THE STATE of ALASKA

State of Alaska – Department of Health

Authorization Package Framework

Authorization Package Framework

Purpose of Document

This document provides an overview of the information that the Department of Health (DOH) security assessment requires. This criteria is based on the NIST 800-53 Revision 4 information security and compliance framework focusing on NIST 800-66 Revision 1 controls. These controls outline legal compliance requirements for systems of a “moderate” risk level, such as HIPAA/HITECH. When completed and kept up to date, this information outlines who is responsible for each role associated with the project, what risk DOH is assuming through use and support of the system, how DOH is mitigating that risk, and how DOH is ensuring that the documented system will have the confidentiality, integrity, and availability needed to fulfill required tasks.

This document provides a list of some of the data required to complete a DOH authorization package and System Security Plan (SSP). Configured as an internal web application, it is customized and maintained by DOH staff per the department’s goals. This document is provided as an example of the type of data requested within an authorization package, but it is not an exact representation of all data DOH will require.

Content

1. Information System Name/Title

<Authorization Package Name>

<Acronym>

2. System Environment

- Business Process Diagram
- Boundary Description
- Boundary Diagram
- Network Diagram
- Data Flow Diagram
- Most Recent Vulnerability Scan Report
- Patching and Support Information
- Regular Maintenance Window Schedule

3. FISMA Network Vulnerability Scan Requirement

- Offerors are expected to have a FISMA compliant network vulnerability scan performed at least once every 30 days
- Results to be provided to the Department Security Office (DSO) and the Division Data Owner.

4. Automated Code Scan Requirement

- Offerors must have an automated code scan, or manual analysis of code security, performed at least once every 90 days prior to any build being released into a production environment (whichever comes first)
- Results to be provided to the Department Security Office and the Division Data Owner.

5. Privacy Threshold Analysis (PTA)

PTA-1: Select an Information System status (select one):

- ☐ This is a new development effort
- ☐ This is an existing project

PTA-2: Does/will the Information System collect, maintain, use, or disseminate personally identifiable information on any of the following parties (select all that apply):

- ☐ This program does not collect any personally identifiable information
- ☐ Employees
- ☐ Contractors
- ☐ Members of the public
- ☐ Other

PTA-3: Does/will the Information System intend to collect, generate, or retain any of the following information considered PII, PHI, CJIS, or confidential on individuals (select all that apply):

- ☐ None of these values apply
- ☐ Name
- ☐ Birth Information (Date and/or Place of birth)
- ☐ Admission Date and/or Discharge Date
- ☐ Date of Death
- ☐ Medical Record Numbers
- ☐ Health Plan
- ☐ Beneficiary Numbers
- ☐ Financial data (credit card numbers, bank account numbers, etc.)
- ☐ Certificate/License Numbers
- ☐ Criminal History
- ☐ Employment History (Wage Information)
- ☐ Biometric Information (fingerprints, voice prints, iris scans, DNA, etc.)
- ☐ Full face photographic images and any comparable images
- ☐ Personal information (mailing and/or residency address, e-mail, phone/fax numbers, etc.)
- ☐ Other unique identifying number, characteristic, or code

PTA-4: Does/will the Information System use or collect Social Security Numbers (SSN)? This includes truncated SSN's (e.g. last 4 digits) (select one):

- ☐ No
- ☐ Yes

PTA-5: Does/will the system connect, receive, or share information with any other Information System (select one):

- ☐ No
- ☐ Yes

PTA-6: Does/will the Information System connect, receive, or share information with any external systems (select one):

- ☐ No
- ☐ Yes

PTA-7: Are there/will there be regular (i.e. periodic, recurring, etc.) data extractions from the Information System (select one):

- ☐ No
- ☐ Yes

PTA-8: Who has/will have access to your system that is not a workforce member of DOH, such as federal or other state departments, grantees, providers, public, etc. (select all that apply):

- ☐ Contractors
- ☐ Federal Government
- ☐ Grantees
- ☐ Other State Governments
- ☐ Other State of Alaska Departments
- ☐ Public
- ☐ Service Providers
- ☐ State of Alaska Courts
- ☐ State of Alaska Legislature
- ☐ Vendors

PTA-9: What procedures are/will be in place to determine which users may access the information and how does the project determine who has access:

<narrative answer required>

PTA-10: How does the project team review information sharing agreements, MOU's, new uses of the information, new access to the system by organizations within the department and outside:

<narrative answer required>

6. System Interfaces/Information Sharing

For each interface that ingress or egress the DOH environment, we must document how they function, where the data stops along the way (ESBs, API management servers, service aggregation systems, etc.), how it's protected in transport, and where it's going. For **each** of these interfaces we need an Interface Risk Assessment Worksheet completed (see below for example).

Please select which model best describes the interface's architecture:

- ☐ One-way, Point-to-point
- ☐ Request/Response, Point-to-point
- ☐ Request/Response, Point-to-point, long-running

Please list each source/recipient system (endpoint):

Interface Description Location	
Endpoint URL	
Message format	
Classified Data Type(s)	
Orchestrated in BizTalk/Mule ESB?	
Orchestration Type	☐ Aggregator ☐ Aggregator, long-running ☐ N/A
Connection Mechanism	
Planned Encryption Mechanism	
Source Authentication Mechanism	
Is the authentication credential unique to this interface?	
Description of Interface	

7. Minimum Security Controls

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

8. Authorization Package Controls

Control Number	Control Name	Control
AC-01	ACCESS CONTROL POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy (as necessary) within every three hundred sixty-five (365) days; and 2. Access control procedures (as necessary) within every three hundred sixty-five (365) days.
AC-02	ACCOUNT MANAGEMENT	The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by defined personnel or roles for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with organizational standards and procedures; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements within every one hundred eighty (180) days; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
AC-03	ACCESS ENFORCEMENT	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-04	INFORMATION FLOW ENFORCEMENT	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.
AC-05	SEPARATION OF DUTIES	The organization: a. Separates duties of individuals as necessary to prevent malevolent activity without collusion; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.
AC-06	LEAST PRIVILEGE	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
AC-11	SESSION LOCK	The information system: a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.
AC-12	SESSION TERMINATION	The information system automatically terminates a user session after fifteen (15) minutes of inactivity.
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization: a. Identifies user actions that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.
AC-17	REMOTE ACCESS	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems.
AC-22	PUBLICLY ACCESSIBLE CONTENT	The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the

		publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information bi-weekly and removes such information, if discovered.
AT-01	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy within every three hundred sixty-five (365) days; and 2. Security awareness and training procedures within every three hundred sixty-five (365) days.
AT-02	SECURITY AWARENESS TRAINING	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. Within every three hundred sixty-five (365) days thereafter.
AT-03	ROLE-BASED SECURITY TRAINING	The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. Within every three hundred sixty-five (365) days thereafter.
AT-04	SECURITY TRAINING RECORDS	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for a minimum of five (5) years.
AU-01	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An audit and accountability policy that addresses purpose, people, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy within every three hundred sixty-five (365) days; and 2. Audit and accountability procedures within every three hundred sixty-five (365) days.

AU-02	AUDIT EVENTS	The organization: a. Determines that the information system is capable of auditing the following events: 1. Server alerts and error messages; 2. Log onto system; 3. Log off system; 4. Change of password; 5. All system administrator commands, while logged on as system administrator; 6. Switching accounts or running privileged actions from another account, (e.g., Linux/UNIX SU or Windows RunAs); 7. Creation or modification of super-user groups; 8. Subset of security administrator commands, while logged on in the security administrator role; 9. Subset of system administrator commands, while logged on in the user role; 10. Clearing of the audit log file; 11. Startup and shutdown of audit functions; 12. Use of identification and authentication mechanisms (e.g., user ID and password); 13. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su); 14. Remote access outside of the corporate network communication channels (e.g., modems, dedicated Virtual Private Network) and all dial-in access to the system; 15. Changes made to an applications or database by a batch file; 16. Application-critical record changes; 17. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility); 18. User log-on and log-off (successful or unsuccessful); 19. System shutdown and reboot; 20. System errors; 21. Application shutdown; 22. Application restart; 23. Application errors; 24. Security policy modifications; and 25. Printing sensitive information; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: All applicable events listed under AU-02 a, audited on a continuous basis or in response to specific situations as appropriate based on current threat information and ongoing assessment of risk.
AU-03	CONTENT OF AUDIT RECORDS	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
AU-04	AUDIT STORAGE CAPACITY	The organization allocates audit record storage capacity in accordance with reducing the likelihood that storage capacity will be exceeded.
AU-05	RESPONSE TO AUDIT PROCESSING FAILURES	The information system: a. Alerts applicable personnel or roles in the event of an audit processing failure; and b. Takes the following additional actions: Generates alerts and takes other actions as appropriate to the information system, possibly including: shut down information system, overwrite oldest audit records, stop generating audit records.

AU-06	AUDIT REVIEW, ANALYSIS, AND REPORTING	The organization: a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity; and b. Reports findings to the Department Chief Security Officer.
AU-07	AUDIT REDUCTION AND REPORT GENERATION	The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.
AU-11	AUDIT RECORD RETENTION	The organization retains audit records for at least ninety (90) days and archives old records for six (6) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
CA-01	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy within three hundred sixty-five (365) days; and 2. Security assessment and authorization procedures within three hundred sixty-five (365) days.
CA-03	SYSTEM INTERCONNECTIONS	The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements within three hundred sixty-five (365) days or when there are changes to the connection.
CA-07	CONTINUOUS MONITORING	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of organizationally defined metrics to be monitored; b. Establishment of defined frequencies for monitoring and defined frequencies for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to the Information Owner, IT management, and the Department Chief Security Officer monthly.

CP-01	CONTINGENCY PLANNING POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy within every three hundred sixty-five (365) days; and 2. Contingency planning procedures within every three hundred sixty-five (365) days.
CP-02	CONTINGENCY PLAN	The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by the Information Owner and Department Chief Security Officer; b. Distributes copies of the contingency plan to the Information Owner, Department Chief Security Officer, contingency plan coordinator, and other stakeholders identified within the contingency plan; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system within every three hundred sixty-five (365) days; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to stakeholders; and g. Protects the contingency plan from unauthorized disclosure and modification.
CP-03	CONTINGENCY TRAINING	The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within ninety (90) days of assuming a contingency role or responsibility; b. When required by information system changes; and c. Within every three hundred sixty-five (365) days thereafter.
CP-04	CONTINGENCY PLAN TESTING	The organization: a. Tests the contingency plan for the information system within every three hundred sixty-five (365) days using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.
CP-06	ALTERNATE STORAGE SITE	The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

CP-07	ALTERNATE PROCESSING SITE	The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within a resumption time period consistent with the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) defined by the Information Owner and documented in the authorization package and contingency plan, when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.
CP-08	TELECOMMUNICATIONS SERVICES	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within a resumption time period consistent with the Recovery Time Objectives (RTO) defined by the Information Owner and documented in the authorization package and contingency plan, when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
CP-09	INFORMATION SYSTEM BACKUP	The organization: a. Conducts backups of user-level information contained in the information system on a daily basis or more frequently if required; b. Conducts backups of system-level information contained in the information system on a daily basis or more frequently if required; c. Conducts backups of information system documentation including security-related documentation; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
IA-02	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
IA-03	DEVICE IDENTIFICATION AND AUTHENTICATION	The information system uniquely identifies and authenticates network devices before establishing a high risk network connection.
IA-04	IDENTIFIER MANAGEMENT	The organization manages information system identifiers by: a. Receiving authorization from Information Owner or Security Designee to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual,

		group, role, or device; d. Preventing reuse of identifiers for at least three (3) years after all previous access authorizations are removed from the system, including all file and other resource accesses for that identifier; and e. Disabling the identifier after ninety (90) days or less of inactivity.
IA-05	AUTHENTICATOR MANAGEMENT	The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators Passwords: ninety (90) days (Users / Privileged Users / Services); Public Certificates: no longer than three (3) years; Internal Certificates: as determined by Information Owner; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.
IA-06	AUTHENTICATOR FEEDBACK	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
IR-01	INCIDENT RESPONSE POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy within every three hundred sixty-five (365) days; and 2. Incident response procedures within every three hundred sixty-five (365) days.
IR-02	INCIDENT RESPONSE TRAINING	The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within ninety (90) days of assuming an incident response role or responsibility; b. When required by information system changes; and c. Within every three hundred sixty-five (365) days thereafter.
IR-03	INCIDENT RESPONSE TESTING	The organization tests the incident response capability for the information system within every three hundred sixty-five (365) days using NIST SP 800-61 to determine the incident response effectiveness and documents the results.

IR-04	INCIDENT HANDLING	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.
IR-05	INCIDENT MONITORING	The organization tracks and documents information system security incidents.
IR-06	INCIDENT REPORTING	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within an expeditious time period; and b. Reports security incident information to the employee's supervisor and the Department Chief Security Officer.
IR-07	INCIDENT RESPONSE ASSISTANCE	The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.
MA-01	SYSTEM MAINTENANCE POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy within every three hundred sixty-five (365) days; and 2. System maintenance procedures within every three hundred sixty-five (365) days.
MA-02	CONTROLLED MAINTENANCE	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that the applicable Information Owner (or an official designated in the applicable security plan) explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.

MA-05	MAINTENANCE PERSONNEL	The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
MP-01	MEDIA PROTECTION POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy within every three hundred sixty-five (365) days; and 2. Media protection procedures within every three hundred sixty-five (365) days.
MP-02	MEDIA ACCESS	The organization restricts access to classified data including but not limited to: PII, ePHI, FTI, CJI, etc. to authorized individuals.
MP-04	MEDIA STORAGE	The organization: a. Physically controls and securely stores all unencrypted media within secure areas; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
MP-05	MEDIA TRANSPORT	The organization: a. Protects and controls unencrypted digital and non-digital media containing sensitive information, such as Personally Identifiable Information (PII), during transport outside of controlled areas using tamper-evident packaging, and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.
MP-06	MEDIA SANITIZATION	The organization: a. Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using State and Department standard sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
PE-01	PHYSICAL AND ENVIRONMENTAL	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the

	PROTECTION POLICY AND PROCEDURES	implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy within every three hundred sixty-five (365) days; and 2. Physical and environmental protection procedures within every three hundred sixty-five (365) days.
PE-02	PHYSICAL ACCESS AUTHORIZATIONS	The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals at least once every one hundred eighty (180) days; and d. Removes individuals from the facility access list when access is no longer required.
PE-03	PHYSICAL ACCESS CONTROL	The organization: a. Enforces physical access authorizations at defined entry/exit points to the facility where the information system resides by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using physical access devices/or guards; b. Maintains physical access audit logs for defined entry/exit points to the facility; c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices every three hundred sixty-five (365) days; and g. Changes combinations and keys within every three hundred sixty-five (365) days and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
PE-04	ACCESS CONTROL FOR TRANSMISSION MEDIUM	The organization controls physical access to information system distribution and transmission lines within organizational facilities using defined security safeguards.
PE-05	ACCESS CONTROL FOR OUTPUT DEVICES	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
PE-06	MONITORING PHYSICAL ACCESS	The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs at least monthly and upon occurrence of security incidents involving physical security; and c. Coordinates results of reviews and investigations with the organizational incident response capability.
PE-08	VISITOR ACCESS RECORDS	The organization: a. Maintains visitor access records to the facility where the information system resides for two (2) years; and b. Reviews visitor access records at least monthly.
PE-17	ALTERNATE WORK SITE	The organization: a. Employs appropriate security controls at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.
PL-01	SECURITY PLANNING POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy within every three hundred sixty-five (365) days; and 2. Security planning procedures within every three hundred sixty-five (365) days.
PL-04	RULES OF BEHAVIOR	The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior every three hundred sixty-five (365) days; and d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.
PS-01	PERSONNEL SECURITY POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy within every three hundred sixty-five (365) days; and 2. Personnel security procedures within every three hundred sixty-five (365) days.
PS-02	POSITION RISK DESIGNATION	The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations within every three hundred sixty-five (365) days.
PS-03	PERSONNEL SCREENING	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to the criticality/sensitivity risk designation of the position, on a periodic basis and at least every three (3) years.

PS-04	PERSONNEL TERMINATION	The organization, upon termination of individual employment: a. Disables information system access within a time period ending prior to or during the employee termination process, or prior to notification if employee is terminated for cause; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies applicable stakeholders within one (1) business day.
PS-05	PERSONNEL TRANSFER	The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates the re-issuing of appropriate information system-related property (e.g., keys, identification cards, and building passes), notification to security management, closing of obsolete accounts and establishing new accounts, and re-evaluation of logical and physical access controls within thirty (30) days; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies applicable stakeholders within one (1) business day.
PS-06	ACCESS AGREEMENTS	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements within every three hundred sixty-five (365) days; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated.
PS-07	THIRD-PARTY PERSONNEL SECURITY	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify contract administrator of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days; and e. Monitors provider compliance.
PS-08	PERSONNEL SANCTIONS	The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies appropriate stakeholders within a reasonable period of time, when applicable, when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

RA-01	RISK ASSESSMENT POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy within every three hundred sixty-five (365) days; and 2. Risk assessment procedures within every three hundred sixty-five (365) days.
RA-02	SECURITY CATEGORIZATION	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

RA-05	VULNERABILITY SCANNING	The organization: a. Scans for vulnerabilities in the information system and hosted applications within every thirty (30) days and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities per State of Alaska (ISP-161 and ISP-193) and department policies and procedures in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with applicable stakeholders to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2. References: NIST Special Publications 800-40, 800-70, 800-115; Web: cwe.mitre.org, nvd.nist.gov.

SA-04	ACQUISITION PROCESS	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.
SA-09	EXTERNAL INFORMATION SYSTEM SERVICES	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, and operation; b. Document, manage, and control the integrity of changes to the information system; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles.
SC-08	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	The information system protects the confidentiality and integrity of transmitted information.
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with requirements defined by Department Chief Security Officer for key generation, distribution, storage, access, and destruction.

SI-01	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy within every three hundred sixty-five (365) days; and 2. System and information integrity procedures within every three hundred sixty-five (365) days.
SI-02	FLAW REMEDIATION	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within the software patching timeframes defined in State of Alaska ISP-161 of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.
SI-03	MALICIOUS CODE PROTECTION	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system every twenty-four (24) hours and real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Block and quarantine malicious code and send alerts to the administrator and Department Chief Security Officer in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

SI-04	INFORMATION SYSTEM MONITORING	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with State of Alaska and department incident handling policy and procedure; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through defined techniques and methods; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides unauthorized connection information to the Department Chief Security Officer and applicable stakeholders as appropriate.
SI-05	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	The organization: a. Receives information system security alerts, advisories, and directives from external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: defined personnel; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
SI-07	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	The organization employs integrity verification tools to detect unauthorized changes to information systems.
SI-08	SPAM PROTECTION	The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
SI-10	INFORMATION INPUT VALIDATION	The information system checks the validity of defined information inputs.

9. Related Laws/Regulations/Policies

(Double-Click on each box to change "marked" status)

☐	Alaska Statutes	☐	DOH Policies	☐	HIPAA/HITECH (EPHI)	☐	CJIS Security Policy
☐	Federal Statutes	☐	SoA Policies	☐	IRS PUB 1075 (FTI)	☐	PCI DSS
		☐	Alaska Personal Information Protection Act (PI)	☐	CMS MARS-E	☐	Other

10. Appendix A – Acronyms and Abbreviations

Acronym	Term
AC	Access Control
ACA	Patient Protection and Affordable Care Act of 2010
AD	Microsoft Active Directory
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
APIPA	Automatic Private IP Addressing
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CCB	Change Control Board
CFR	Code of Federal Regulations
CI	Configuration Item
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMS	Centers for Medicare & Medicaid Services
CMRS	Continuous Monitoring and Risk Scoring
CMSR	CMS Minimum Security Requirements
COOP	Continuity of Operations Plan
CP	Contingency Planning
DES	Data Encryption Standard
DFCS	Department of Family and Community Services
DIFSLA	IRS Publication 3373 Disclosure of Information to Federal, State, and Local Agencies
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DOH	Department of Health

Acronym	Term
IT	Information Technology
LAN	Local area network
MA	Maintenance
MARS-E	Minimum Acceptable Risk Standards for Exchanges
MITA	Medicaid Information Technology Architecture
MP	Media Protection
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
OMB	Office of Management and Budget
PDA	Personal digital assistants
PE	Physical and Environmental Protection
PHI	Protected Health Information
PHR	Personal Health Record
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PL	Planning
PM	Information Security Program Plan
POA	Plan of Action
POA&M	Plan of Action and Milestones
PS	Personnel Security
PUB	Publication
RA	Risk Assessments
RAC-F	Resource Access Control Facility
ROB	Rules of Behavior

Acronym	Term
DoS	Denial of Service
DPA	Division of Public Assistance
DR	Disaster Recovery
DSO	Department Security Office
EIS-R	Eligibility Information System – Replacement
EPHI	Electronic protected health information
ESI	Electronically Stored Information
FIPS	Federal Information Processing Standards
FTI	Federal Tax Information
GSS	General Support Systems
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
HTTPS	Hypertext Transfer Protocol Secure
IA	Identification and Authentication
ID	Identifier
IDS	Intrusion detection system
INR	Incident Response Report
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
IRS	Internal Revenue Service
IRT	Incident Response Team
IS	Information Security
ISO	International Organization for Standardization

Acronym	Term
RSS	Registration Support Specialist
SA	System and Services Acquisition
SAR	Safeguard Activity Report
SAM	Security Access Manager
SC	System and Communications Protection
SDLC	Software Development Lifecycle
SFTP	Secure File Transfer Protocol
SI	System and Information Integrity
SOA	State Of Alaska
SSA	Social Security Administration
SSL	Secure Sockets Layer
SSN	Social Security Number
SSO	State Security Office
SSP	System Security Plan
TLS	Transport Layer Security
URL	Uniform Resource Locator
USGCB	U.S. Government Configuration Baselines
VLAN	Virtual Local Area Network
VM	Vulnerability Management
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Points
WP	Worker Portal

11. Change Log

This document is updated as needed. The following change log reflects the person, revision date and summary of the change.

Author	Date	Summary of change
C Boom	9/24/2021	Changed letterhead to the Seal of the State of AK, removed reference to governor. Added a changed log Changed the footer date to 9/24/2021
D. Garcia	08/03/2022	Updated almost all of the content, added the network scan and code scan requirements, added 8 controls, updated the System Interface section.