remnants or artifacts purposely disbursed or covertly hidden within the filesystem, memory or other storage area.
- Currently approved media wiping should follow disposal techniques in ISP-143: Information Disposal.
- Systems or devices compromised by malicious software other than noted above may be remediated in accordance with procedures recommended by the manufacturer of the antivirus/anti-malware software which detected the malicious software.

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	System Planning and Acceptance	Next Review:	Per policy
Number:	ISP-162		
Version:	1.2	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To establish information security requirements with respect to the purchasing and implementation process for new and updated software and hardware in the State of Alaska (SOA) network environment.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- System planning and acceptance;
- System criteria and testing;
- Implementation training;
- Information system documentation; and
- Security planning.

5.1. System Planning and Acceptance

5.1.1 Capacity Planning

Executive Management must ensure that the capacity and performance of information systems are monitored to assure the confidentiality, integrity and availability of SOA information.

SOA Internal

5.1.2 Security Requirements in Purchases

Prior to the acquisition or upgrade of any information system, personnel tasked with purchasing responsibilities must ensure that information security requirements, including SOA policy requirements, are considered and addressed in the planning, selection, approval, and authorization of the information system.

5.1.3 Involvement of Security Employees

Executive Management must ensure that Department Information Security Officers (ISO) are involved in the process of planning, selecting, updating, approving, and authorizing information systems to ensure that each system provides adequate safeguards to protect sensitive SOA information.

5.2. System Criteria and Testing

5.2.1 Acceptance Criteria

Personnel tasked with implementing or upgrading information systems, with the assistance and approval of the State Security Office (SSO) must establish criteria for acceptance of information systems based on user need, technical requirements, and information security requirements.

5.2.2 System Testing

Prior to a new or upgraded information system being put into production, Executive Management must ensure that testing is performed to ensure that the system; is configured correctly, implements safeguards as required by SOA policy, and does not present an increased risk to the protection of SOA information. All testing must be done in a secure environment that is not connected to the production network, and must not be performed on production systems.

5.2.3 Minimum Test Requirements

Personnel tasked with system testing must access and test for vulnerabilities as defined on following websites:

- SANS top 20 internet security methods of protection. http://www.sans.org/top20/
- Open Web Application Security Project (OWASP) top 10 internet security methods of protection. http://www.owasp.org/index.php/Top 10 2007

5.3. Implementation Training

5.3.1 Training

SOA ISOs must be trained on the secure operation of new or upgraded information systems prior to implementation in production. They are responsible to train department personnel and Executive Management must maintain a record of the training.

5.4. Information System Documentation

5.4.1 Updating and Storage

Executive Management must ensure that documentation, including software licensing, for all information systems is maintained, protected, and updated as appropriate, and that each

SOA Internal

Department's information asset inventory is updated whenever information systems are added or upgraded.

5.5. Security Planning

5.5.1 Security Planning Documentation

Executive Management must maintain on record a system security plan for all systems, services and networks matching one or more of the following criteria:

- Externally accessed systems that are exposed to the internet;
- Systems that facilitate or contain safety of life information or processes, confidential or SOA internal information; or
- Systems that are categorized as "high" or "medium" according to the SOA policy ISP-121 Asset Classification and Control documentation.

Personnel must submit all security plan documentation to the SSO for approval and adoption before making these systems available in production use.

5.5.2 Security Plan Format

Personnel preparing system security plans must use the approved security plan format available through the SSO web site.

Security plan documents must include the minimum topic requirements defined in the approved format.

Templates are located at the following:

Template for Security Planning Guide Applications
https://oit-int.alaska.gov/media/1548/application_security_plan.docx

Template for Security Planning Guide Systems
https://oit-int.alaska.gov/media/1545/system_security_plan.docx

Security plan documents must include information accessed through the planning guide:

Security Planning Guide
https://intranet.state.ak.us/admin/ETS/security/SOA_Security_Planning_Guide.pdf

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Electronic Messaging and Archiving	Next Review:	Per policy
Number:	ISP-163		
Version:	1.2	Approved by:	CIO
Pages	4	Distribution:	SOA

1. Purpose

To define security criteria for the deployment, use, archiving and retention of electronic messaging systems within the State of Alaska (SOA) network environment.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- System ownership and email account management;
- Use of messaging systems;
- Message protection;
- Electronic messaging administration, archiving and retention; and
- Safeguards.

5.1. System Ownership

5.1.1 No Expectation of Privacy

Information sent by, received by, or stored on SOA electronic messaging systems is the property of the SOA. Executive Management must ensure that all personnel are informed there is no expectation of privacy when communications sent by, received by, or stored on SOA electronic messaging systems, and that electronic messages are subject to review by authorized personnel without prior notice as defined within this policy.

SOA Internal

5.1.2 Email Account Management

All personnel with an email account must be educated on the executive branch email management and all new personnel with an assigned SOA email account must be educated on the policy before the account is activated. The education portion of this policy does not take effect until the State implements the email archiving system.

Guidelines for determining what types of emails must be archived can be found in the document entitled "Email: FAQ and Rules," linked on the Division of Archives home page and found at http://www.archives.state.ak.us/pdfs/records_management/email.pdf

5.2. Use of Messaging Systems

5.2.1 Business Use

Executive Management must inform personnel that SOA information messaging systems are intended for approved purposes only, and that Executive Management understands that incidental personal use of such systems may be unavoidable. Personnel must ensure that incidental use is de minimus and complies with SOA policy ISP-172 Business Use/Acceptable Use and AS 39.52.

5.2.2 Time Critical Communication

Electronic messaging systems must not be used for time critical or emergency security communications where a delay in delivery or reading of an electronic message would have an adverse impact on SOA operations, unless the communications are otherwise confirmed as being received or reviewed (e.g., Critical "Life Safety" system failures, virus threats, compromises or unauthorized disclosure notifications).

5.2.3 Personal Accounts

When executive branch personnel conduct state business through email they must, whenever feasible, use the SOA electronic mail system. In some circumstances, personnel may need to use, or may inadvertently use, private email accounts to conduct state business. In those instances, personnel must send copies of those messages to their SOA email accounts, as required in the Email Archiving Policy AS 44.21.

Under no circumstance may SOA personally identifiable information (PII) be sent to or from an executive branch personnel's private email account. PII is defined in AS 45.48.590 (4).

5.2.4 Third Party Recipients

Personnel tasked with the responsibility for communication with third parties (e.g., customers, residents, or vendors) by way of electronic messaging systems must ensure that such communication complies with SOA privacy and confidentiality statutes, administrative orders, policies, procedures and directives.

5.3. Message Protection

5.3.1 Sensitive Information

Personnel must not transmit sensitive information to a third party by way of SOA electronic messaging systems without the explicit approval of the Data Owner, and must safeguard sensitive information according to SOA statutes, administrative orders, policies, procedures, and directives when sending such information to external recipients by way of SOA electronic messaging systems.

SOA Internal

5.4. Electronic Messaging Administration, Archive and Retention

5.4.1 Electronic Message Notice

Personnel tasked with system administration responsibilities must configure electronic messaging systems such that a notice is appended at the end of each electronic message indicating that the message will contain sensitive information and is for the use of the intended recipients only, and requesting notification and prompt deletion if a message is incorrectly delivered.

Below is an example of an acceptable notice.

> *This message contains information that may be confidential. Unless you are the addressee you may not use, copy, or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender by reply e-mail to <NAME> and delete the message.*

5.4.2 Electronic Message Retention

Emails, including attachments, are subject to the same records retention requirements that apply to any other electronic or non-electronic records and must be archived for the longest applicable period. The applicable records retention requirements are the SOA executive branch records retention schedules imposed pursuant to AS 40.21 and any implementing regulations, and the requirements imposed pursuant to a notification of a legal hold in connection with judicial or administrative litigation, or imposed because of a request under the Alaska Public Records Act, AS 40.25.100 - 40.25.220.

The use of local personal file folders (PST files) to store or archive emails is prohibited. All email retention must occur within the Enterprise email system; exceptions must be documented by the department's internal policies and procedures and approved by the SSO.

All executive branch employees are responsible for archiving into the designated executive branch email archiving system their sent and received emails, including any attachments in accordance with the Email Archiving Policy AS 44.21.

Executive Employees: Any email sent or received by an executive employee may be deleted within 90 days unless the email is subject to a records retention requirement, public records request or legal hold. If within that 90-day period a sent or received email becomes subject to a records retention requirement, public records request or legal hold then it cannot be deleted unless the requirement, request, or hold is lifted before the end of the period.

Non-Executive Employees: If a records retention requirement applies to a sent or received email of a non-executive employee, then within 90 days after the email was sent or received, it must be archived into the state's designated email archiving system in accordance with the records retention requirement. If an email is subject to multiple records retention requirements, it must be archived for the longest applicable period.

5.4.3 Identification and Third Party Contacts

Personnel tasked with system administration responsibilities must ensure that electronic messaging systems are configured to clearly indicate the source of messages sent by way of such systems, and that adequate measures are taken to allow third parties to contact the SOA and resolve issues related to electronic messages.

SOA Internal

5.5. Safeguards

5.5.1 Malicious Software

Personnel tasked with system administration responsibilities must ensure that electronic messaging systems are configured to detect and protect against malicious software transmitted by way of such systems.

5.5.2 Protection and Monitoring

Personnel tasked with system administration responsibilities must ensure that electronic messaging systems are configured appropriately to detect and protect electronic messages from unauthorized access, and to permit authorized monitoring and administration according to SOA policies and procedures.

SOA Internal

Title:	Operations Security	Effective:	2/12/2025
		Last Review:	2/12/2025
		Review Frequency:	Tri-annually
Number:	ISP-165		
Version:	1.02	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To ensure that information security requirements are addressed in the operation of State of Alaska (SOA) information systems.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Operational responsibilities;
- System recovery requirements; and
- Requirements for electronic commerce protections.

5.1. Operational Responsibilities

5.1.1 Documented Operating Procedures

Business Managers must document technical operating procedures to be used by information technology personnel. Business Owners must ensure that such documented procedures are periodically reviewed to ensure appropriateness and to verify that information security requirements, including policy requirements, are addressed.

SOA Internal

5.1.2 Change Management

Business Managers must document substantive changes to information systems and processing facilities and must maintain a record of implementation of these changes.

5.1.3 Segregation of Duties

Executive Management must segregate duties and responsibilities of personnel consistent with the sensitivity of information in order to prevent intentional or unintentional disruption or exposure of information assets.

5.1.4 Separation of Facilities

Business Managers must maintain separate development, test, and production environments for their information systems. In information systems where sensitive information is processed, stored, or transmitted, personnel must not use production data in a test or development environment.

5.1.5 Supporting Utilities

Business Managers must take measures to minimize power and communication equipment disruption to maximize protection of all communication equipment.

5.1.6 Off-Site Equipment

Business Managers must take measures to apply security to off-site equipment. Security measures should specifically address the different risks involved in performing work, storing or transporting equipment to any off-site premises.

5.1.7 Business Information Systems

Executive Management must develop and implement policies and procedures for the purpose of establishing technical and procedural protocols associated with the interconnection of business information systems.

5.2. System Recovery Requirements

5.2.1 Information Backup

Business Managers must ensure that appropriate information backups of critical systems, databases, and information repositories are maintained. Backups must be labeled as per the requirements for data labeling defined within SOA policy ISP-121 Asset Classification and Control.

Business Managers must ensure that backup products and procedures are appropriately tested to ensure that system recoveries are suitable and functional for complete recovery of information assets.

5.3. Requirements for Electronic Commerce Protection

5.3.1 Protection of Electronic Commerce

Business Managers using electronic commerce must ensure transactions with bank cards or other financial account data or information meet or exceed the Payment Card Industry Data Security Standard (PCI DSS), and follow the requirements defined in SOA policies ISP-122 Privacy of Personally Identifiable Information and ISP-167 External Email Encryption.

SOA Internal

Business Managers tasked with operational oversight responsibilities for electronic commerce systems must ensure that appropriate technical and operational controls are in place to protect the organization from fraudulent activity, disputes, or unauthorized access to information and follow the requirements defined in SOA policy ISP-142 Equipment Security.

5.3.2 On-Line Ecommerce Transactions

Business Managers tasked with operational oversight responsibilities for electronic commerce systems must ensure that appropriate technical and operational controls are in place to protect and monitor information during transactions conducted over public or private networks and follow the requirements defined in SOA policies ISP-195 Prohibited Password Protection & Pre-Encrypted Attachments, ISP-112 Third Party Security and ISP-164 Security Monitoring and Logging.

5.3.3 Public Information

Business Managers tasked with operational oversight responsibilities for systems providing data to the public must deploy technical and operational measures to protect the data from unauthorized modification or deletion.

SOA Internal

		Effective:	5/16/2025
		Last Review:	5/16/2025
Title:	Web Filtering	Next Review:	Annually
Number:	ISP-166		
Version:	1.04	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To define the waiver process State of Alaska (SOA) personnel must use to obtain access to otherwise prohibited internet websites when there is a defined business requirement for the exception. Personnel who circumvent the SOA security policies by providing internet access to personnel without waivers are subject to discipline up to and including dismissal. A waiver for one individual cannot be extended to another.

The SOA monitors and filters all web-based traffic to the internet for malicious content and non-business related material to conserve bandwidth, to minimize the cost of conducting SOA business and to provide security to the SOA networks and assets which contain sensitive and/or confidential information.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Prohibited website categories;
- Website filtering waiver form requirements; and
- Website waiver form example.

6. Prohibited Website Categories

Access to certain categories listed below will NOT be granted and are NOT accessible within the SOA networks. All categories and restricted websites may change without prior notice to adapt to evolving SOA business requirements or risk exposure to meet SOA mission and services.

SOA Internal

6.1. Prohibited Categories:

- Entertainment/Recreation
  - Video Streaming
- Information Technology
  - File Host
- Internet Communication
  - Online Chat
  - Other Internet Communication
  - Peer-to-Peer Site
  - Remote Access Tools
  - Webmail
- Adult Material
  - Adult Themes
  - Lingerie/Bikini
  - Nudity
  - Other Adult Material
  - Pornography
  - Sexuality
  - Social Networking Adult
- Religion
  - Alt/New Age
  - Cult
  - Other Religion
  - Traditional Religion
- Drugs
  - Other Drugs
- Gambling
- Sports
- Illegal or Questionable
  - Anonymizer
  - Copyright Infringement
  - Other Illegal or Questionable
- Militancy/Hate and Extremism
- Games
- Society and Lifestyle
  - Social Networking
- Security
  - Other Security
  - Spyware/Adware

To ensure the integrity and security of our network and data, employees are strictly prohibited from accessing or using websites and applications that are commonly associated with malware or other malicious activities. This includes, but is not limited to, sites known for distributing pirated software, illegal streaming services, or those flagged for suspicious behavior by reputable cybersecurity organizations.

7. Website Filtering Waiver Form Requirements

All SOA personnel, who have a defined business requirement for access to websites that are otherwise restricted, must submit a *Web Filtering Waiver Form* for evaluation and approval.

SOA Internal

The departmental specific form can be accessed and printed from the following site:

https://oit-int.alaska.gov/security/web-filtering-and-web-waivers/

Waivers must be approved by the requester's Commissioner or designee. Departments should carefully review the form to ensure that requested categories and/or websites are necessary to the position for which the waiver is requested. If a waiver is requested for a department, division or section, as a whole, the Business Owner will be required to sign the waiver form and will be held accountable for the users for the department, division or section. Each user's IP address and name must be provided.

Requesters may be required to provide additional detail to support the request for web access. Personnel with approved access to certain prohibited categories and the department's IT manager must work directly with the State Security Office (SSO) to determine appropriate methods for alternative Internet access for this individual. Access must only be allowed once the waiver authorization is in place. All participating personnel must provide an original signature on the web waiver filtering form. Waivers are for a specific user or endpoint. Configuring proxies or other shared endpoints for waivered access is prohibited.

Business Owners must ensure their users have read and understand all aspects of SOA policies ISP-166 Web Filtering and ISP-172 Business Use/Acceptable Use prior to submitting a waiver form.

8. Implications of Non-compliance

Violation of this policy is subject to disciplinary action as described in SOA policy ISP-001 Information Security Framework.

SOA Internal

		Effective:	5/16/2025
		Last Review:	5/16/2025
Title:	Identity Management	Next Review:	Tri-annually
Number:	ISP-171		
Version:	1.04	Approved by:	CIO
Pages:	5	Distribution:	SOA

1. Purpose

To ensure a uniform and consistent process for managing user identities and access rights within the State of Alaska (SOA).

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- User accounts;
- User account controls;
- Authentication;
- Account management; and
- Account and access management.

5.1. User Accounts

5.1.1 Unique Identifier (ID)

Personnel tasked with identity management responsibilities must ensure that SOA user accounts are provisioned with a single unique identifier (ID) within all information systems and applications.

SOA Internal

5.1.2 Record of Identifiers

Personnel tasked with identity management responsibilities must maintain a record of all IDs assigned with access to SOA systems, networks, and applications.

5.2. User Account Controls

5.2.1 User Logon Tracking

Personnel tasked with system administration responsibilities must ensure each system is configured such that information about failed logon attempts are presented for verification , when possible.

5.2.2 Limited Attempts

Personnel tasked with system administration responsibilities must ensure that each system is configured to limit the number of logon attempts by a connecting user, and to limit the number of attempts that are made to logon to an individual account as defined in SOA policy ISP-178 Password Management.

5.2.3 Event Logging

Personnel tasked with system administration responsibilities must ensure that each system is configured to log all attempts to access any SOA information systems, whether successful or not.

5.3. Authentication

Authentication for access to State of Alaska resources is required.

5.3.1 Authenticators

Individual authenticators may include, for example, passwords, security tokens, biometrics, certificates, mobile devices, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length, see SOA policy ISP-178 Password Management).

5.3.2 Multi-factor Authentication (MFA)

State information technology solutions shall utilize a multi-factor authentication (MFA) mechanism whenever possible. Personnel must use MFA when the system supports it. Examples of such systems include O365 productivity applications, email, and SOA VPN connectivity. The MFA requirement applies to all remote network connectivity and all State IT devices and solutions. Business managers shall plan, prioritize, and implement remediation to support MFA access. Business owners shall update and adapt business policies and procedures to support this requirement.

5.3.3 Legacy Authentication Protocols

State information technology solutions and services unable to meet current, supported authentication mechanism, such as multi-factor authentication, are prohibited.,. Understanding legacy protocols are in use, Business managers shall prioritize, plan, and complete remediation of existing systems that use such protocols. All new solutions and services must be compliant with support for current, supported authentication mechanisms.

SOA Internal

5.4. Account Management

5.4.1 Account Registration Requests

Personnel tasked with identity management responsibilities must use a formal request process for all access requests (e.g., additions, changes, or deletions) to SOA systems, networks, or applications.

5.4.2 Status Notification

Business managers must ensure that prompt notice is provided to personnel tasked with network user administration whenever a change in an individual's status (e.g., hiring, termination, reassignment) requires a change in user privileges. Personnel tasked with network user administration must ensure that changes to user privileges are promptly and consistently applied across systems.

5.4.3 Changing and Disabling/Removing User Accounts

Upon notice of termination, personnel tasked with identity management responsibilities must promptly disable or remove the user accounts of terminated individuals, and must promptly review and appropriately update the access rights of personnel who change job responsibilities.

5.4.4 Authorized Access Only

Personnel tasked with identity management responsibilities must ensure that all user accounts for SOA systems, networks, or applications meet the following criteria:

- User accounts to SOA systems, networks, or applications must be authorized by a designated Data Owner;
- User access to SOA systems, networks, or applications must be based on a business need related to the user's duties; and
- Users must acknowledge rules of behavior for system access when required.

5.4.5 Administrative Access Accounts

Personnel tasked with identity management responsibilities must ensure that administrative access to SOA systems, networks, or applications meet the following minimum requirements:

- Personnel with identity management responsibility must maintain a record of personnel with administrative access to SOA systems, networks, or applications;
- Personnel with identity management responsibility must assign administrative access only when such access is required for business requirements;
- Personnel with identity management responsibility must configure access to administrative accounts in such a way as to allow for an audit log indicating which individuals have used an administrative account; and
- Personnel with identity management responsibility must regularly review access rights to administrative accounts.

5.4.6 Review of User Account Access

Personnel tasked with system administration responsibilities must review users' access rights to systems on a regular basis for accuracy.

5.5. Account and Access Management

5.5.1 Role Based Access Control

Personnel tasked with system administration responsibilities must ensure that all system and

SOA Internal

application user accounts incorporate role based access control, where possible, in order to restrict access to authorized users and uses only.

SOA Internal

5.5.2 Third-Party Accounts

Personnel tasked with network user administration must ensure that each third-party account is configured to provide access to only systems, applications, and information that is required for each third party's responsibilities. Third-party access to sensitive information is only permitted when required and in accordance with applicable laws, regulations, and SOA policies. Third-party access must be reviewed and re-approved, at least, annually.

SOA Internal

1. Purpose

To outline acceptable use and clarify the protection of State of Alaska (SOA) information assets and technology resources. Unacceptable use exposes SOA to unwarranted risk (e.g., virus attacks, compromised network systems, services and legal issues associated with data tampering, data theft and privacy).

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Acceptable Use and Rules of Behavior.

5.1. Acceptable Use and Rules of Behavior

5.1.1 Access for Authorized Purposes

Acceptable use applies to all personnel (e.g., employees, partners, contractors, consultants, temporaries, other SOA workers and workers affiliated with third parties or anyone having access to SOA information that is not directly accessible to the general public from a non-SOA network). This also applies to the use of information processing equipment and services, including but not limited to computer equipment, software, operating system, storage media, email, internet, file transfer protocol (FTP), smartphones, etc. and further

SOA Internal

applies to resources owned, leased, or managed by SOA or its designees and to non-SOA resources used at SOA facilities in the conduct of SOA business.

Personnel must use SOA networks and associated systems for authorized business purposes only. Personnel must not access information, programs, or systems when such access is not required for an authorized business purpose. This includes system administrators who must have system access rights due to their job responsibilities.

Administrators must not view or otherwise access SOA user information without the express consent of the user, Executive Management or the Division of Personnel and Labor Relations (DOPLR).

SSO personnel will monitor equipment, systems, and network traffic at any time, for the purpose of security and network maintenance.

5.1.2 State Managed Computing Equipment and Applications Access

Personnel must use state managed computing equipment or state managed applications for SOA business. Equipment and applications used for SOA business are subject to monitoring, collection, public records request and enforcement.

5.1.3 Contractors Computing Equipment Authorization

Contractors may use their personal or company owned devices within the SOA WAN or LANs, but these devices must be subject to all SOA policies when connecting to the SOA networks and will be monitored, reported and audited for security proposes. Contractors forfeit any right to privacy.

Contractors who connect personal or company owned devices to the SOA network acknowledge that all materials and information on each device are subject to monitoring, review, collection and public disclosure by State or federal statute, regulations, administrative order, policy or directive.

5.1.4 Application of Passwords

Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed regularly. Personnel must use passwords of strength, specific criteria and control to access and protect the SOA WAN and LANs and must adhere to what is defined in SOA policy ISP-178 Password Management.

With the exception of public-access terminals or by SOA SSO written authorization, all non-mainframe computers (e.g., servers, workstations, terminals and laptop computers) must be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less. When personnel leave a computer unattended this password-protected screensaver feature must be manually activated or the computer must be turned off.

5.1.5 Posting of SOA Sponsored Accounts

SOA sponsored accounts to news groups or web forums shall contain a disclaimer which states the opinions expressed are strictly the poster's own and not necessarily those of the SOA, unless posting is in the course of business duties.

5.1.6 Use of Issued Credentials

Personnel must use only the user IDs, network addresses, and network connections defined by the SOA or department information technology administration staff to access SOA networks and associated systems.

SOA Internal

5.1.7 Unauthorized Security Tools

Personnel must not download, install, or execute any security program or utility (e.g., password cracker, network sniffer, vulnerability scanner) designed to reveal weaknesses in the security of a system without explicit authorization from the State Security Office (SSO).

5.1.8 Records in the Cloud are State Records

All state records may be subject to review and disclosure in the context of litigation, investigations, and responses to Alaska Public Records Act requests.

You must retain all state records residing in cloud services, such as M365, as required by any applicable state records retention schedule, if the schedule requires retention for longer than one year. Emails must be saved according to the State's email retention policy. If you must retain any other state record for longer than one year, save it in your agency's electronic system or hard-copy file as your agency requires. If you do not know the records retention requirements that apply to your records, contact your supervisor, agency's records officer, or the Alaska State Archives Records & Information Management Service.

5.1.9 Execution of Electronic Information

Personnel must use extreme caution when opening files that have been sent to or received either electronically or on removable media (e.g., floppy disk, CD/DVD, USB Flash drive). Examples of such files are email attachments received from unknown senders, files downloaded from the www or FTP sites, seemingly innocuous commercial files, etc. Any and all of these items can contain viruses, e-mail bombs, trojan-horse code, spyware/ad-ware, BOT net, other malware, or inappropriate material and should be suspected. If personnel experience unusual computer symptoms when opening unknown files, they must report these to their department IT staff immediately. If contractors with SOA business suspect any of the above listed items they shall disconnect from SOA network and notify their client supervisor immediately for remediation in all efforts to protect SOA information assets.

5.1.10 Unacceptable Use

Under no circumstances are personnel of the SOA authorized to engage in any activity that is illegal or in violation of local, State, federal or international law, or Alaska Administrative Code.

Prohibited email, communication activities, system and network activities are listed below. Personnel may be exempted from some of these restrictions during the course of their valid job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services or the requirement of a law enforcement investigation) however, cautious and meticulous adherence must be followed by all users.

5.1.10.1 E-mail and Communications Prohibited Activities

- Any illegal activity.
- Intentionally sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
- Any form of harassment via email, instant messaging, telephone, paging, or other electronic means, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

SOA Internal

- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within SOA networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SOA or connected via the State's network.
- Posting the same or similar non-business-related messages to Usenet news groups or web forums.
- Use for access to or distribution of indecent or obscene material, including child pornography.
- Use for commercial activities, including advertising, unless specific to charter, mission, or duties of the government agency.
- Use for fundraising, political campaign or partisan activities, or public relations activities not specifically related to SOA government activities.
- Use of SOA information technology resources for personal gain.

5.1.10.2 System and Network Prohibited Activities:

- Violations of the rights of any person or company protected by copyright “©”, or trade mark “™” or registered “®”, or trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the SOA.
- Unauthorized copying of Copyright Material “©” including, but not limited to, digitization and distribution of photographs from magazines, books or other copyright sources, copyright music, and the installation of any copyright software for which the SOA or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Intentional introduction of malicious programs into SOA information technology resources (e.g., introducing viruses, worms, Trojan horses, e-mail bombs, etc. into the SOA network or individual SOA computing devices).
- Revealing SOA account information to others or allowing use of SOA assigned accounts by others. This includes family and other household members when work is being done at home.
- Using SOA computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any SOA account.
- Intentionally causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forging route information for malicious purposes.
- Network vulnerability testing, security scanning, virus or Trojan horse testing or executing any form of network monitoring, which will intercept data not intended for the user's host.
- Any activity, application or service that disables, tampers with, circumvents security solutions, services, controls, user authentication, security of any host, network or account, or interfering with or denying service to any authorized user or service is prohibited and strictly enforced. (e.g., URL filtering, network monitoring, remote access requirements through SOA virtual private network, SOA ingress/egress access control requirements, enterprise endpoint security solution, and other security

SOA Internal

solution, service, or control, intentionally evading a security solution or process, or creating a denial of service to a user, applications, host, network, or other SOA process).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable another user's terminal session via any means, locally or via the Internet/intranet/extranet.
- Providing information about or lists of SOA personnel to any outside parties, without a business case or SSO approval.
- Personal use of or divulging of private or confidential information regarding any individual obtained by any personnel, as a result of performance of job duties or as a result of their employment with the SOA.
- Use of non-enterprise supported encryption (at rest or in transit).
- Uses of peer-to-peer (P2P) file transfer solutions.
- Use of non-enterprise provided instant messaging technologies.
- Use of non-standard remote control technologies or other similar technologies.
- Use of non-operating system standard screen saver or other similar technologies.
- Use of any external proxy systems or other similar technologies.
- Use of any non-enterprise program or application that performs off-site document or file indexing.
- Use of any streaming media technologies for non-business purposes.

5.1.11 Least Privilege

Personnel tasked with network user administration must ensure that network and system access controls are configured to limit the privileges extended to users to the least necessary to accomplish authorized business purposes.

5.1.12 Need to Know

Personnel who have access to data are prohibited from perusing data unrelated to assigned tasks or projects.

5.1.13 Applicable Statutes and Enforcement

The Executive Branch Ethics Act states a public employee may not "**use state time, property, equipment, or other facilities to benefit personal or financial interests**" (AS 39.52.120(b)(3)). Further, "standards of ethical conduct for members of the executive branch need to distinguish between those minor and inconsequential conflicts ... and those conflicts of interests that are substantial and material." (AS 39.52.110(a)(3)).

The Executive Management acknowledges that incidental personal use may be unavoidable in today’s electronic environment. In cases where SOA office technology incidental personal use occurs, users must be aware that there is no right to privacy regarding these occurrences. Applicable Statutes, Administrative Orders and Codes include, but are not limited to: AS 39.52, Alaska Executive Branch Ethics Act; Administrative Order #81, Nondiscrimination and Non-Harassment; Administrative Code 9 AAC 52, Alaska Executive Branch Code of Ethics; AS 39.25.160, Alaska Little Hatch Act; AS 24.60, Legislature Standards of Conduct.

Personnel found to have violated this policy are subject to discipline up to and including dismissal.

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Network Security	Next Review:	Per Policy
Number:	ISP-173		
Version:	1.02	Approved by:	CIO
Pages	6	Distribution:	SOA

1. Purpose

To ensure the networks and workstations operated by the State of Alaska (SOA) provide a secure foundation for business applications.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Network management;
- Network systems;
- Network audits;
- Network design; and
- Network security.

5.1. Network Management

5.1.1 Network Operations

Personnel must protect and secure the operation of SOA networks in a manner appropriate to the sensitivity of the electronic information traversing those networks. Personnel must not purchase or deploy firewalls or other network security solution without the approval of the State Security Office (SSO) as defined in SOA policy ISP-179 Firewall Use.

SOA Internal

5.1.2 Changes to Architecture

SOA network architecture is planned, coordinated, implemented, and maintained by the OIT. Personnel must not make changes to this architecture without approval from and coordination with OIT and technology management personnel.

5.1.3 Business Traffic

Personnel must use SOA networks only for approved business purposes. Non-business use of network resources is strictly prohibited.

5.1.4 Use of Authorized Tools

Personnel tasked with network management, such as the remote administration and gathering of information about network devices and border controls, must use only approved tools and procedures. Personnel must not install or configure unapproved network management tools, or utilize unapproved protocols, to access or gather electronic information from networks, network devices, or computer systems without the approval of the SSO.

5.1.5 Authentication Required

Personnel tasked with network management must ensure that each networked system is configured such that it does not permit unauthorized access to itself or SOA networks. Personnel must not configure a networked system such that it permits anonymous access to the system, except to the extent that such access is required for an authorized purpose. (e.g., FTPS services or general public web pages or other general public accessible service).

5.1.6 Authority of Domain Name Services

Personnel must not configure external network services to respond authoritatively for SOA network services; for example, personnel must not configure Domain Name Servers (DNS) to send referrals directly to root level queries or configure email servers outside of those maintained centrally by SOA. Departments must not configure their DNS to send referrals directly to the Internet for DNS root level queries. Personnel must ensure that all external-facing services are configured to utilize the SOA centralized demilitarized zone (DMZ) infrastructure as a gateway or chokepoint. OIT will pro-actively maintain primary DNS servers at the latest secure operating system and service level available to ensure the security of DNSs for the entire state network.

5.1.7 All DNS Configured to OIT

All DNS connected to SOA internal Local Area Network and Wide Area Network (LAN/WAN) infrastructure must be configured to use OIT DNS servers as forwarders.

5.2. Networked Systems

5.2.1 No Unauthorized Devices

Personnel must not attach a device, computer system, or network to SOA networks without explicit authorization. Attached devices must adhere to and comply with published, CIO approved standards and State policies.

SOA Internal

5.2.2 Business Purposes

Personnel tasked with network management must ensure that each networked system is configured such that it does not provide network services or permit network connections that are not required for a business purpose.

5.2.3 Approved Systems for Remote Access

Personnel must use only SSO approved systems, software, and networks to remotely connect to SOA networks.

5.3. Network Audits

5.3.1 Audits, Tests and Scans

Network security auditing, testing and scanning must have prior approval by the SSO. Personnel must not conduct, nor allow to be conducted, a network attack or penetration test by any internal or external party without the explicit approval of the SSO.

5.3.2 Regular Security Perimeter Testing

SSO must ensure that periodic network security scans of systems that process, transmit, or store sensitive information are performed by an authorized party, no less than annually, to detect vulnerabilities or control weaknesses that will expose such electronic information. SSO must review and maintain the results of each scan, and must ensure that any issues identified are handled in accordance with SOA policies and applicable laws, regulations, and standards.

5.4. Network Design

5.4.1 Logical Borders

SOA network is defined by its logical borders, which are planned, implemented, and maintained by OIT staff. Personnel must not extend or open this border without approval from and coordination with SSO.

5.4.2 Ingress/Egress

To receive approval for ingress and egress access permission, modification exposing any service, system or network to external environment, service, system or network a department must complete a security plan as referenced in ISP-162: System Planning and Acceptance. and submit it to the SSO for authorization as defined in SOA policy ISP-191 Security in Systems Development.

- Ingress/Egress points will not be established outside the State's Enterprise DMZ environments;
- Ingress/Egress environments will consist of a multi-layer architecture that provides clear separation between the bastion host environment and the SOA Internal networks or services.
- Architecture must include Stateful Packet Inspection (SPI) of inbound and outbound traffic from bastion host environment and external networks and the SOA intranet environment.
- The architecture must include firewall technology separation between bastion host, external and internal (intranet) environments.

SOA Internal

- The architecture must include intrusion prevention and/or intrusion detection solutions on both the inside and outside of all interfaces of the firewall.
- The architecture must include logging solutions on all interfaces and devices that are complaint with state policy;
- All network traffic must pass through at least two separate sets of firewalls and traffic must be monitored in real-time for possible intrusions or threats
- All network, system, service, application, appliances, or other devices within an Ingress/Egress environment must report to a security event correlation solution.
- All ingress/egress environments will support application and user proxies.
- All ingress/egress with any availability to the internet, or other non-soa business environment, will actively utilize Web Filtering technology to help ensure user access is only for state business purposes.
- All ingress/egress environments will log and report to SSO specified logging devices or solutions.
- The SSO will be provided read-only access to all ingress/egress environments and all devices supporting environment for the purposed of ensuring security.

5.4.3 Network Segmentation

Personnel tasked with network management must segment SOA networks to ensure that risks from exposure and operations in different environments are not shared with other environments that do not have appropriate controls to mitigate those risks. This network segmentation must not obscure or obstruct SPI from the WAN by OIT networking or the SSO.

5.4.4 External Networks

Personnel tasked with network management must segment any externally-exposed network, such as those connected to the public Internet, using a firewall. Whenever possible, personnel tasked with network management must segment systems by risk, so that systems at a higher risk of compromise do not pose an additional threat as an attack platform to systems with more sensitive electronic information.

5.4.5 Internal Networks

Personnel tasked with network management will segment internal department data center networks behind a firewall in order to segregate systems and data by sensitivity (e.g., human resources systems) upon the approval of the SSO. Personnel tasked with network management must also segment internal department data center networks by system status, such that production systems are protected and isolated from those used for development and testing. Internal networks must be segregated with a security device and have SPI on all traffic.

Note: Firewalls, encryption or other security related solutions will not be used within local LAN environments or used to obscure or obstruct the view of packets within any wide or local area networks from OIT networking or the SSO.

5.4.6 Wireless Network

Personnel tasked with network management must segment all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.), including any form of wireless communication device capable of transmitting packet electronic information, connected to any SOA internal networks behind a firewall. State wireless access points must be compliant with the security requirements defined by the SSO.

SOA Internal

5.4.7 User Authentication for Connections

Personnel tasked with network management must ensure that appropriate authentication methods are in place to control access to services by remote users.

5.4.8 Remote Diagnostic and Configuration Port Protection

Personnel tasked with network management must ensure that physical and logical access to diagnostic and configuration ports is appropriately controlled.

5.4.9 Limitations on Connection Time

Personnel tasked with network management must ensure that high-risk applications appropriately maintain limitations on connection time.

5.5. Network Security

5.5.1 Dedicated Security Mechanisms

Personnel tasked with network administration must ensure that security devices (e.g., firewalls, intrusion detection systems, perimeter routers) do not have other services installed on them that might impede or compromise their security functionality.

5.5.2 Firewalls

Personnel tasked with network administration must ensure that firewall devices, in concurrence with SOA policy ISP-179 Firewall Use, are configured to incorporate the following:

- Any service that is not explicitly permitted must be denied, for both inbound and outbound traffic,
- All permitted services must be approved by the SSO;
- SSO must approve services as restrictively as possible based on business requirements;
- Firewall must be configured to generate audit logs;
- Firewall must include the ability to perform stateful inspection and threat detection of all packets; and
- All changes to a firewall must be assessed and approved by the SSO.

5.5.3 Security Devices

Personnel tasked with network management must ensure the deployment of department security solutions do not segment, obscure, obstruct, or impede the view of the network traffic or local area networked devices or create additional cost or resource impacts to the SSO or OIT networking personnel.

5.5.4 Virtual Private Network (VPN)

Personnel tasked with network administration must ensure that remote access is restricted to only pre-approved individuals, and that such access is permitted only using an approved VPN device. All VPN solutions must be approved by the SSO and be in the SOA DMZ enterprise environment.

SOA Internal

5.5.5 Prevent Unauthorized View or Access

Personnel must not configure devices for dial-up (e.g., modem) access to SOA networks or systems without SSO approval. The SSO, in coordination with the department information security officers (ISO), must ensure that any remote access solution used by a vendor to access a system for support or maintenance purposes is configured to have the least access necessary, and their access is in compliance with SOA policies, statutes, regulations, and standards; including, if applicable, two-factor authentication for remote network access.

5.5.6 Configure Network Time Protocol (NTP) - Date and Time Synchronization

Personnel tasked with system administration responsibilities must configure the use of the OIT NTP server to establish the date and time for any system, service, or network. This process synchronizes the date and time of information systems and is critical to establish events and log information that can be correlated between disparate information systems to support incident detection, forensic investigations, and other related requirements. All system, services, or networks must reflect the Alaska Time Zone.

5.5.7 SOA Minimum Security Requirements

SOA minimum security requirements and features sets must be followed for network routers, switches, firewalls and VPN solutions. Security standards and configuration procedures applied to network technologies and infrastructure must be approved by the SSO and align with ISP 173, along with other relevant ISP guidelines, and must be compatible with current OIT standards for equipment and network infrastructure before subject devices are connected to the WAN.

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Operating Systems Security	Next Review:	Per Policy
Number:	ISP-174		
Version:	1.02	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To ensure workstations, servers and other State of Alaska (SOA) information systems are deployed using a documented, reproducible, and secure configuration.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Configuration and deployment of information systems;
- User authentication and access control;
- Systems utilities;
- Connection time; and
- Configuring Network Time Protocol (NTP).

5.1. Configuration and Deployment

5.1.1 Documented Configuration

Personnel tasked with duties related to the configuration, deployment, and maintenance of information systems (e.g., workstations, servers, networks) must develop and document a standard baseline configuration (i.e., "build") for each operating system platform based on information security "best practices", as defined by best practices entities seen in National Institute of Standards and Technology (NIST.gov), and/or Center for Internet Security (CISECURITY.org), and/or Defense Information System Agency (DISA.mil). Unless otherwise approved by the SSO all SOA infrastructure will be harden to standards as provided by Center for Internet Security (cisecurity.org).

SOA Internal

5.1.2 Configuration Deployment

Personnel tasked with duties related to the configuration, deployment, and maintenance of information systems must ensure that the documented standard configuration is applied when information systems are deployed.

5.1.3 Evaluation of Secure Configuration

The State Security Office (SSO) must review documented configuration standards to ensure that appropriate safeguards and hardening are applied in accordance with this and other SOA policies, procedures or standards.

5.2. User Authentication and Access Control

5.2.1 Logon Procedures

Personnel tasked with duties related to the configuration, deployment, and maintenance of information systems must ensure that logon procedures are implemented to restrict system access to authorized individuals only.

5.2.2 User Identification and Authentication

Personnel tasked with duties related to the configuration, deployment, and maintenance of information systems must ensure that secure system logon, individual user authentication, and resource access controls are implemented in each operating system configuration.

5.3. System Utilities

5.3.1 Use of System Utilities

Personnel tasked with duties related to the configuration, deployment, and maintenance of information systems must ensure that utilities capable of overriding system and application security parameters are controlled and that only approved administrators have access.

5.3.2 Secure System and Application Parameters, Configurations and Settings

Personnel tasked with duties related to the configuration, deployment, and maintenance of information systems must ensure that security hardening is performed on system and application parameters, configurations and settings. The SSO must provide personnel tasked with duties related to configuration with an approved list of hardening utilities or configuration settings.

5.4. Connection Time

5.4.1 Session Timeout

Personnel tasked with duties related to the configuration, deployment, and maintenance of information systems must ensure that user sessions expire and that the connection to system resources is discontinued after a defined period of inactivity.

5.5. Configure Network Time Protocol (NTP) - Date and Time Synchronization

All system, services, or networks must reflect the Alaska Time Zone as defined in SOA policy ISP-173 Network Security, § 5.5.6.

SOA Internal

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Mobile Computing and Remote Access	Next Review:	Per Policy
Number:	ISP-175		
Version:	1.02	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To ensure that appropriate technical and operational controls are implemented when mobile computing devices or remote access connections are used to store, process, or transmit State of Alaska (SOA) information.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy defines requirements for:

- Mobile computing devices;
- Remote access; and
- Secure configuration.

5.1. Mobile Computing Devices

5.1.1 Authorized Use of Mobile Devices

Personnel must not store, process, or transmit sensitive SOA information using a mobile computing device (e.g., laptop, portable PC, smart phones, tablets, IOT-devices) which is not approved for use by Executive Management. Personnel must not connect an unapproved mobile computing device to any SOA computer or network. Personnel must not share access to an approved mobile computing device with any individual not authorized by Executive Management to use the device.

SOA Internal

5.1.2 Technical Safeguards

Personnel must ensure that the safeguards required by SOA policy for information systems (e.g., disk encryption, password protection, and use of VPN) are employed for mobile computing devices that process, store, or transmit sensitive SOA information.

5.1.3 Prevention of Unauthorized Viewing

When using a mobile computing device in a public location, personnel must ensure that unauthorized individuals cannot view sensitive SOA information.

5.1.4 Physical Safeguards for Sensitive Information

Personnel must protect mobile computing devices from loss or theft by keeping such devices within their possession whenever possible, and by locking or securely storing such devices when not in their possession.

5.2. Remote Access

5.2.1 Authorized Use or Remote Access Technologies

Personnel must not use a computing device that has not been approved for use by Executive Management to remotely access an SOA information system (i.e., from a network not controlled by SOA). Personnel must only use methods approved by the State Security Office (e.g., SOA Enterprise VPN and DMZ environment) to access SOA information systems.

5.2.2 Multiple Network Connections

Personnel must not connect a computing device used for remote (or other) access to two networks simultaneously. Split-tunnel network connections are not permitted.

5.2.3 Physical Protection

Personnel must ensure that portable and offsite computers used for remote access are protected against physical theft or damage.

5.2.4 Logical Protection

Personnel tasked with information technology management must ensure that portable and offsite computers used for remote access to SOA networks or internal services have technical or physical controls applied to protect against unauthorized access, information theft, or malicious monitoring (e.g., encryption, hardening, device secured to non-movable object, no administrative (leveled) privilege user accounts, remote wipe, GPS locator services, or other technological methods of securing devices).

SOA Internal

5.3. Secure Configuration

5.3.1 Security Software and Network Protection

Personnel tasked with system administration responsibilities must ensure that mobile computing devices and devices used to remotely access SOA (State Office of Administration) computers and networks adhere to the following security guidelines.

5.3.1.1 Antivirus on Endpoints

All mobile workstations and remote endpoints must have anti-virus enabled at all times. This includes situations where personnel are working remotely or using mobile hotspots.

5.3.1.2 Firewalls on Endpoints

All mobile workstations and remote endpoints must have firewalls enabled at all times. This includes situations where personnel are working remotely or using mobile hotspots.

Disabling of endpoint firewalls should only be performed for limited testing, and behind a network firewall device or other compensating control. At no time shall a workstation firewall be disabled while publicly facing.

5.3.1.3 Network Firewall Protection for Workstations

Personnel should ensure that workstations have an additional layer of protection in the form of network firewall devices, such as consumer firewall-routers.

These network firewalls provide an added level of security by filtering incoming and outgoing traffic at the network perimeter. They help prevent unauthorized access and protect workstations from external threats.

5.3.1.4 Mobile Hotspot Configuration

Most mobile hot spots provide basic measures preventing attached endpoints from direct exposure to public facing internet.

When using a mobile hotspot, personnel must avoid configuring it in a way that directly exposes a device to the public internet.

5.3.2 Remote Access Systems Control

Personnel tasked with network administration responsibilities must ensure that remote access systems are implemented such that they require authentication and encryption that meet the Federal Information Processing Standards (e.g., FIPS 140-2), and access controls in accordance with this and other SOA information security policies.

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Application Lifecycle Management	Next Review:	Per policy
Number:	ISP-176		
Version:	1.2	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure that an appropriate level of security is in place for applications developed, administered, or otherwise in use by the State of Alaska (SOA).

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Security review; and
- Application planning and acceptance.

5.1. Security Review

5.1.1 Requirement for Application Security Review

The State Security Office (SSO) and Information Security Officers (ISO) must conduct a technical security review of all applications developed, purchased, licensed, or otherwise acquired for the purpose of storing, processing, or transmitting sensitive information assets.

5.1.2 Security Review Criteria

Business managers, with the SSO, must establish and maintain baseline application security controls and security architecture specifications for applications, and must employ the baseline and specifications in a formal review of information security for each application.

SOA Internal

This baseline must be determined by using best practices entities such as the National Institute of Standards and Technology (NIST.gov), Open Web Application Security Project (OWASP.org) and others.

5.2. Application Planning and Acceptance

5.2.1 Incorporation of Controls

Business management must incorporate information security requirements and controls throughout all phases of the deployment and maintenance lifecycle for new applications as well as for applications undergoing major revisions.

SOA Internal

		Effective:	7/1/2017
		Last Review:	7/1/2017
Title:	Wireless Network Security	Next Review:	Annually
Number:	ISP-177		
Version:	1.0	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To ensure that proper security controls are implemented when wireless networking technology is used to access State of Alaska (SOA) information.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to all SOA branches, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Wireless connections;
- Secure configuration of wireless devices;
- Secure configuration of wireless networks; and
- Secure monitoring.

5.1. Wireless Connections

5.1.1 No Wireless Connections without Authorization

Personnel shall not connect a wireless networking device to an SOA computer or network without explicit approval from a Business Owner. Personnel shall not access an SOA computer or network by way of an unauthorized wireless networking device.

SOA Internal

5.1.2 No Sensitive Transmissions without Safeguards

Personnel shall not transmit sensitive data over a wireless network, including a public wireless network (i.e., a “wireless hot spot”) or a home network, unless approved wireless configuration settings and protocols, including approved encryption, are used.

5.1.3 Multiple Network Connections

Personnel shall not connect a computing device with an approved wireless network component to two networks simultaneously. Split-tunneled network connections are not permitted.

5.2. Secure Configuration of Wireless Devices

5.2.1 Disable Unapproved Wireless Components

Personnel tasked with system administration responsibilities shall disable any wireless network component that is installed in an SOA computing device but is not approved for use.

5.2.2 Standardized Configuration

Personnel tasked with system administration responsibilities shall ensure that any wireless network component authorized for use is configured according to standards approved by the Technology Management Council (TMC).

5.3. Secure Configuration of Wireless Networks

5.3.1 Authentication

Personnel tasked with network administration responsibilities shall ensure that approved wireless implementations support and employ strong authentication (e.g., TACACS+, RADIUS) to restrict access to SOA wireless networks to authorized users only.

5.3.2 Device Access Controls

Personnel tasked with network administration responsibilities shall ensure that approved wireless implementations support and employ the capability to limit access to authorized devices only (e.g., by use of MAC address access control lists).

5.3.3 Network Identification

Personnel tasked with network administration responsibilities shall ensure that approved wireless implementations are configured such that the network name or ID (e.g., 802.11 Service Set Identifier (SSID)) does not include information that may be deemed valuable to a potential attacker.

5.3.4 Network Segmentation

Personnel tasked with network administration responsibilities shall ensure that approved wireless implementations are segmented from wired networks by use of a Stateful Packet Inspection (SPI) firewall.

SOA Internal

5.3.5 Physical Configuration

Personnel tasked with network administration responsibilities shall ensure that approved wireless implementations are configured such that emanations beyond SOA facilities are minimized, and that wireless network devices are installed in locations that are protected from unauthorized physical access.

5.4. Security Monitoring

5.4.1 Wireless Network Surveys

Personnel tasked with security and compliance monitoring responsibilities shall regularly survey SOA facilities to ensure that unauthorized wireless networking devices are not in use.

5.4.2 Use of Wireless Security Tools

Personnel shall not use software or hardware designed to test or evaluate wireless network security, or to capture wireless network traffic, without the explicit permission of the CSO.

SOA Internal

		Effective:	12/19/2025
		Last Review:	12/19/2025
Title:	Firewalls	Next Review:	Bi-annually
Number:	ISP-179		
Version:	1.02	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To establish requirements for firewalls in the State of Alaska (SOA) wide area network (WAN) system and prohibit the Departments from implementation of firewalls without proper coordination with the State Security Office (SSO). All external facing SOA servers must be protected by firewalls in a Demilitarized Zone (DMZ) to ensure security of SOA internet and internal networks.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Firewall Requirements; and
- Department Specific Firewall Requirements.

5.1. Firewall Requirements

5.1.1 Office of Information Technology (OIT) Ownership of All Enterprise Firewalls

OIT must retain ownership of all enterprise firewalls within the State's wide area network (WAN) and Departments, except for specific firewalls required by federal regulation, for which the SSO may provide an MOU for the management control or shared access of such firewalls. The SSO must approve all enterprise firewall configurations and changes.

SOA Internal

5.1.2 Intrusion Detection System (IDS)/Intrusion Protection System (IPS) on Internal and External Interface

IDS/IPS solutions must be installed and operated on both the internal and external interfaces for all firewalls. Logging of all IDS/IPS solutions must be performed at the enterprise level and sent to the SSO's enterprise logging solutions.

5.1.3 Network Address Translation (NAT) & Port Address Translation (PAT)

SOA IP scheme must be used whenever possible. NAT or PAT solutions are prohibited unless they are approved and documented by the SSO.

5.1.4 Firewalls Must Not Impede View, Operational Tools or Service of the SSO and OIT

No firewall will be deployed that adversely affects the SSO's solutions or proposed solutions for the management, monitoring, auditing, logging, or reporting within the SOA WAN or Local Area Network (LAN) environments. The SSO must evaluate all firewall requests on a case-by-case basis for adverse effects.

5.1.5 Firewalls Log to Enterprise Solutions

All firewalls within SOA environments must log to the SSO enterprise logging solutions. The SSO will provide Departments with the required information necessary to complete this requirement during the implementation phase of approved firewalls.

5.1.6 Firewalls Ensure Incorporation into Security Operation Center Services

All firewalls must be incorporated within the Enterprise Security Operation Center Services.

5.1.7 Firewalls Compliant with SOA Standards

All firewall solutions must be compliant with SOA governance standards for hardware and software.

5.2. Department Specific Firewall Requirements

5.2.1 Firewalls are Prohibited within Departments

Firewalls are prohibited within Departments local area network (LAN) environments. Firewalls may be deployed within a Department main data center environment, in compliance with SOA policies. For Departments to purchase or deploy a firewall within their department, written authorization from the SSO is required. Requestors are required to provide a business justification for all requests.

5.2.2 Department Firewall Requests

No firewall solution requests will be accepted for the purposes of, or which have the effect of, performing unauthorized isolation within the State's combined network infrastructure (WAN/LAN environments). Departments can ONLY obtain data center firewalls. LAN or Host based requests will NOT be authorized or accepted.

SOA Internal

5.2.3 Department Firewall Costs

Departments assume all costs for the operation and management of the entire infrastructure that is used to support a department firewall. These costs must include all equipment, licensing, network bandwidth and systems utilization, managing, maintenance, monitoring, reporting, logging and training costs at a minimum. Full burden costs will be developed by the SSO, once a solution request has been initially approved..

SOA Internal

		Effective:	8/20/2024
		Last Review:	8/20/2024
Title:	Security in System Development	Next Review:	Per policy
Number:	ISP-191		
Version:	1.03	Approved by:	CIO
Pages	4	Distribution:	SOA

1. Purpose

To define security criteria for systems and software purchased for or developed by the State of Alaska (SOA) and describe the security requirements related to planning, evaluating, implementing, and maintaining those systems and software.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP 002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- System planning;
- Software development and implementation;
- System awareness;
- System testing;
- System acceptance; and
- Secure system build.

5.1. System Planning

5.1.1 Implementing System and Networks

Personnel must not install servers, add services, connect networks, or otherwise implement systems onto or within existing SOA systems or networks without the specific approval of Executive Management.

SOA Internal

5.1.2 System Configuration

Personnel tasked with the configuration of servers, personal computers, mobile devices, firewalls, network equipment, and other computing devices must configure those systems according to security requirements specified by the State Security Office (SSO) and Executive Management.

5.1.3 Production Development Lifecycle

Business Managers must define a formal lifecycle for each production system, defining the system build process, testing and staging plan, implementation plan, maintenance plan, security plan, disaster recovery plan, continuity of operations plan and expectation for system retirement. Security, Disaster Recovery and Continuity of Operations plans can be a combined plan.

5.1.4 Production Systems Documentation

Personnel tasked with developing or implementing production software or hardware systems must clearly document those systems prior to deployment. Appropriate design documentation including detailed network diagrams, software architecture, and data flow diagrams must be submitted to all appropriate entities, which include Department Management, ETS, SSO, Technology Management Council (TMC), for approval prior to development.

5.1.5 Production Systems Segregation

Personnel tasked with network administration responsibilities must ensure that production systems are physically segregated from development environments through the use of firewalls and must follow the requirements as defined in SOA policy ISP-179 Firewall Use.

5.2. Software Development and Implementation

5.2.1 Software & System Development Lifecycle

Personnel tasked with the development of software must comply with documented SOA coding standards, applicable State policies and procedures, and other applicable laws, regulations, and standards.

Personnel must not develop software, scripts, or queries that handle sensitive or critical information without the approval of the applicable Information Owner, and must follow the additional requirements of this policy and SOA change control processes.

5.2.2 Software Security Feature

Personnel tasked with the development or implementation of software must ensure that appropriate security features, including preventing the display of sensitive information to unauthorized individuals, are included in any software acquired by or developed for the SOA.

5.2.3 Source Code Protection

Personnel tasked with the development of software must ensure that the source code of information systems is safeguarded and access to such source code is limited to only personnel with a legitimate business requirement.

SOA Internal

5.2.4 Third Party Development

When third party developers are involved in the development of information systems for the SOA, personnel responsible for the management of third party developers must ensure that the development is adequately supervised and monitored. All third party development must comply with State and federal, statutory, regulatory, administrative orders, policies, procedures, standards and directives and follow the requirements as defined in SOA policy ISP-112 Third Party Security.

5.3. Security Awareness

5.3.1 Security Coding and Best Practices

The Department Information Security Officers (ISO) must ensure that personnel responsible for implementing or developing software receive training, at least annually, with respect to security and coding best practices.

5.4. Security Testing

5.4.1 Software Security Testing

Personnel tasked with software release and change management responsibilities must review and test new or changed software to assess software security levels prior to deployment in the SOA system.

5.4.2 Test Data and Test Electronic Information

Personnel tasked with software testing responsibilities must ensure that production data and electronic information are not used in testing and development environments. All test data and test electronic information must be appropriately tested and controlled and once considered secure must be removed before systems go into production.

5.5. System Acceptance

5.5.1 New Technology Evaluation

The SSO must evaluate and authorize all new security technologies in software, hardware, or network devices prior to their use in any SOA production environment.

5.5.2 Production Systems Control

The Department ISO and the SSO must review and approve all new or significantly changed application systems prior to their use in any SOA production implementation.

5.5.3 Security Impact Analysis

The Department ISO and the SSO must develop or require a risk assessment prior to implementing all new or significantly changed production software, hardware, or network devices.

5.5.4 Implementation Contingency Plans

The Department ISO and the SSO must develop or require a contingency plan prior to implementing all new or significantly changed production software, hardware, or network devices.

SOA Internal

5.6. Secure System Builds

5.6.1 Isolated Secure System Builds

Personnel tasked with system administration responsibilities must build systems disconnected from any externally-connected network until the complete operating system and current security patches are applied to the new system; the new system may be connected subsequently to a staging network for automated configuration. Standard builds for all hardware platforms must be developed to ensure adherence to security best practices and must follow the requirements as defined in SOA policy ISP-193 Vulnerability and Patch Management.

Personnel building systems must follow the security planning guide and the minimum security requirements. See *ISP-162: System Planning and Acceptance*, section *5.5 Security Planning* and *ISP-173: Network Security*, section *5.5.7 SOA Minimum Security Requirements* for security planning templates and guides, and additional information regarding minimum security requirements.

5.6.2 Best Practice Security Standards

The Department ISO and the SSO must ensure that standards for the secure configuration of software, hardware, network devices, and operating systems in the SOA production environment are available to personnel. Personnel tasked with administration responsibilities must apply applicable standards when implementing such systems.

SOA Internal

		Effective:	6/10/2025
		Last Review:	6/10/2025
Title:	Encryption	Next Review:	Tri-annually
Number:	ISP-192		
Version:	1.03	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To ensure the confidentiality of sensitive State of Alaska (SOA) information by applying appropriate encryption safeguards during transmission and storage.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Use of encryption
- Implementation of encryption services
- Sufficient encryption

5.1. Use of Encryption

5.1.1 Storage

When confidential or personally identifiable information (PII) is stored electronically, personnel must protect such information from unauthorized disclosure or access. When using data encryption it must be pre-approved by the State Security Office (SSO) and must not significantly impact the State's ability to perform discovery, monitoring, reporting, or detailed data analysis.

SOA Internal

5.1.2 Transmission

When confidential information or PII is transmitted over an external (non-SOA controlled or managed) network by electronic means (e.g., e-mail, text messaging, social media), file transfer, web service, or interactive session, personnel must protect such data from unauthorized disclosure or access by using data encryption according to the standards provided and approved by the SSO.

5.1.3 Encryption of Backups

Whenever technically and operationally feasible, personnel tasked with data backup responsibilities must protect confidential data from unauthorized disclosure or access by using data encryption for backup media according to the standards set forth by the SSO.

5.2. Implementation of Encryption Services

5.2.1 Balancing Email Discovery and Archiving

In cases of AS 40.25 Public Records Requests along with employee investigation requests, the availability of all information to be indexed and searched in an unencrypted form is a fiduciary requirement of the SOA to the public. To this end the SOA prohibits password protected content or attachments in email as well as pre-encrypted content or attachments.

5.2.2 Balancing Availability and Protection

Personnel tasked with the design and implementation of encryption systems must ensure that the implementation of encryption technologies balances data availability and data protection. When encryption cannot be technically or feasibly implemented as a control for confidential data, other approved controls must be implemented to ensure that data is protected from unauthorized disclosure or access.

5.2.3 Implementing Key Management

Where cryptographic key management is implemented, personnel tasked with design and implementation responsibilities must define and put into operational practices or processes to assure the secure handling and appropriate recoverability of data protected, by using an enterprise and centralized key management system. This centralized key management system must be maintained by the SSO in concurrence with the department business managers.

5.2.4 Implementing Key Recovery

Where public-key encryption is implemented, personnel tasked with design and implementation responsibilities must ensure that encryption practices incorporate a second recovery key, or a copy of the single private key must be escrowed with a trusted entity approved by the SSO. Key recovery must be implemented using a method that preserves the separation of duties and requires the participation of at least two authorized individuals.

5.3. Sufficient Encryption

5.3.1 Use of Standard Algorithms

Personnel tasked with encryption system design and implementation responsibilities must ensure that proven, non-proprietary algorithms of sufficient strength which meet the latest Federal Information Processing Standards (FIPS 140) validated cryptographic modules are

SOA Internal

used as the basis for encryption technologies. Encryption technologies and specifications must be approved by the SSO prior to implementation.

5.3.2 Review of Non-Standard Algorithms

When a department specific or proprietary encryption algorithm is required to satisfy a particular, defined, and single-scope business requirement, the SSO must evaluate the adequacy of and risks associated with use of the algorithm. Personnel must not implement a department specific or proprietary encryption algorithm without the explicit written approval of the SSO in the form of a memorandum of understanding (MOU).

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Vulnerability and Patch Management	Next Review:	Per policy
Number:	ISP-193		
Version:	1.2	Approved by:	CIO
Pages	3	Distribution:	SOA

1. Purpose

To ensure the State of Alaska (SOA) has an effective and standardized process for identifying, managing, and mitigating vulnerabilities related to SOA computers, networks, and applications to limit their exposure to vulnerabilities.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Vulnerability management; and
- Patch management.

5.1. Vulnerability Management

5.1.1 Routine Vulnerability Assessment and Monitoring

Personnel tasked with vulnerability assessment responsibilities must regularly scan SOA computers, networks, and applications in order to identify potential vulnerabilities. Personnel not specifically tasked with these duties must not conduct any form of technical vulnerability assessment and monitoring without specific approval from the State Security Office (SSO).

SOA Internal

5.1.2 SSO Assessment

At least annually, business managers must use the SSO to perform an information security vulnerability assessment of SOA computers, networks, and applications. Read access administrative accounts will be issued to SSO for authenticated vulnerability assessment requirements.

5.1.3 Vulnerability Research and Tracking

Personnel tasked with vulnerability assessment and monitoring responsibilities must regularly monitor vendor sources, security web sites, and relevant third party resources to identify potential vulnerabilities, and must inform the SSO of security issues that impact SOA systems. US-CERT National Cyber Alert System is a collection of three products consisting of alerts, tips and bulletins available at the following URLs:

https://www.cisa.gov/uscert/ncas/alerts

Vendor web sites and mailing lists are a resource for vulnerability and patch information, as well as third party web sites which can offer more detailed information and cover a large number of vendors and products or may specialize in a specific product.

5.2. Patch Management

5.2.1 Identification

Personnel tasked with system administration responsibilities must regularly monitor vendor sources, security web sites, and similar resources in order to identify potential patches, updates, or upgrades that are required in managing and maintaining SOA information systems security. Personnel tasked with system administration responsibilities must maintain documentation of patches, updates, or upgrades that have and have not been applied and work with SSO to determine priority of remediating vulnerabilities as defined in SOA policy ISP-161 Protection Against Malicious Software.

5.2.2 Evaluation

Personnel tasked with system administration responsibilities must review each patch, update, or upgrade prior to implementation to ensure that the item satisfies a business function or technical requirement and will not adversely impact SOA information systems.

5.2.3 Application

Security patches and upgrades must be applied to all systems and applications in compliance with SOA policy ISP-161 Protection Against Malicious Software. In cases where the installation of a patch or upgrade is shown to cause an adverse affect to a business application or system, the personnel tasked with system administration responsibilities will request authorization from the SSO to waive the patch requirement. A system or application which has been granted a waiver for a patch or upgrade must have its associated security plan amended to reflect the specific patch or upgrade and the reason it was not installed or applied.

5.2.4 Testing and Deployment

Standard security techniques must be used when deploying patches and upgrades. Prior to production implementation, personnel tasked with system administration responsibilities must adequately test each patch, update, or upgrade. Following testing, system administration personnel must use an SSO approved change control process in order to manage the deployment of each patch, update, or upgrade and consistently measure the effectiveness.

SOA Internal

5.2.5 System Backup

System backups must be conducted on a regular basis depending on the vulnerability exposures. Prior to the deployment of a patch, update, or upgrade, personnel tasked with system administration responsibilities must ensure that the target system has been adequately backed up and the backup and recovery processes have been tested and confirmed satisfactory.

SOA Internal

		Effective:	5/16/2025
		Last Review:	5/16/2025
Title:	External Email Encryption	Next Review:	Tri-annually
Number:	ISP-194		
Version:	1.03	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure unauthorized interception of electronically transferred information for State of Alaska (SOA) information assets, to include but not limited to, Personally Identifiable information (PII), Electronic Protected Health Information (EPHI), Payment Card Industry Data Security Standard (PCI DSS) or any other information protected by State, federal or local laws is obstructed by using encryption mechanisms on the SOA statewide system.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy defines:

- Encryption mechanism implementation; and
- Encryption availability for all SOA emailed information assets.

5.1. Encryption Mechanism Implementation

5.1.1 Encryption Mechanism

Encryption mechanisms have been implemented for SOA outbound email and have been configured to encrypt specific sensitive information such as, PII, EPHI and PCI, which shall be encrypted as it is passed outside the SOA statewide system. An exception to this process would be if the recipient's email domain has been configured to a transport layer security (TLS) connection with the SOA.

SOA Internal

This process is to prevent disclosure and unauthorized interception of electronically transferred information and provides protection to the sender and the receiver.

5.2. Encryption Availability for SOA Emailed Information Asset

5.2.1 Encryption Process Subject Field Requirement

To ensure that all SOA emails containing information such as, PII, EPHI and PCI are encrypted, especially where attachments have NOT gone through the Optical Character Recognition (OCR) mechanism, the email subject field must contain the following text: **[encrypt]** or **[secure].** The square brackets must be included to ensure encryption is accomplished for transmissions outbound to external domains. The "Confidential – State of Alaska" Sensitivity Label can also be used to encrypt email and is applied when the [encrypt] or [secure] tokens are added to the subject line.

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Prohibited Use of Password Protected Content & Pre-Encrypted Attachments	Next Review:	Per policy
Number:	ISP-195		
Version:	1.2	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure that text based documents, which are converted into an image format, are converted into an Optical Character Recognition (OCR) compatible format. To ensure that using local password protecting and pre-encrypting of content or attachments that impede discovery capabilities is prohibited; especially, SOA information asset content or attachments containing Personally Identifiable Information (PII), Electronic Protected Health Information (EPHI), Payment Card Industry Data Security Standards (PCI DSS), Criminal Justice Information Security (CJIS) or any other information protected by State, federal or local laws in electronic mail (email).

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Local password protection and attachment encryption are prohibited;
- Image format text based documents must be converted to OCR; and
- SOA system wide encryption must be implemented.

SOA Internal

5.1. Prohibit Local Password Protection and Attachment Encryption

5.1.1 Prohibit Local Password Protection & Attachment Encryption

It is the SOA's fiduciary responsibility to monitor email systems for internal policy compliance, suspected criminal activity, privacy of personally identifiable information (PII) and other systems management reasons. Using local password protecting and pre-encrypting of content or attachments that will impede discovery capabilities is prohibited. SOA is required to meet authorized public records requests, comply with State, federal and local statutes, regulations and policies and retain the ability to appropriately store and process SOA government documents and records.

5.2. Ensure All Image Format Text Based Documents are Converted to OCR and Encrypted

5.2.1 Ensure All Image Format Text Based Documents are converted to OCR compatible format

It is the SOA's responsibility to ensure that all text based documents (e.g., birth certificate) that have been changed to an image format are converted into an OCR compatible format for attachment.

5.2.2 Ensure Encryption

SOA emails, outbound to external domains, containing PII, EPHI, PCI DSS or CJIS information must be encrypted, as defined in SOA policy ISP-194 External Email Encryption.

SOA Internal

Title:	Cloud and Offsite Hosting	Effective:	12/19/2025
Number:	ISP-196	Last Review:	12/19/2025
Version:	1.02	Next Review:	Tri-annually
Pages	2	Approved by:	CIO
		Distribution:	SOA

1. Purpose

The State of Alaska (SOA) must establish information security requirements for procuring and utilizing cloud or offsite hosting services.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

This policy applies to all Information Technology (IT) related RFPs, contracts or service agreements initiated after the effective date. This policy does not apply to the use of Software as a Service (SaaS) solutions with integrated cloud elements specific to that solution.

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Cloud and Offsite Hosting.

5.1. Cloud and Offsite Hosting

5.1.1 Cloud Smart Strategy

The State of Alaska has a cloud smart strategy which balances aggressive cloud adoption with business value assessment. New and renewed services should look for cloud services before in-house solutions based on cost and efficiency.

SOA Internal

5.1.2 Mandatory Terms and Conditions

Every Cloud computing engagement must include the Mandatory Terms and Conditions clauses for cloud computing and a cloud exit assessment/strategy/ plan.

5.1.3 Formal Authorization

Use of cloud computing services for work purposes must be formally authorized by the Department of Administration (DOA) Chief Information Officer (CIO), the Department of Administration (DOA) Chief Information Security Officer (CISO), and agency/department Admin Services Director (ASD.

5.1.4 Platform Certification

The State Security Office (SSO) will certify that security, privacy and all other IT management and security requirements will be adequately addressed by the cloud computing vendor and that they conform to SOA Cloud Computing Standards.

5.1.5 Compliance

The use of such services must comply with SOA's policies, standards and procedures, data sovereignty requirements, compliance requirements, laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by the SOA and shall be audited by the SOA cloud agreement signatory at regular intervals, as required by external compliance specifications, or as requested.

5.1.6 Break-glass Credentials

The cloud computing services administrators will securely maintain break-glass documentation and credentials for business continuity purposes.

5.1.7 Personal Accounts Prohibited

Personal cloud computing services accounts may not be used for the storage, manipulation or exchange of SOA-related communications or SOA-owned data.

5.1.8 FedRAMP Preference

The Office of Information Technology (OIT) recommends the use of Federal Risk and Authorization Management Program (FedRAMP) listed/compliant cloud computing vendors.

5.1.9 SOA Identity Mgmt Preference

Cloud services that integrate with employee's existing network credentials reduce the number of passwords employees need to maintain and promote efficiency and security. OIT recommends cloud computing services that leverage SOA identity management.

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Continuity of Operations Plan (COOP)	Next Review:	Per policy
Number:	ISP-201		
Version:	1.2	Approved by:	CIO
Pages	4	Distribution:	SOA

1. Purpose

To ensure the availability of State of Alaska's (SOA) critical services, and to ensure that continuity of operations plans (COOP) are in alignment with the Department of Military and Veterans Affairs (DMVA) COOP efforts and address requirements to protect the confidentiality, integrity and availability of SOA critical services.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets. DMVA is responsible for SOA COOP planning under AS 26.23.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates:

- Establishment of COOP;
- COOP infrastructure; and
- COOP planning.

5.1. Establishment of COOP

5.1.1 COOP Framework

DMVA is responsible for COOP planning. Business Owners must maintain their individual COOP that must incorporate a risk assessment process, business impact analysis, recovery strategies, and incident response plan, as well as security requirements.

SOA Internal

5.1.2 Framework Authority

SOA has designated the DMVA as the single point of authority responsible for establishing continuity of operations plans. For critical business systems, the continuity of operations framework must be developed through the State Security Office (SSO) in collaboration with DMVA.

5.1.3 Business Owner Responsibility

Business Owners must provide evidence of their commitment to ensuring the availability of critical services that support business processes by:

- Determining the organization's approach to managing COOP in coordination with DMVA;
- Ensuring that appropriate plans and budgets are in place to support the COOP objectives of the SOA;
- Ensuring that the COOP integrates with existing plans for:
  - Incident response;
  - Emergency evacuation;
  - Crisis communication; and
  - Other relevant policies, procedures, and standards of the SOA.
- Approving, publishing, and communicating the COOP;
- Assigning responsibility and accountability for each individual COOP, including the appropriate resources with the seniority and authority needed to establish, implement, operate, and maintain the COOP framework;
- Ensuring that all personnel assigned COOP responsibilities are proficient to perform the following required tasks:
  - Assessing necessary competencies;
  - Conducting training needs analysis;
  - Providing training;
  - Ensuring that the necessary competencies have been achieved; and
  - Maintaining records of education, training, skills, experience, and qualifications of such personnel.
- Establishing the requirement for a formal, on-going COOP training and awareness framework;
- Assigning responsibility for internal audits of the COOP framework and ensuring that such audits are performed and reported appropriately to Executive Management;
- Ensuring that necessary corrective and preventative actions are taken to identify, mitigate, and eliminate potential disruptions to personnel, processes, and technology that support SOA operations; and
- Identifying any potential exception(s) to COOP policy, communicating the exception(s) to the SSO, and coordinating the appropriate activities and controls to reduce risk related to any such exceptions.

5.2. COOP Infrastructure

5.2.1 COOP Requirements

DMVA must define a set of requirements that must be met in the SOA COOP to ensure that the plans adequately safeguard SOA critical services.

5.2.2 COOP Review

DMVA must periodically, and upon significant change, review the COOP planning policy to verify and ensure that the framework adequately addresses the recovery requirements of the SOA critical services.

SOA Internal

5.2.3 COOP Approval

DMVA must approve COOP and updates prior to distribution to ensure business recovery requirements are appropriately addressed in the plans.

5.2.4 Addressing COOP in Risk Assessment

DMVA must ensure that events that will adversely impact the availability of SOA critical services are considered in risk assessment activities. During a risk assessment, the Departments and SSO must assist in the identification and qualification of risks that must enable SOA executive management to understand threats and vulnerabilities of its critical activities and supporting resources, including those provided by suppliers and outsourced partners.

5.2.5 Addressing COOP in Business Impact Analysis

DMVA must ensure that events that will disrupt the availability of SOA critical services are considered in business impact analysis activities. During business impact analysis, the SSO must assist in the identification, documentation and determination of impact of events that will interrupt the critical activities of the SOA.

5.2.6 Addressing COOP in Recovery Strategies

DMVA must ensure that, for each critical service, Business Owners identify available risk treatments that can reduce the likelihood of a disruption, shorten the period of a disruption, and limit the impact of a disruption. Business Owners must select and implement appropriate risk treatments for each critical activity in accordance with the SOA level of risk tolerance.

5.3. COOP Planning

5.3.1 COOP Requirements

Business Owners, with assistance from the DMVA, must develop individual COOP to maintain critical services or to restore critical services in the event of an interruption or failure. The Business Owner's Business Management must establish time-frames, categories, and priorities for maintenance and resumption of critical services consistent with SOA requirements.

5.3.2 Accessibility of COOP

Business Owners must ensure electronic and printed copies of COOP are provided, communicated and remain accessible to Department incident management teams and ensure the information (electronic and paper) is available in the event of activation, to guarantee effective response when a COOP event has been activated.

5.3.3 Testing and Maintaining COOP

Business Owners, assisted by DMVA, must periodically test each individual COOP to ensure it adequately addresses business recovery requirements. Business Owners must update each individual COOP to keep pace with changes in information technology and business requirements and in response to the results of testing and/or Business Owner review.

5.3.4 COOP Training

DMVA must ensure that COOP training and awareness programs include appropriate information and instruction regarding the COOP planning process and SOA COOP.

SOA Internal

5.3.5 COOP Auditing

Business Owners, assisted by DMVA, must periodically monitor and review the effectiveness and efficiency of each individual COOP; review the appropriateness of their COOP policy, objectives, and scope; and determine and authorize necessary activities for remediation and improvement.

SOA Internal

		Effective:	2/24/2023
		Last Review:	2/24/2023
Title:	Copyright Information and Software Licensing	Next Review:	Per policy
Number:	ISP-211		
Version:	1.2	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure that copyrighted information is used throughout the State of Alaska (SOA) in a legal and ethical manner.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Proper use of copyright material;
- Software Licensing; and
- Preservation of intellectual property rights.

5.1. Proper Use of Copyright Material "©"

5.1.1 Proper Use of Copyright Material "©"

Personnel must not knowingly incorporate Copyright Material into any SOA information system or artifact without obtaining written consent of the copyright owner.

SOA Internal

5.1.2 "Fair Use"

SOA personnel must use Copyright Material in accordance with the "fair use" doctrine (Title 17 USC § 107) or must license or purchase the Copyright Material for use within SOA information systems or artifacts.

5.2. Software Licensing

5.2.1 Use of Licenses

Personnel must not knowingly use software or other information products in a manner inconsistent with licensing agreements, including but not limited to software "piracy", unauthorized duplication of software, or exceeding the number of licenses purchased for licensed software.

5.2.2 License Inventory

Department Information Security Officers must maintain an inventory of software licenses purchased for use within SOA administrative, technical, and other operations. This inventory must be accurately maintained and must reflect all licensed software products deployed to SOA personnel.

5.3. Preservation of Intellectual Property Rights

5.3.1 Preservation of Property Rights

Business managers must ensure that appropriate procedures and policies are developed and implemented to ensure compliance with legislative, regulatory and contractual requirements regarding the use of materials, software or other products for which there may be intellectual property rights.

SOA Internal

Title:	Compliance Monitoring	Effective:	2/24/2023
Number:	ISP-212	Last Review:	2/24/2023
Version:	1.2	Next Review:	Per policy
Pages	2	Approved by:	CIO
		Distribution:	SOA

1. Purpose

To establish the requirement for monitoring of the State of Alaska (SOA) information security management system and to assure implementation of mandates and compliance with applicable policies and regulatory requirements.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Implementing and reviewing controls; and
- Methods for assessing compliance.

5.1. Implementing and Reviewing Controls

5.1.1 Controls Must Be Enforceable

Personnel who implement security controls to satisfy security requirements must ensure that those controls are approved and enforceable by the State Security Office (SSO) prior to adopting those controls as a part of standard operating procedure.

SOA Internal

5.1.2 Controls Must Be Verifiable

Personnel who implement security controls to satisfy security requirements must implement those controls so that they are verifiable by the SSO, either through direct examination or logged information that provides an auditable activity record.

5.1.3 Security Control Review

Personnel tasked with auditing responsibility must periodically review the design, implementation, and operation of information security controls and must identify instances of non-compliance and immediately report non-compliance to the SSO.

5.1.4 Protection of Records

Personnel tasked with the processing and storage of organizational records must ensure that such records are protected in accordance with applicable statutory, regulatory, administrative order, policies, or directive requirements and are verifiable by the SSO.

5.1.5 Cryptographic Controls

The SSO must ensure that cryptographic controls are implemented, safeguarded, and distributed in accordance with applicable statutory, regulatory, administrative order, policies, or directive requirements.

5.2. Methods for Assessing Compliance

5.2.1 Internal Audit Review

Personnel tasked with internal auditing responsibilities must periodically review log and audit information for purposes of determining efficacy and compliance and must ensure the SSO has direct access to all log and audit information.

5.2.2 External Audit Review

Business Managers must regularly engage the SSO to review log and audit information for purposes of validating security controls and ensuring compliance with applicable legal and regulatory requirements.

5.2.3 Legal and Regulatory Requirements

The SSO, with the assistance of the Department Information Security Officers, must periodically, not less than annually, identify and review the regulatory and legal requirements of the SOA and must maintain a record of those requirements that apply to SOA information assets.

SOA Internal

1. Purpose

To ensure that all internal and external State of Alaska (SOA) system audits are appropriately performed in a manner that is least-disruptive to SOA IT operations.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions, or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Information system audits;
- CIO advance notification requirement of electronic and IT audits; and
- Audit tools authorization.

5.1. Information Systems Audit

5.1.1 Requirement for Periodic Audit

Business Managers must conduct periodic audits of SOA information, systems, policies, procedures, processes and standards to ensure that controls are appropriate to the level of identified risk. Business Managers must provide Executive Management and the State Security Office (SSO) with results of audits to ensure that Executive Management can perform proper risk analysis on all findings.

SOA Internal

5.1.2 Technical Compliance Validation

Business Managers must conduct periodic audits of SOA information system technical security controls to ensure that controls are uniformly implemented throughout the infrastructure. Business managers must make sure that all findings are provided to the executive management and the SSO; to provide an opportunity for proper risk analysis to be performed on all findings.

5.1.3 Audit Planning

Business Managers must ensure that audit activities are planned and that timeframes are agreed upon to minimize disruption of production information systems.

5.2. CIO advance notification requirement of electronic and IT audits.

5.2.1 CIO Notifications to all External Electronic and IT Audit Requests

Once an external audit request has been received by an SOA department, the CIO must be notified of the request within two SOA business days. The external audit request notification must include the following:

- Name of entity or department requesting audit;
- Requested date for the audit;
- IT information requested (if specified);
- Access permissions (if required); and
- Copy of same entity or department previous audit (if applicable).

5.2.2 CIO advance approval of all External Audit Information Distribution

Departments must forward their audit results and responses to the CIO for review and approval prior to distribution.

5.3. Audit Tools Authorization

5.3.1 Protection of Audit Tools

Personnel must not use system auditing tools, which can perform network scans or capturing, unless specifically authorized to do so by the SSO.

SOA Internal

		Effective:	5/16/2025
		Last Review:	5/16/2025
Title:	Auditing and Compliance	Next Review:	Tri-annually
Number:	ISP-214		
Version:	1.02	Approved by:	CIO
Pages	2	Distribution:	SOA

1. Purpose

To ensure independent auditing and compliance monitoring on all information technology or telecommunication networks, systems, services, electronically processed and stored information, data or information records is executed for the State of Alaska (SOA) Executive Branch Agencies, Corporations, and Commissions.

2. Statutory Authority

Under Alaska Statute (AS) 44.21 et. Seq., the Department of Administration is assigned responsibility for statewide Executive Branch automated data processing and telecommunication support.

The Governor's Administrative Order 284 (AO 284) establishes the statewide Office of Information Technology (OIT) to be housed within the Department of Administration. The AO further establishes the position of Chief Information Officer (CIO), with designated authority for all telecommunication and information technology services within the SOA Executive Branch.

Records owned by executive branch agencies are subject to oversight as designated by the Commissioner of their respective department as specified in AS 44.17. Record retention requirements are subject to comply with State archivist statutes AS 40.21. OIT sets and enforces digital information security, privacy, and protection standards and practices assuring all SOA information assets.

3. Policy Scope

This policy is applicable to the SOA executive branch, departments, divisions, corporations, commissions or other related entities which will be referred to as Department(s).

4. Definitions

Terms in this document are defined in the SOA policy ISP-002 Information Security Glossary.

5. Policy Statement

This policy stipulates requirements for:

- Independent information system auditing and compliance monitoring; and
- Authorizations for auditing and compliance monitoring.

5.1. Independent System Auditing and Compliance Monitoring

5.1.1 System Auditing and Compliance Monitoring

The State Security Office (SSO) may develop, deploy, maintain and perform independent auditing and compliance monitoring on all information technology or telecommunication networks, systems, services, electronically processed data, stored information, or records for the Executive Branch Agencies, Corporations, and Commissions. The SSO may perform and direct this function to include the Executive Branch networks, computers, workstations, servers, email, databases, or other electronic devices, systems, services and for information handling processes. In addition, the SSO may perform detailed analyses, as part of the

SOA Internal

auditing and compliance monitoring and reporting process for the purposes of determining the accuracy of the information, as requested by the Executive Management.

SOA Internal