Reference A
Information Technology Requirements

State of Alaska
Department of Health

TABLE OF CONTENTS

1 Purpose of IT Requirements

The State of Alaska Department of Health (DOH) is engaged in a Cloud First initiative strongly favoring SaaS solutions. We have embraced an Information Technology (IT) Roadmap for shared services using our Enterprise Service Bus (ESB), and Master Client Index (MCI).

The response to this request must address if, and how, the proposed product solution will integrate into this environment, where appropriate.

1.1 IT Requirements Intent and Approach

DOH Information Technology Services (ITS) values our partner relationships with external vendors, contractors, and grantees. DOH ITS is focused on providing the best value to our customers by supporting IT procurements from the RFP solicitation process, through project initiation, planning, execution, and closing.

At a high-level, these IT requirements support the proposal solicitation by meeting two goals:

1. The requirements help the Offeror understand our service delivery approach. They give Offerors the opportunity to shape their proposals to best fit the team of program staff, ITS staff, and Offeror staff that will work together to deliver the solution.
2. The requirements identify specific requirements and statements that Offerors must address to be classified as responsive.

These IT requirements are structured into services and standards sections, corresponding to a service line within DOH ITS. For example, the solicitation-relevant requirements for end-user desktop configurations are in the “Enterprise Desktop Services and Standards” section.

As part of our Cloud First initiative, DOH IT is seeking proposals for solutions which are vendor hosted and vendor managed, rather than provided locally or hosted within the department’s network.

However, we recognize that solutions are available in many forms. Offerors may consider proposing one or more of the following options:

- DOH hosted and managed solution components;
- 3rd party hosted, DOH managed solution components;
- Software as a Service (SaaS)
- Anything as a Service (XaaS);
- Hybrid/Combination of above.

DOH recognizes that SaaS and XaaS delivery models afford some additional value to our department. It offers the opportunity to leverage the business value of the solutions without bearing the costs and risks of having to maintain development and operational infrastructure. This value is achieved when the SaaS/XaaS vendor carries the burden of managing technical operations and ongoing development/maintenance, while collaborating with their clients to meet and maintain the functional requirements and integrity of the solution.

Offerors should read each section carefully to understand how DOH ITS applies a particular service-line to procured services and what specific requirements, questions, and statements must be answered. Please be aware that the State of Alaska requires all resources utilized as a part of the RFP response, system development, and implementation to be US based or DOH approved resources. This includes hosted services, vendor personnel, vendor contracted services, and personnel and vendor contracted consulting services.

2 Technical Qualifications Response

2.1 Minimum Qualifications

Offerors must complete **Required Vendor Response - DOH IT Requirements**, which correspond to the requirements described in Section 3 of this document and return it as part of their proposal. A failure to complete and return this IT Reference will result in a proposal being deemed non-responsive.

2.2 Understanding of the Technical Aspects of the Project

In the body of their proposal, Offerors must provide comprehensive narrative statements that illustrate their understanding of the technical requirements and must respond to all applicable sections, or respond why a section is not applicable.

A failure to demonstrate how the solution being proposed addresses the Technical Requirements outlined may result in the proposal deemed non-responsive and rejected.

3 State of Alaska DOH Technology Services, Standards, and IT Road Map

Information technology services for DOH agencies are provided by DOH Division of Finance and Management Services Information Technology Services (ITS). DOH ITS provides the following functions: maintenance of the DOH Data Centers in Juneau and Anchorage; project execution support; operational support; and integration assistance for systems hosted on site. We also manage some IT services hosted and operated out of the State of Alaska Office of Information Technology (SOA-OIT) data centers (separate from our datacenters), and services out of Microsoft's Azure Government Community Cloud.

This section describes many of the services offered in detail and highlights elements of our IT Environment we think you need to know to work with us.

3.1 DOH Information Technology Services Staffing Support

Regardless of whether the Offeror proposes a totally outsourced, partially outsourced, or hosted on DOH Premise solution, expectations for support must be clearly defined.

DOH ITS staffing support hours are:

- Customer & Application Support hours are M-F, 8:00am to 5:00PM Alaska Time
- Network Support hours are M-F, 7:00AM to 5:00PM Alaska Time

Support from DOH ITS required outside of those hours, including evening and weekend batch job support, must be defined and documented. This must include the duties and expectations for DOH ITS staff. All hours of operation **must be expressed in Alaska Time.**

3.1.1 Requirement – Production Operations Phases

The Offeror must:

- Define and document a schedule of hours they plan to operate, including the time zone(s) they plan to operate from;
- Identify hours their staff will work outside of the DOH ITS standard hours, defined in this section;
- Identify the daily schedule of hours during which they expect DOH ITS and DOH Program staff to support the activities under the execution of the proposal;
    - The schedule will include and differentiate hours for end-user access and hours for technical support, including any offline batch or after-hours system maintenance activities.
- Commit to deliver a plan that includes Offeror and DOH agreed upon daily scheduled hours.
    - The plan must also include the schedule of Offeror and State of Alaska observed holidays.
    - SOA Holidays can be found at: https://doa.alaska.gov/calendar/
- ***If solution is to be DOH managed in the Production and Operations*** phase, additional requirements are:
    - The Offeror's proposal must include a solution that requires no regular after-hours system support
    - If the Offeror's proposed solution requires after-hours system support, the Offeror must reach formal agreement via:
        - An accepted Operations Support Model deliverable;
        - The OIT Department Technology Officer for DOH and DOH Assistant Commissioner approval.
        - This agreement must be reached at least 6 months prior to commencement of proposed training activities that precede DOH assuming operational responsibilities for the solution.

3.2 Engagement and Service Delivery Management Services and Standards

Engagement and Service Delivery Management Services includes the activities DOH ITS performs to engage with our DOH Program staff and manage delivery of all IT services. This includes defining the organization's requirements, assisting with DOH IT Governance alignment, change request processes, and applying and managing the correct DOH ITS service-lines for specific DOH ITS initiatives and procurements.

3.2.1 Contract Negotiations ITS Review and Approval

DOH ITS participates directly on the contract negotiations team to review and approve all IT related contract elements further specified in the final contract.

3.2.1.1 Requirement – IT Contract Review

The Offeror must be prepared to work with DOH ITS, Procurement, and Program staff to review and approve all IT related contract elements.

3.2.2 Project Kickoff Service Alignment Conference

As part of project kickoff activities, DOH ITS and Program representatives will meet with the Offeror's execution team to agree upon the necessary DOH ITS service lines required to support the execution of the procurement. This activity will be based on a review of the scope and schedule defined in the solicitation, the proposal, and the final contract.

The outcome will be a list of DOH ITS service lines supporting execution of the procurement and a list of any gaps identified by the Service Alignment Conference team. Gaps identified may include services or products DOH ITS does not support, DOH ITS staffing resource constraints, or other gaps.

3.2.2.1 Requirement – DOH ITS Service Alignment Conference

The Offeror must include project activities to reach agreement with DOH ITS and DOH Program staff on DOH ITS support service lines and identify any gaps. All gaps identified must include a plan of action to address and resolve the gaps.

3.2.3 DOH Service Line Engagement and Planning

Different procurements require customized support activities to succeed within scope, schedule, and resource constraints. To ensure the best outcome, the DOH ITS service lines identified to support the procurement will work with DOH Program staff and Offeror staff to roadmap the service line engagement schedule, review the gaps identified in the service alignment conference, and detail the action plans to address those gaps.

3.2.3.1 Requirement – DOH IT Service Line Engagement and Planning Workshops

The Offeror must include project activities to reach agreement with DOH ITS and Program staff on the service line engagements identified in the Service Alignment Conference deliverables. These activities must roadmap the schedule of service line engagements, identify the service line team members, review the gaps previously identified, and detail the action plans to address those gaps.

3.2.4 DOH Service Line Management Processes and Tools

DOH ITS service line staff will use their standard, defined processes and management tools to document and manage their work (See Sections 2.1 and 2.2 of Information Technology Standards Reference D).

For cost and operational efficiency, DOH ITS prefers that the Offeror align their processes and tools with those of DOH ITS. The Offeror may propose leveraging the DOH processes and tools in their proposal.

3.2.4.1 Requirement – Service Line Management Processes and Tools Alignment

DOH prefers the Offeror be prepared to work with DOH ITS service line management processes and tools. For each DOH IT service line supporting the project, the Offeror must review the applicable processes and tools with DOH ITS and DOH Program staff to align processes and tools of the project with those used by DOH ITS.

If the Offeror and DOH Program staff determine a benefit to using alternate tools, the Offeror must accept the cost of any duplication of effort required of either the Offeror's staff or DOH Program staff to maintain and synchronize requirements, documentation, service requests or other artifacts applicable to the DOH ITS service line.

Whichever tools are selected, the Offeror must document agreed upon decisions made with DOH ITS and DOH Program staff.

3.2.5 DOH Managed Off-site Hosting Scenarios

All DOH Engagement and Service Delivery Management Services and Standards apply to DOH managed off-site hosting scenarios.

3.2.5.1 Requirement

The Offeror must understand and acknowledge 3.2.5.
The Offeror must identify any elements of your proposed solution that will be hosted outside of DOH datacenters.
The Offeror must identify the geographic location of each of those elements.

3.2.6 Software as a Service (SaaS) and Anything as Service (XaaS) Scenarios

All DOH Engagement and Service Delivery Management Services and Standards apply to SaaS/XaaS scenarios.

3.2.6.1 Requirement

The Offeror must understand and acknowledge that all DOH Engagement and Service Delivery Management Services and Standards apply to SaaS and XaaS scenarios.

Identify any elements of your proposed solution that will be fulfilled via Software-as-a-Service delivery models.

3.3 Project Portfolio Management Services and Standards

See IT Reference B—DOH Project Management Requirements.

3.3.1 DOH Managed Off-site Hosting Scenarios

All DOH Project Portfolio Management Services and Standards apply to DOH managed off-site hosting scenarios.

3.3.1.1 Requirement

The Offeror must understand and acknowledge 3.3.1.

3.3.2 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

All DOH Project Portfolio Management Services and Standards apply to SaaS/XaaS scenarios.

3.3.2.1 Requirement

The Offeror must understand and acknowledge 3.3.2.

3.4 Asset Management Services and Standards

Asset Management Services include the activities DOH ITS performs to manage software licensing and other software and information assets. DOH considers all data, software source code, configuration files, binaries, licenses, and configured systems as “assets”. DOH Policies and Standard Operating Procedures require that stewards, responsible for creating and maintaining assets, properly manage these assets. This means asset stewards should apply proper inventory and version control practices to ensure individual assets are identified and version consistent artifact sets can be recreated to support disaster recovery, testing, audit, and other scenarios.

3.4.1 Artifact Version Management

DOH ITS operates a document and code management repository that supports version control (see Information Technology Standards Reference D). The Offeror must transfer ownership of all project artifacts to DOH as part of the scope of work, including the effort to convert/migrate the artifacts into the DOH artifact version management repository. To reduce project overhead and transition costs, the Offeror is encouraged to use the DOH artifact version management repository during project execution.

3.4.1.1 Requirement

Requirements, design documents, source code, configuration files, and binaries that are versioned over time must be managed in one or more version control repositories such that any released version of these artifacts can be retrieved later to rebuild the information system or application. Platforms that support configuration changes via a graphical user interface must support an extract of the changes made that can be loaded into the version control repository and release-managed in an equivalent manner to source code.

3.4.2 Licensing Agreement

3.4.2.1 Requirement

The license shall include, but not be limited to:

- All supporting programs in the most current version;
- All scripts, programs, transaction management or database synchronization software, and other system instructions for operating the system in the most current version;
- All data files in the most current version;
- User and operational manuals and other documentation;
- System and program documentation describing the most current version of the system,
- The most current versions of source and object code;
- Training programs for the State and other designated State staff, their agents, or designated representatives, in the operation and maintenance of the system;
- All performance-enhancing operational plans and products, exclusive of equipment; and
- All specialized or specially modified operating system software and specially developed programs, including utilities, software, and documentation used in the operation of the system.

Ongoing upgrades of the application software and supporting 3rd party programs must be provided through the end of the contract.

Any other specialized software to be integrated into the system, and not covered under a public domain license, must be identified as to its commercial source and the cost must be identified in the Cost proposal. DOH may, at its option, purchase commercially available software components itself.

The contractor must convey to DOH, upon request and without limitation, copies of all interim work products, system documentation, operating instructions, procedures, data processing source code, and executable programs that are part of the system, whether they are developed by the employees of the contractor or any subcontractor as part of this contract or transferred from another public domain system or contract.
The provision of this section related to ownership/support for the product must be incorporated into any subcontract that relates to the development, operation, or maintenance of any component part of the system.

3.4.3 Software Procurement Assurance – Guaranteed Access to Software

3.4.3.1 Requirement

DOH shall have full and complete access to all source code, documentation, utilities, software tools, and other similar items used to develop/install the proposed solution or may be useful in maintaining or enhancing the equipment and solution after it is operating in a production environment.

DOH executive leadership may choose to waive the above requirement upon written request explaining your unique business need. SaaS/XaaS solutions may also request waivers for these requirements (see 3.4.7).

In such cases any of the above-mentioned items not turned over to DOH upon completion of the installation, the Offeror must provide a written guarantee to DOH of uninterrupted future access to, and license to use, those items. The guarantee must be binding on all agents, successors, and assignees of the contractor and subcontractor. State access to source code may be protected by use of a third-party escrow account.

If an escrow account is used, the terms must include at a minimum:

- Update of the source code in escrow as often as required for the source code to reflect the current version of each application of the software licensed by DOH.
- DOH has the right to view or access the source code to:
  - Verify the source code’s completeness and readability of the media.
  - Obtain a copy of the source code in the event of a filing of Bankruptcy where the Offeror is no longer able to provide acceptable service.
  - Obtain a copy of the source code if the Offeror ceases to do business completely, or to do business in the line of business marketplace the system supports.

DOH reserves the right to consult legal counsel as to the sufficiency of the licensing agreement and guarantee of access put forth by the Offeror.

3.4.4 Software Procurement Assurance – Federal Rights

3.4.4.1 Requirement

If a federal grant was used for this solution, the federal government reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use, for federal government purposes, the copyright in any work developed under a grant, sub-grant.

3.4.5 Data Ownership

3.4.5.1 Requirement – Data Ownership

DOH shall have unlimited rights to use, disclose or duplicate, for any purpose whatsoever, all information and data developed, derived, documented, installed, improved, or furnished by the Offeror under this contract.

All files containing any DOH information are the sole and exclusive property of DOH. The Offeror agrees not to use information obtained for any purposes not directly related to this contract without prior written permission from DOH. Offeror agrees to abide by all federal and state confidentiality requirements.
In addition, the Offeror agrees to provide to DOH, at the end or at any time during the contractual period, the data managed by the solution, in whole or in part, in a format agreed upon by both parties.

3.4.6 DOH Managed Off-site Hosting Scenarios

All DOH Asset Management Services and Standards apply to DOH managed off-site hosting scenarios.

3.4.6.1 Requirement

The Offeror must understand and acknowledge 3.4.6.

3.4.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH ITS expects that by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DOH ITS Asset Management Services and Standards.

3.4.7.1 Requirement

If proposing SaaS/XaaS components for all or part of the solution, the Offeror's proposal must comply with all Asset Management Services and Standards requirements.

The Offeror may propose leveraging variations or exceptions under this subsection, *Software as a Service Scenarios (SaaS) and Anything as a Service (XaaS)*. If the Offeror wishes to leverage variations or exceptions, these must be defined. If exceptions are to be requested please clearly outline

- Which requirement you are seeking an exception for
- What alternative measure you are offering in its place
- How the department's interests will be protected, even in the event the Offeror goes out of business or files for bankruptcy

3.4.7.2 Requirement – Data Stewardship

The Offeror will maintain Alaska's data in the solution for the life of the contract. The Offeror must explain how data will be archived for the solution. Turnover requirements will be negotiated between DOH and the Offeror to ensure that all DOH data will be returned to DOH in a cooperative manner at the close of the contract or the decommissioning of the solution. DOH data may include; deliverables, reports, configuration details, business requirement documents, test plans, scripts, and results.

3.4.7.3 Requirement – Geographic Location Identification

The Offeror must identify the geographic location of any non-DOH hosted external information systems that receive, process, store, or transmit proposed solution data.

3.5 Systems Integration and DDI Services and Standards

DOH ITS provides a full range of Systems Integration and Design, Development, and Implementation (DDI) Services. These services follow DOH standards to ensure maximum leverage of staff and other resources and ensure scalability. DOH expects the Offeror to understand and align their proposal and activities with DOH Systems Integration and DDI Services and standards.

The most noted points of integrations include:

- Our department's information exchange architecture;
- Master data management;

- Integrated Resource Information System (IRIS) and Alaska Data Enterprise Reporting (ALDER) integration;
- Authentication and Single Sign-On.

Maintaining alignment will be an ongoing activity during the project. However, the Offeror must demonstrate how they anticipate reaching alignment within their proposal.

3.5.1 Information Exchange Architecture

To simplify the effort and reduce costs of DOH systems implementation and long-term operations, DOH has implemented an Enterprise Service Bus (ESB) that supports system integration and information exchange. Additionally, DOH has partnered to create an Alaska statewide Health Information Exchange (HIE). Together, the ESB and the HIE can substantially reduce the operational complexity of moving data between systems hosted on-premise or in the cloud.

3.5.1.1 Requirement

Data exchange interfaces must leverage the DOH Enterprise Service Bus and/or the statewide HIE, where applicable.

The Offerer must describe

- What interfaces and data exchange processes do you anticipate implementing with the HIE?
  - If you do anticipate implementing these processes, please describe how the proposed solution would transfer data to and from the HIE, as applicable.
- What interfaces, data exchange processes and services do you anticipate implementing via the DOH Enterprise Service Bus (ESB)?
  - If you do anticipate implementing these processes, please describe how the solution would transfer data using this method?
- Your architectural approach to transferring data sets to/from your system. Include both single-record/case and batch transfer scenarios.

3.5.2 Master Data Management

DOH has implemented master data management services for client/consumer/person demographic records via the DOH Master Client Index (MCI). The MCI connects client demographic records across applications and systems.

Solutions that create, read, or update client, consumer, or other person demographic data must integrate with the MCI to ensure their demographic records are registered in the MCI and appropriately merged with matching client records in the index.

Such solutions must integrate with the DOH MCI and ensure the end-users of the solution can leverage the Person service operations to register and maintain their person demographic records in the MCI. This must include interactions that update the MCI when record duplication, deactivation, and similar record management scenarios occur within the scope of the Offeror’s proposed solution.

3.5.2.1 Requirement – Master Client Index (MCI) Integration

The Offeror must integrate their proposed solution with the DOH Master Client Index (MCI) if the Offeror’s proposed solution will store person demographic data of clients, members, beneficiaries, or other individuals who:

- Apply for or receive DOH program services or benefits; or
- Are the subject of a DOH registry; or

- Are a participant in a case, filing-unit, or other group for which DOH expends funds or must measure services.

The Offeror must:

- Indicate whether your proposed solution will include demographic records for individuals.
- Indicate whether your proposed solution will integrate with the DOH Master Client Index.
  - If your solution will not integrate with the DOH MCI, please indicate why.
  - If your solution will integrate with the DOH MCI, please describe your process to register and merge client demographic information records with the MCI.
    - Include the technical approach and the high-level search, create, update, and synchronization procedures for managing MCI relevant demographic data in your solution.

3.5.3 IRIS and ALDER Integration

DOH uses the State of Alaska Enterprise Resource Planning (ERP) system, IRIS, for managing finance, accounting, property-asset, and HR management functions. DOH uses the State of Alaska ALDER data warehouse for reporting and extracting finance, accounting and HR data.
Solutions that include these functions should plan for a gap analysis to determine the appropriate integration approach that avoids duplication of services and addresses developing and integrating complementary solution services and functions.

3.5.3.1 Requirement

Offerors whose proposed solution includes finance, accounting, and HR functions must plan to conduct a gap analysis activity with DOH ITS, DOH Program staff, and Department of Administration Division of Finance IRIS support subject matter experts. This analysis is to determine which system will own which processes, how the systems will integrate and where the data will live.

Offeror's proposal must include activities to support this gap analysis and associated DDI activities to interface between IRIS, ALDER and the proposed solution.

3.5.4 Authentication and Single Sign On

DOH has established a standard authentication platform, using Microsoft's Active Directory (AD) to support authentication for DOH hosted systems.

DOH has established a standard federated authentication platform, Microsoft Active Directory Federation Services (ADFS), to support single sign on authentication scenarios for DOH employees who use systems external to the department that cannot integrate with the DOH Active Directory.

Integration with either of these methods provides a uniform authentication mechanism for DOH staff and sponsored external partner/contractor staff to manage authorized access to department information systems. Leveraging the DOH AD allows the Offeror's solution to inherit the account management, authentication, and audit-logging features of the DOH AD to validate authorized access and meet several technical security controls.

3.5.4.1 Requirement – Single Sign-On and Authentication

The Offeror must integrate their solution with the Alaska DOH Active Directory or DOH Active Directory Federated Services (ADFS). The integration must support authentication access requests prior to authorization.

The Offeror will include cost and activities in their proposal to support the DOH AD integration.

3.5.5 Technical Services and Development Platform

DOH expects the Offeror to align their proposal with this DOH standard technical services platform to the maximum extent possible.

DOH ITS operates a leading software development lifecycle (SDLC) management platform. See IT Reference D for details on this tool. To reduce project overhead and transition costs, the Offeror is encouraged to consider using the DOH artifact version management repository.

3.5.5.1 Requirement – Development Platform

The Offeror will use the software identified in IT Reference D for the development and deployment of this application. The Offeror must state which version the application components are designed in and how this solution will be accessed in the DOH environment. You will need to identify what skills and expertise would be needed to support your proposed infrastructure.

For each non-DOH standard software component in the proposed solution:

- Describe the purpose of the non-standard component;
- Propose a component in the DOH IT standards that could be used instead of the non-standard component;
- Include an optional cost adjustment to implement the solution using that DOH standard component within the cost proposal section of the RFP;
- If there is no DOH standard software component identified that meets the function of the non-standard component proposed, identify a Microsoft component that meets the purpose of the non-standard proposed component;
- Include an optional cost adjustment to implement the solution using that Microsoft component within the cost proposal section of the RFP; and
- If no Microsoft component exists that meets the purpose of the proposed non-standard component, indicate there is no equivalent component available.

3.5.5.2 Requirement – Software Development Lifecycle (SDLC)

The Offeror must apply a methodology that demonstrates key elements of the SDLC, including:

- Gathered and validated requirements and acceptance criteria artifacts;
- Documented and validated design artifacts;
- Documented development and build tools and processes;
- Versioned and managed development artifact change sets;
- Documented deployment and promotion processes for moving builds and release candidates from lower environments to higher-confidence environments and ultimately production (e.g., development > system integration test > user acceptance test > production & training);
- Documented quality assurance, system test, and user acceptance test script and results artifacts;
- Documented release management procedures.

The Offeror must use a set of industry standard tools to track and manage artifacts of the SDLC and must align this toolset with the standard DOH SDLC tools.

3.5.5.3 Requirement – Secure Systems Development Lifecycle

The Offeror must complete software development in compliance with DOH Secure Systems Development Lifecycle, including:

- **Secure Coding** - The Offeror shall disclose what tools are used in the software development environment to encourage secure coding.
- **Disclosure** - The Offeror shall document in writing to the Purchaser all third-party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or proprietary.
- **Evaluation** - The Offeror shall make reasonable efforts to ensure third party software meets all the terms of this agreement and is as secure as the custom code developed under this agreement.
- **Source Code Scanning -** The Offeror shall work with DOH staff to facilitate static code scanning for all product and 3rd party files using a DOH provided scanning solution.
- **Hosting Environment Hardening** – The Offeror shall work with DOH staff to ensure that any hosting environment utilized complies with department adopted standards for security hardening.
- **Vulnerability and Penetration Testing** – for SaaS and XaaS environments, the Offeror shall facilitate requests for 3rd party vulnerability and/or penetration testing of DOH solutions.

3.5.6 DOH Managed Off-site Hosting Scenarios

All DOH Systems Integration and DDI Services and Standards apply to DOH managed off-site hosting scenarios.

3.5.6.1 Requirement

The Offeror must understand and acknowledge 3.5.6.

3.5.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH IT expects that, by owning ongoing maintenance and technical operations, SaaS solutions implicitly provide a limited degree of freedom to deviate from DOH IT Systems Integration and DDI Services and Standards. Specifically, when federal funding rights do not apply, and when DOH is not performing technical services administration within the SaaS hosting environment, SaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation.

3.5.7.1 Requirement

When federal funding rights apply, see *section 3.4.4 Software Procurement Assurance – Federal Rights*, the Offeror's proposed solution must employ DOH IT Systems Integration and DDI Services and Standards compliant platform components. This requirement supports State of Alaska maintenance risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DOH must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future maintenance risks.

3.6 Systems Operations and Administration Services and Standards

System Operations and Administration Services includes the activities DOH ITS performs to support technical system operations and system administration. This section describes information system administration services that support solutions operating in production.

3.6.1 Administration Services and Standards

DOH ITS operates and manages technical services for DOH information systems and applications. This includes ongoing administration, configuration monitoring and security patching of the underlying software components of the solution.

See IT Reference D for the list of technical service components administered by DOH IT within the System Operations and Administration Services service line.

3.6.1.1 Requirement – Centralized Technical Administration

The Offeror must understand that information technology administration duties are restricted to qualified individuals within the centralized DOH ITS section. DOH Program staff outside the DOH ITS section are not authorized to manage or administer technical information technology services. Examples of technical services include, but are not limited to administration of: relational database management systems (Oracle, SQL Server, MySQL, PostgreSQL, etc.); application servers (ASP.NET, JEE, PHP, etc.), and desktop and server operating systems.

Non-ITS, DOH Program staff may be delegated administration of business services via secured, audited user-interfaces in the application, such as interfaces to create user accounts within the application, assign security roles within the application, maintain code-lookup tables, and other business administration functions. All business administration changes must be completed via a privileged, secured application user-interface that logs all data changes and which user made the change.

The Offeror must validate all technical administration designs with DOH IT stakeholders in the System Operations and Administration Services service line.

The Offeror must include appropriate documentation and training for DOH ITS staff in the technical services administration for the proposed solution.

3.6.1.2 Requirement – Authorized Access

The Offeror must follow DOH standard operating procedures for obtaining and terminating access to DOH facilities and systems. To support proper access management, the Offeror must notify the DOH contract administrator of any personnel transfers or termination of Offeror personnel, including sub-contractors, who possess DOH credentials and/or badges, or who have DOH information system privileges, within fifteen (15) calendar days. Notification must be in writing. This personnel transfer and termination notification requirement may not be extended and does not supersede other Offeror personnel notification requirements with stricter timelines within the contract. (NIST 800-53 r4 PS 07 D)

3.6.2 DOH Managed Off-site Hosting Scenarios

All DOH Systems Operations and Administration Services and Standards apply to DOH managed off-site hosting scenarios.

3.6.2.1 Requirement

The Offeror must understand and acknowledge 3.6.2.

3.6.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH ITS expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DOH ITS Systems Operations and Administration Services and Standards. Specifically, when federal funding rights do not apply, and when DOH is not performing technical services administration within the SaaS/XaaS hosting environment, SaaS/XaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation.

3.6.3.1 Requirement

When federal funding rights apply, *see section 3.4.4*, the Offeror's proposed solution must employ DOH ITS Systems Integration and DDI Services and Standards compliant platform components. This requirement supports State of Alaska operational risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DOH must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future operational risks.

3.7 Information Security Compliance and Privacy Services and Standards

Information Security Compliance and Privacy Services include the activities DOH ITS performs to support legal compliance with information security, privacy, and ongoing development/maintenance of security policy and practice. DOH maintains a robust information security compliance and privacy program. This section describes the information security compliance and privacy services and standards applied throughout the lifecycle of each DOH information system.

3.7.1 Data Retention/Destruction

Destruction of Electronic Protected Health Information (ePHI) and Personally Identifiable Information (PII) on electronic media requires that the organization employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

3.7.1.1 Disposing of Printed Information

All protected printed media (ePHI, PII, PI, PCI, CJI, etc.) must be disposed of in a manner consistent with the guidance provided by the NIST Special Publication 800-88 Revision 1 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf).

3.7.1.2 Disposing of Information on Electronic Media

All protected electronic media (ePHI, PII, PI, PCI, CJI, etc.) must be disposed of in a manner consistent with the guidance provided by the Department of the Army's brief, Cybersecurity: Sanitization of Media (https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6681_Pam25-2-8_WEB_FINAL.pdf#:~:text=The%20procedures%20in%20this%20chapter%20establish%20the%20requirement,the%20disposal%20and%20handling%20of%20hazardous%20IT%20waste) and NIST Special Publication 800-88 Revision 1 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf). Disposed of electronic media must receive a Certificate of Media Disposal or agreed upon proof of disposal for each device disposed.

3.7.1.3 Requirement – Record Retention

The Offeror must comply with the DOH policies and procedures for record retention and disposal of sensitive information (IT Reference F—Data Destruction Information and References), if applicable.

3.7.1.4 Requirement – Data Destruction

The Offeror must provide procedures and agree to all data (including test data) destruction when contract ends if continuing operations and maintenance is not provided by the contractor.

3.7.2 Security Controls

Department, State, and Federal security standards are enforced through State of Alaska and DOH policy and procedure. The procedures leverage FIPS 199 information security categorization and NIST 800-53 information security controls documentation. The DOH Governance, Risk, and Compliance system serves as the system of record to capture this documentation in an "authorization package".

3.7.2.1 Requirement – Authorization Package

Within the proposed scope of work and activities, the Offeror must:

- Work with the Department Security Office (DSO) to document the approach, methodology, roles, responsibilities, processes, and tasks the Offeror will assume to complete the authorization package;
- Develop and submit a complete Authorization Package for review and approval by the DSO;
- Submit to the DOH Security Designee, a thoroughly completed Authorization Package for review and comment within four (4) weeks of the project's initiation and receipt of the Authorization Package questionaire.
  - Offeror shall respond to clarification questions within two (2) weeks of receipt of DOH comments on the Authorization Package.

Security controls are reviewed for risk regardless of whether an application/solution is hosted on premise or elsewhere. A paper version of the Authorization Package is included in IT Reference H – DOH Sample Security Authorization Package.

3.7.2.2 Requirement – Code Vulnerability Scanning

DOH employs a code vulnerability scanning engine. The Offeror shall process all scannable code through the DOH static code vulnerability scanning engine. Findings from the code vulnerability scan will be attached to the systems Authorization Package for review and acceptance from the DOH Department Security Office (DSO).

3.7.2.3 Requirement – Security Control Verification

After the Authorization Package is complete, it is subject to review and acceptance from the DOH Department Security Office (DSO). Approval to operate in the DOH environment is predicated on acceptance of the Authorization Package responses as well as compliance with the processes outlined in *section 3.5.5.3* of this document. These processes may require changes and updates to the system by the Offeror in order to comply with regulatory requirements.

The Offeror must plan activities to work towards security compliance requirements and accommodate an appropriate number of remediation cycles to address any identified defects.
Please note, although workload varies in proportion to the size of the solution, we have found that most small to medium size solutions require 80 to 120 hours to complete the initial security control responses.

3.7.2.4 Requirement – Business Associate Agreement

If data is determined to be ePHI, the DOH Business Associate Agreement must be signed at contract. Other types of data must be treated with appropriate confidential data handling and may be covered by a data usage agreement.

3.7.2.5 Requirement – Authority to Operate

Once all security compliance is established via an approved Authorization Package and signed Business Associate Agreements (BAA) or data usage agreements (as applicable), the solution will be granted an Authority to Operate (ATO) by the DOH designated Division Data Owner, the Department Chief Information Security Officer, and the OIT Department Technology Officer for DOH. The Offeror must plan activities and milestones that support obtaining the ATO prior to production rollout.

The Offeror must plan for delays associated with a solution's inability to initially obtain ATO. These delays must take into consideration the business's implementation targets. It is imperative that authorization package responses be scheduled with ample time for completion, DSO review, and mitigation to not negatively affect the business's implementation targets.

3.7.3 Auditing and Logging Integration

For logging and audit, DOH uses an industry standard Security Information and Event Management (SEIM) system. All systems are required to be capable of logging and auditing in a concise summary that can be easily integrated into the DOH SEIM. The package produced by the application must be inclusive of all the data for who is accessing, reading, and writing data.

3.7.3.1 Requirement

The Offeror's proposed solution must integrate with DOH's SEIM infrastructure. The Offeror's proposed solution must include activities to collaborate with DOH ITS in establishing log collection activities for standard log formats and customizing log parsing for non-standard log formats.

3.7.4 Data Security

Sensitive and/or confidential data includes (but is not limited to) Electronic Protected Health Information (ePHI) as defined in the Federal Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII) as defined by the US Privacy Act, Personal Information (PI) as defined in the State of Alaska Personal Information Protection Act (APIPA), and Payment Card Information (PCI) as defined by Payment Card Industry Data Security Standard (PCI DSS), and Criminal Justice Information (CJI) as defined by the Federal Bureau of Investigation.

3.7.4.1 Requirement

The Offeror's proposed solution must include, define how they will ensure all sensitive, confidential, and/or restricted data is encrypted in-transit and at-rest. Criminal Justice Information Systems (CJIS) and those systems requiring MARS-E compliance must meet these encryption requirements using a FIPS 140-2 certified product.

DOH owns the data and can demand it at any time. Proposed solutions that leverage public or private data sources resulting in DOH business decisions – especially where the business decision reflects a DOH legal jurisdiction related to due process – must ensure DOH retains access to all the data required to support the decision.

3.7.4.2 Requirement

The Offeror's proposed solution must include, define, and validate the capabilities to return DOH owned data to DOH.

Recovery Point Objective (RPO) refers to the maximum amount of data loss – typically defined in terms of time – that may occur in the event of a system failure and consequent rollback to a known consistent state. *Recovery Time Objective* (RTO) refers to the maximum time that may pass between the point in time when a system failure occurs and the point in time when the system is recovered.

3.7.4.3 Requirement – Recovery Point and Recovery Time Objectives

The Offeror's proposed solution must include and define RPO and RTO capabilities. If there are cost-add RPO and RTO capbilities available that exceed the assumptions, scope and cost of your proposal, please identify those options.

3.7.5 Integration Security Controls

When system interfaces (data exchange between systems) and integration requirements exist for a system, integration security controls must be documented and implemented to ensure the confidentiality, integrity and availability of the data for all valid business consumers. To simplify the DOH operating environment, and ensure that many of the required controls are met at the least cost, DOH has implemented an Enterprise Service Bus (ESB) and partnered to leverage the Alaska Health Information Exchange (HIE). Both the ESB and the HIE provide architectural system integration and data exchange services that can be leveraged for re-use by On-DOH premise and Off-site hosted information systems.

3.7.5.1 Requirement

The Offeror must demonstrate leveraging existing DOH security control investments by integrating with DOH systems via the DOH ESB and/or the statewide HIE.

The Offeror must complete and submit to the DSO for review, one Interface Risk Assessment Worksheet, per interface, outlining the specifications and security components of said interface.

3.7.6 DOH Managed Off-site Hosting Considerations

All DOH Information Security Compliance and Privacy Services and Standards apply to DOH managed off-site hosting scenarios.

3.7.6.1 Requirement

The Offeror must understand and acknowledge 3.7.6.

3.7.7 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH IT expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DOH IT Information Security Compliance and Privacy Services and Standards. Specifically, when federal funding rights do not apply, and when DOH is not performing technical services administration within the SaaS/XaaS hosting environment. SaaS/XaaS solutions may employ non-compliant infrastructure and non-compliant platform components in their design and implementation provided those infrastructure and platform components meet the security compliance requirements of the information managed by the SaaS/XaaS, and if applicable, the requirements in the DOH Business Associate Agreement.

The Offeror's SaaS/XaaS proposal should include encrypting and securing any confidential data, and adopting the latest security measures available to prevent unauthorized access. Security controls include patching application/operating system/firmware, minimizing administrative controls, and completing a DOH Authorization Package and submitting the Authorization Package to our department security office for review and approval, per the requirements under section 3.7.2. The authorization package must be approved before systems or applications are authorized for production. The Offeror assumes the responsibility for any and all authentication and account creations or modifications.

3.7.7.1 Requirement – SaaS/XaaS Security Responsibilities

Proposals for SaaS/XaaS offerings should include a clear delineation of the system's security mechanisms and configurations the Offeror will be responsible for, and those for which DOH will be responsible.

The Offeror is also responsible for service patching and completing an RSA Authorization Package.

3.7.7.2 Requirement – SaaS/XaaS Logging and Auditing

For proposals that include SaaS/XaaS solutions that may manage confidential data, the SaaS/XaaS must include a logging and auditing solution. All components and systems within the Offeror's proposal are required to be capable of logging all data access requests to read or write data, including the requesting user id. The audit-log data that is produced by the application must include all the data to identify who created, accessed, updated, and deleted data and when each event occurred.

The application must be readily capable of generating logging and auditing reports in a concise summary that can be easily subject to research by indexing. The industry standard solution the Offeror chooses to implement must be described, including how responsible DOH entities (DSO, Division Data Owner) will be able to access it to perform oversight related tasks.

3.8 Enterprise Desktop and Mobility Services and Standards

Enterprise Desktop and Mobility Services include the activities DOH ITS performs to define, deploy, and support the DOH enterprise desktop and mobility endpoints. DOH maintains an enterprise desktop for all datacenter and field-deployed hosts. The desktop is based on a golden image, created and maintained based on input from the integration and development, information security, and operations service lines and standards. This section describes the procurement relevant enterprise desktop services and standards used to manage and maintain DOH end-user desktops.

3.8.1 Desktop Access and Configuration

DOH utilizes Dell workstation and server hardware. Offerors should propose solutions that are device independent. The DOH Enterprise Desktop is a supported version of Microsoft Windows, with the supported web browser, productivity suite and other common, standard or approved software components and applications. See IT Reference D for currently supported hardware and operating system(s).

DOH is a least privilege environment and staff are not granted elevated privilege without individually reviewed and approved security policy waivers. DOH Program staff work with DOH ITS to request, review, and determine compatibility, redundancy, and fit of non-standard software. DOH Program staff are not permitted to install, nor can they independently authorize the installation of, new software components or applications on the desktop. Offerors should avoid solutions that require customization of the DOH Enterprise Desktop.

If the Offeror's proposed solution requires use of a desktop web browser, the solution must be browser independent and be fully capable of functioning with the standard browser in the DOH Enterprise Desktop Standards. See IT Reference D for currently supported web browser version(s).

If the Offeror's proposed solution requires use of desktop productivity suite software, the solution should be fully capable of functioning with the standard desktop suite in the DOH Enterprise Desktop Standards. See IT Reference D for currently supported desktop productivity software.

3.8.1.1 Requirement – Desktop Access and Configuration

The Offeror must propose a solution that supports the DOH currently deployed desktop operating system (OS) and does not require elevated privileges for the end-user on their desktop. The Offeror must include activities in their proposal to establish whether each and every end-user desktop software component required to support the proposed solution is a part of the standard DOH Enterprise Desktop. The Offeror must include activities in their proposal to work with the DOH Enterprise Desktop team to integrate each non-standard software component. These activities must include working with DOH Enterprise Desktop service line staff to:

- Accept or identify acceptable alternatives for each non-standard software component.
- Establish installation, configuration, and support procedures for each non-standard software component.

3.8.1.2 Requirement – Web Browser Compatibility

The Offeror must plan to support proposed solution compatibility with DOH' currently deployed web browser version(s). The required functionality of the solution must be fully supported, or the Offeror must include in their proposal the plan, cost, and activities to make the proposed solution fully supported. The Offeror must review the DOH standard browser vendor's support lifecycle material, published at the time of proposal. The Offeror's proposal must include a plan to migrate or upgrade any browser versions that will become unsupported during the execution of the contract (per the vendor's published support lifecycle material).

3.8.1.3 Requirement – Desktop Productivity Software Compatibility

The Offeror must plan to support DOH currently deployed desktop productivity suite version(s). The Offeror must review the DOH standard desktop productivity suite vendor's support lifecycle material, published at the time of proposal. The Offeror's proposal must include a plan to migrate or upgrade any versions of productivity suite software versions that will become unsupported during the planned execution of the contract (per the vendor's published support lifecycle material). The Offeror must include in their cost proposal, the optional contingency cost of one unanticipated productivity suite software version compatibility upgrade for the proposed application.

3.8.1.4 Requirement – Other Desktop Software and Components

The Offeror must delineate all the desktop software, access, and configuration requirements of the application not addressed elsewhere in the Enterprise Desktop Services and Standards section.

3.8.2 Mobile Devices and Tablets

Mobile devices for DOH are:

- Dell Windows based Tablets
  - Configured with the latest version of Microsoft Standard browsers
  - Web applications are to be Browser version independent which means they support current versions of Internet browsers for Microsoft, FireFox, and Google Chrome.
  - Software should not be dependent on a specific version of MS Office Suite.
    - We move the organization as a whole during Department wide upgrades.
- Apple iOS based Tablets and Smart Phones
  - Configured with the latest version of Safari and Google Chrome.
  - Software should not be dependent on a specific version of MS Office Suite.
    - We move the organization as a whole during Department wide upgrades.

Dell and Apple Devices are configured with the latest operating systems or 1 version previous.

The DOH mobile device strategy is evolving rapidly and is not stable or complete for supporting the ability to store or transmit confidential data. If their solution includes mobile device end-points, Offerors should plan for extensive engagement with the DOH Enterprise Desktop and Mobility service line

3.8.2.1 Requirement

The Offeror must plan appropriate activities to support mobile device endpoint integration. These activities must include selecting and adapting mobile solution software components to a DOH standard mobile device that supports all security compliance requirements of the data being stored on or transmitted to/from the mobile device endpoints.

3.8.3 DOH Managed Off-site Hosting Scenarios

All DOH Enterprise Desktop and Mobility Services and Standards apply to DOH desktops managed off-site hosting scenarios.

3.8.3.1 Requirement

The Offeror must understand and acknowledge 3.8.3.

3.8.4 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH IT expects that, by owning ongoing maintenance and technical operations, SaaS/XaaS solutions implicitly provide a limited degree of freedom to deviate from DOH ITS Systems Operations and Administration Services and Standards. Specifically, when federal funding rights do not apply, and when DOH is not performing technical services administration within the SaaS/XaaS hosting environment, SaaS/XaaS solutions may employ embedded, non-compliant, end-user desktops within the SaaS/XaaS, provided that:

(a) Equivalent desktop security controls are proposed and implemented to those present on the DOH Enterprise Desktop, and
(b) The SaaS/XaaS supports DOH Enterprise Desktop supported standard software for accessing SaaS solution desktops. See IT Reference D for supported software.

3.8.4.1 Requirement

When federal funding rights apply, *see section 3.4.4*, the Offeror’s proposed solution must employ DOH ITS Enterprise Desktop Services and Standards compliant platform components. This requirement supports State of Alaska operational risk mitigation in the event the Offeror determines to discontinue the service at a future date, and DOH must assume maintenance and/or operations. If the Offeror cannot meet this requirement, they may propose an operational contingency statement the State of Alaska can consider as a viable risk mitigation alternative to assuming the future operational risks.

3.9 DOH Hosting and Datacenter Services and Standards

DOH Hosting and Datacenter Services include the activities DOH ITS performs to design, implement, and operate standard information technology infrastructure and platform offerings in DOH managed datacenters. This includes both the primary DOH data centers in Juneau and Anchorage, as well as satellite facilities in secondary locations that require similar services to meet disaster recovery and business continuity requirements. Relying on robust, appliance style hardware with advanced storage area network data deduplication and replication functions, advanced firewalls, and virtualized host infrastructure, DOH datacenter infrastructure provides the flexibility to rapidly deploy new hosts in a physically and logically secure environment.

Please see the DOH Hosting and Datacenter Service Standards section of Reference D - Information Technology Standards,

3.9.1 On-DOH Premise Hosting Considerations

DOH provides and maintains a standardized set of infrastructure and platform services to deliver a full-service private cloud offering, leveraging the State of Alaska Wide Area Network to span two geo-redundant data centers located in Juneau and Anchorage.

3.9.1.1 Requirement

Proposals for hosting the solution on the State network should include the responsibilities and communication process for DOH IT for development, test, and production environments and follow DOH directives for migration to production.

The Offeror will not have direct access to the production environment on the State Network and must work through the appropriate protocols to effect change appropriately. The Offeror must work with DOH IT for all security mechanisms, including patching updates.

3.9.1.2 Requirement

The Offeror will use the software identified in IT Reference D for the hosting of this application. The Offeror must state which version the application components are implemented in and how this solution will be accessed in the DOH environment. The Offeror will need to identify what skills and expertise would be needed to support the proposed infrastructure.

3.9.2 DOH Managed Off-site hosting considerations

All DOH Hosting and Datacenter Services and Standards must be followed and applied to DOH managed off-site hosting scenarios.

3.9.2.1 Requirement

The Offeror must understand and acknowledge 3.9.2.

3.9.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

DOH Hosting and Datacenter Services and Standards do not support Software as a Service (SaaS) or Anything as a Service (XaaS) offerings. Offerors proposing SaaS/XaaS solutions must provide and manage their own hosting and datacenter services. Offerors may subcontract these hosting and datacenter services, provided appropriate security agreements, such as a Business Associate Agreement or data usage agreement, are in place for the data being stored in or transported to/from the subcontracted hosting datacenter.

3.9.3.1 Requirement

The Offeror must understand and acknowledge 3.9.3.

3.10 DOH Wide Area Network, Telecommunications, and Perimeter Security Services and Standards

DOH Wide Area Network, Telecommunications and Perimeter Security Services include the activities DOH IT performs to integrate the DOH LAN with the State of Alaska (SOA) wide area network, telecommunications and perimeter security managed by Department of Administration (DOA) Office of Information Technology (OIT). These services are built upon a layered architecture design that includes VPN, ingress/egress, network address translation and port address translation services and capabilities provisioned, managed, and maintained by OIT. To maximize the security capabilities of these services and ensure systems maintain compliance with system security requirements and industry standards, DOH ITS and OIT follow strict change management processes that include reviews and approvals for all information systems and applications changes that impact WAN, Telecommunications, and Perimeter Security. See 3.7 Information Security Compliance and Privacy Services and Standards for additional details regarding security compliance. Work and service requests reflecting these changes are managed via an OIT ticketing system (Reference D, section DOH Wide Area Network, Telecommunications and Perimeter and WAN Security Service Standards).

3.10.1 State WAN and Bandwidth

The State Wide Area Network (WAN) is maintained at the enterprise level by the Department of Administration (DOA)/Office of Information Technology (OIT); WAN connectivity and bandwidth available to grantees via the WAN is controlled by contractual agreements between OIT and local internet providers. Some rural areas experience internet connection speed as low as 56k and frequent network disruptions. Changes to the State WAN, for example new ingress points, IPSEC tunnels, etc., require both DOH IT Security Office and DOA State Security Office review and approval.

Due to the great distances between communities in Alaska and the lack of road connections in most areas of the state, electrical power is locally generated in most parts of the state. While Anchorage has redundant transmission lines from its electrical generating plant and rarely experiences system-wide outages, local outages can occur due to weather-related conditions or damage to the distribution system. Electrical power in most other parts of the state is subject to periodic system-wide outages as well as localized outages. Broadband service is available in most of the larger communities in Alaska. However, in communities located off the road system that rely on satellite connections, a T1 line is a significant expense.

3.10.1.1 Requirement

The Offeror must understand and acknowledge Bandwidth constraints and denote any performance degradation that could be encountered by their solution and suggested mitigations. Offeror must note any services requiring communications outside the State of Alaska WAN.

3.10.2 DOH Managed Off-site Hosting Scenarios

DOH operates only within the State of Alaska Wide Area Network and uses only State of Alaska provided telecommunications services. Proposals requiring new State of Alaska Wide Area Networks or telecommunications (phone, fax, etc.) services must be approved by the OIT Department Technology Officer.

3.10.2.1 Requirement

The Offeror must understand and acknowledge 3.10.2.

3.10.3 Software as a Service (SaaS) and Anything as a Service (XaaS) Scenarios

Offerors proposing SaaS/XaaS solutions must provide and manage their own Wide Area Network and telecommunications services to support any required network and telephony services of the proposed solution. The proposed solution must grant access to the DOH Program staff via a supported DOH desktop web-browser, or a desktop thin client, or similar DOH approved and supported software. See Reference D - Information Technology Standards.

3.10.3.1 Requirement

The Offeror must understand and acknowledge 3.10.3.

3.11 Accessibility

Alaska Administrative Orders 262 and 129 establish the Americans with Disabilities Act (ADA) compliance program in accordance with the American with Disabilities Act (42 U.S.c. 12101 et seq.). DOH expects the Offeror to propose and deliver solutions that meet the Alaska ADA program.

3.11.1 ADA Compliance for Access to Information Systems and Applications

DOH requires ADA compliant application access.

Two important resources provide guidance for web developers designing accessible web pages. One is the Section 508 Standards, which Federal agencies must follow for their own new web pages. To learn more about the Section 508 Standards the Access Board maintains information on its website at www.access-board.gov.

The second is the General Services Administration information for web developers interested in accessible web design at https://www.gsa.gov/technology/build-websites-and-digital-services. This information was developed in conjunction with the Access Board, the Department of Justice, and the Department of Education
A more comprehensive resource is the Web Content Accessibility Guidelines developed by the Web Accessibility Initiative. These guidelines help designers make web pages as accessible as possible to the widest range of users, including users with disabilities. The Web Accessibility Initiative is a subgroup of the World Wide Web Consortium — the same organization that standardizes the programming language followed by all web developers.

Information for web developers interested in making their web pages as accessible as possible, including the current version of the Web Content Accessibility Guidelines (and associated checklists), can be found at https://www.w3.org/WAI/standards-guidelines/wcag/.

3.11.1.1 Requirement

DOH requires that web pages and web applications be accessible for ADA compliance. This includes online forms and tables which must be made so that those elements are accessible. Documents on the website must be provided in HTML or a text-based format in addition to any other formats.

It is the responsibility of the Offeror to ensure that the web page\web application features are ADA compliant.

3.12 State of Alaska DOH MITA Standards and Department IT Technology Standards

The Department is migrating toward an enterprise Service Oriented Architecture (SOA) consistent with Medicaid Information Technology Architecture (MITA) and the Centers for Medicare and Medicaid Services (CMS) Seven Conditions and Standards (7C&S) outlined below:

- Modularity
- MITA Condition
- Industry Standards Condition
- Leverage Condition
- Business Results Condition
- Reporting Condition
- Interoperability Condition

3.12.1 MITA Requirements

The Offeror’s proposal must respond to the questions on how their solution addresses or does not address each of the 7C&S.

Reference B
Project Management Requirements

State of Alaska
Department of Health

TABLE OF CONTENTS

Introduction

As part of the Department of Health's (DOH) Project Portfolio Management, this project must address the standards and best practices to support the decisions at not just the Division, but the Department level for IT resourcing, support, and project performance.

Section 1 of this document, the Preliminary Project Management and Work Plan, outlines the elements you are required to respond to in your proposal.

Sections 2 through 6 are narrative explanations of the items referenced in Section 1. They provide greater detail as to the expectations should your proposal be selected.

1 Preliminary Project Management and Work Plan

1.1 Project Life Cycle Methodology

The contractor will adhere to a Project Life Cycle Methodology and must state and define what that methodology is and how they will manage the Project Artifacts and Development/Configuration required by the DOH IT Project Portfolio and best practices.

Project artifacts must be managed in a document repository throughout the life of the contract. The repository must be accessible to all project team members and the department's IT Project Management Office. The department will provide a SharePoint site that can be used to track project status, progress, issues, schedules, and as a documentation repository.

The Project Life Cycle Methodology proposed must encompasses both project and product activities. This includes the management of any Application Development/Configuration, Data Migration/Conversion, and rollout/implementation activities.

1.2 Preliminary Project Management Narrative and Work Plan

As part of the proposal the contractor must provide the Preliminary Project Management Narrative (how the work, stakeholders, and expectations will be managed) and a prospective work plan. A prospective schedule/work breakdown structure (WBS) by itself addresses the schedule.

The contractor must provide a narrative of their management of the Project Life Cycle.

The contractor must agree they will complete the Master Project Management Plan and Master Project Work Plan Schedule as part of their project planning activities.

The contractor may propose an alternate schedule with appropriate justification and level of detail for any proposed alternatives.

The Preliminary Project Management Plan (narrative/document for this proposal) must include how the following project subject/process areas will be addressed and managed.

1.2.1 Scope Management

a) State how the project and product scope will be managed.
b) State how the Business Requirements Analysis will be performed.
c) State how Traceability will be completed for the WBS deliverable from requirements to deliverable acceptance.
d) Provide the Preliminary Work Plan - Work Breakdown/Requirement Breakdown Structure to include:
    1) Anticipated individual project resources by (Contractor, DOH business, DOH IT)
    2) Anticipated external resource dependency requirements
    3) Anticipated effort required for each resource

e) Note: If using an Agile methodology – state how the Requirement Breakdown Backlog (Initiatives, Features, Product Backlog Items (PBIs) with anticipated effort and anticipated velocity), and Release Plan will be managed.
    1) State the number of states anticipated for an iteration.
    2) State what number of releases are anticipated, the number of iterations and effort expectations.
    3) State what resource expectations are anticipated per iteration for contract and DOH staff.
    4) State the velocity expectations for DOH staff.

1.2.2 Schedule/Task Management

a) State how the schedule will be managed.
b) State how you propose task assignments will be generated and tracked.
Note:
    1) Internal DOH IT Developer resources are managed with Azure DevOps (ADO) Scrum Templates.
    2) Internal DOH IT infrastructure resources are managed through Service Desk Requests.
c) Propose how you will coordinate with the DOH project manager to use these resources if DOH IT resources are needed.
d) Propose how you will coordinate the overall master schedule.
e) State how tracking traceability from requirements to acceptance for scheduled Milestones will be managed.
f) State what method will be used for progression of work.
g) Note: If an Agile methodology will be used:
    a. State what the boundaries are and what ceremonies will be established for vision, release, iteration and stand up and how they will be used.
    b. State what the number of anticipated iterations for Milestones and buffer iterations and how the management of the product backlog be handled against the overarching goals.

1.2.3 Change Management

a) State how the Scope, Cost, and Schedule Changes will be managed.
b) State how Task Discovery Clarification updates, that are deemed in scope, will be handled.

1.2.4 Risk Management

a) Identify any known risks, assumptions, or constraints based on this proposal request and your experience with a similar project.
b) State what method will be used for tracking known and unknown risks and how these risks, if they occur, will be managed and progressed to resolution.

1.2.5 Issue Management

a) State how you will handle issue identification, tracking, resolution, and escalation.
b) State how you will address concerns that may not appear to be issues.

1.2.6 Quality Management

a) State how quality will be managed.
b) State how traceability from requirements to acceptance will occur.
c) State the anticipated Testing and Acceptance process.

d) If you are using Test Driven Design state how testing, requirements, and documentation processes will be handled.
e) State the anticipated training for product processes.
f) State the anticipated training for maintenance and operational support.

1.2.7 Staffing Management

a) State the anticipated roles and responsibilities and subcontractor management areas.
b) State that the Contractor has submitted resumes for all contract resources assigned to the project to the HSS project manager.
c) State that if the proposed contract resources change at the time of award, or during the life of the project, the contractor will submit all new resource resumes.
d) State all assumptions of the DOH roles and responsibilities and any anticipated DOH resources.
e) State what DOH resource dependent activities will be needed for the contractor's effort to be successful.
f) State all assumptions regarding skills and support needs for DOH Staff support.
g) State what expectations are anticipated for work outside the standard support hours during the project, including Rollout, and post support. Note: DOH IT standard operation support hours are 7:00 AM to 5:00 PM Alaska Time Zone.

1.2.8 Communication Management

a) State how communication will be managed between contractor, project resources, and impacted project stakeholders.
b) State how you will use the document repository for collaboration and document versioning.
c) State how notifications and escalations will be handled.

1.2.9 Implementation Management

Note: DOH IT standard operation support hours are 7:00 AM to 5:00 PM Alaska Time Zone.

a) State the Rollout expectations and Integration dependencies anticipated.
b) State how you will manage the rollout.
c) State what expectations are anticipated for work outside the standard support hours during the project Rollout.
d) State the anticipated maintenance and operations management after rollout.
e) State the expectations anticipated for after standard work hour support.

1.2.10 Master Project Management Plan and Master Work Schedule

Note: The high-level narrative is required for the proposal; the updated more detailed Plan is required as part of the project deliverables within the Planning phase of the project.

a) State that you will provide the updated Master Project Plan and Master Work Schedule as part of the project deliverables. Those deliverables are noted in section 2.1.
b) If alternative processes are proposed to any deliverable process areas listed in Section 2.1 Master Project Plan and Master Work Schedule, state those alternatives. They must be defined in your proposal.
c) The preliminary Master Project Work Plan/Schedule should be included

2 Master Project Management Plan and Master Work Schedule

The Master Project Management Plan provides in descriptive terms “how” the management processes and expectations will be performed to ensure deliverables occur and meet requirements success measures. The Master Project Management Plan also provides traceability back to the Master Project Work Plan/Schedule (the “what” that will be done).

2.1 Master Project Management Plan

The Master Project Management Plan is the document that covers the Project Life Cycle Methodology proposed for managing this project. (This includes the methodology for managing both business and IT activities and dependencies for the life cycle of the project.)

The Master Project Management Plan includes the following areas:

a) Scope Planning (Section 3.1)
b) Schedule, Tracking, Change, Risk, and Issue Management Planning (Planning Section 3.2)
c) Quality (Project and Product) Planning (Section 3.3)
d) Communication, Stakeholder, and Staffing Management Planning (3.4)
e) Execution and Monitoring Activities (Section 4)
f) Closing and Handoff Planning (Section 5)
g) Post Closure and Handoff (Section 6)

Note: While the Master Project Management Plan is often viewed as static, for this project it is a living document that governs the execution of the project and is to be used for monitoring the project support.

Additional Plans related to the Product will also be delineated in the Project Planning Section 3, the IT Requirements. These include:

a) Product Design/Configuration Roadmap (Section 3.1.2)
b) Security Plan (see IT Requirements section 3.7.2)

2.2 Master Project Work Plan/Schedule

The Master Project Work Plan/Schedule will include all anticipated project and product tasks, project resources by name, and effort levels for each resource. The Master Project Work Plan/Schedule must include a schedule of work, including a Gantt chart illustrating project milestones, dates, and timeframes for resource utilization and contract deliverables.

The Master Project Work Plan/Schedule should include the high-level milestone timetable regardless of the project management methodology.

If using an Agile methodology, the anticipated iterations backlog should be provided for the anticipated Feature target dates for milestone release delivery. Provide the backlog that supports the Feature target dates and the anticipated release dates, the standard iteration length, number of iterations per release, anticipated effort.

Provide the timeline for the number of anticipated iterations for Milestones and their capacity buffer iterations and how the management of the product backlog will be handled against the overarching goals.

Provide what the tracking method will be used for both Contract and DOH resources and what tools will be used to manage this and how this will be coordinated with the DOH IT assignment tracking methods.

The Master Project Work Plan/Schedule provides the tasks, activities tracking, assignment of individual project resources by (Contractor, DOH business, DOH IT), the effort required for each resource, and the Traceability Matrix for WBS deliverables/Features to deliverable acceptance.

3 Project Planning

Within the specified number of days listed in the Scope of Work (RFP Section 3) regarding the project initiation meeting, the contractor shall deliver the Master Project Management Plan and an updated Master Project Work Plan/Schedule that reflects any changes from the preliminary Master Project Work Plan/Schedule submitted with the contractor's proposal that were discussed and agreed to during the project initiation meeting.

The Master Project Work Plan/Schedule shall be maintained throughout the life of the project. Dates in the Master Project Work Plan/Schedule shall not be updated without mutual agreement between the contractor and the State Project Manager to reflect the accurate status of the project.

3.1 Project Scope Planning

The State of Alaska is procuring a new system/solution. As such, it is not interested in replicating what or how the current system stores, manipulates, and processes data.

3.1.1 Business Requirements Analysis

As part of the Project Scope Planning, the Master Project Plan must clarify how the Business Requirements Analysis will be performed and how they will be progressed (tracked) for completeness and traceability of activities through acceptance of the requirements.

The outcome of the Business Requirements Analysis / system modification meeting(s) will be documentation in a format agreed to by DOH IT and Division staff containing the following:

a) Identified business and system requirements that are satisfied by the contractor’s solution.
b) Identified business and system requirements that are not satisfied by the contractor’s solution.
c) Identified and descriptive modifications that will be required to meet stated requirements, including any associated costs for requirements identified during the analysis that were not part of the contract.
    1) Each modification description will need to include whether modifications are configurations, customizations, or alternate business workflow patterns by users.
d) Diagrams supporting application schema with structures and linkages.
e) Mockups of forms and reports.
f) Identified and updated business process flows.

Note: If Agile is used there should still be Requirements Documentation in the method of User Stories and Test Cases that would include the above bullets. The Project Management Plan should explain how this information will support the system documentation.

This information shall not be orphaned on a system that is not under DOH control or left in the contractor tracking system. This information must be stored in, or exportable to, the DOH SharePoint Project site, or the DOH DevOps repository.

3.1.2 Product/Application/System Design or Configuration Roadmap

As part of the Project Management Plan, the Scope planning needs to include the management for the Product/Application/System Design or Configuration Roadmap which provides information to the State on how the product will be architected/configured and implemented.

The outcome of the Product/Application/System Design or Configuration Roadmap will be:

a) The detail of the contractor's approach to the configuration, architecture, integration modifications of the Product and the associated activities that need to be performed.
b) System Design Configuration Documents for review and comment by DOH IT and Division staff.
c) A final Product Design/Configuration Plan shall be produced and submitted based on the review and comments on the draft plan.

All product design documents will be reviewed and approved by the State prior to the initiation of project tasks to that are needed to perform activities associated with product design.
This information must be stored in, or exportable to, the DOH SharePoint Project site, or the DOH DevOps repository.

3.1.3 Data Conversion or Data Migration Roadmap

The Scope planning needs to include the Data Conversion or Data Migration Roadmap provides information to the State on how the product will be architected/configured and implemented.

The outcome of the Data Conversion or Data Migration Roadmap will be:

a) The details of the contractor's approach to the Data Conversion or Data Migration the associated activities that need to be performed.
b) The detail of the contractor's testing and acceptance criteria approach to the Data Conversion or Data Migration the associated activities that need to be performed.
c) Data Conversion and Data Migration Documents provided for review and comment by DOH IT and Division staff.
d) A final Data Conversion and Data Migration Roadmap shall be produced and submitted based on the review and comments on the draft plan.

All product design documents will be reviewed and approved by the State prior to the initiation of project tasks that are needed to perform activities associated with product design.

This information must be stored in, or exportable to, the DOH SharePoint Project site, or the DOH DevOps repository.

3.1.4 Application/System Documentation

As part of the Project Management Plan, the Scope planning needs to include the production and acceptance of comprehensive documentation for the new system and any subsequent modifications.

The documents produced will include:

- System Design Documents

    - System Architecture.
    - Entity Relationship Diagrams / Model(s).
    - System Configuration and Parameters.
    - Data Dictionary.
    - Data Design.
    - User Interface Design.
    - Hardware.
    - Software.
    - Backup and Recovery Processes.
- Operations Manuals
    - Query and Report Process(s) and operations.
    - System Configuration and Parameters.
    - Maintenance Process(s) and operations.
    - Online help and appropriate error messages for all forms and processes.
    - To the extent possible error messages should inform users how to proceed to resolve an error condition.

All product design documents will be reviewed and approved by the State prior to the initiation of project tasks to that are needed to perform activities associated with product design.

This information must be stored in, or exportable to, the DOH SharePoint Project site, or the DOH DevOps repository. If any of the documentation is web-based access, URL links will be established on the DOH SharePoint Project site for those resources.

3.2 Project Schedule and Tracking Planning

The Master Project Work Plan/Schedule will be a live document to manage and progress all anticipated project and product tasks, project resources by name, and effort levels for each resource. If a task tracking application is used by the contractor that is not used by DOH, then that information must be easily exportable to provide an MS project like timeline and percentage of completion of milestones.

The Master Project Work Plan/Schedule must include a schedule of work, including a Gantt chart illustrating project milestones, dates, and timeframes for resource utilization and contract deliverables. The DOH Project Manager must have access to this information.

If the contractor's Project Work Plan/schedule does not contain all activities for the entire project work effort – only the contractor effort, there must be stubbed work package activity entries for DOH and IT). Those stubbed out work activities must provide the dependencies and timelines expected for the additional stakeholders so that the agreement between the Contractor Project Manager, the DOH Project Manager, and the DOH IT Business, Network Services and Customer Service Managers of how those items will be progressed (tracked).

3.2.1 Schedule Milestones and Tracking

The Schedule tracking must readily provide support progressing of Milestones and have the ability to track who is responsible for outstanding work. The Contractor and DOH project managers must agree on how the schedule will be managed.

Note:

- Internal DOH IT Developer resources are managed with Azure DevOps Scrum Template.
- Internal DOH IT Infrastructure resources are managed by Service Desk Requests.

The scheduling, assignment, and tracking of Contractor and DOH resources must be documented and provide traceability from assignment of tasks to requirements acceptance.

The Master Project Management Plan must document the method used for Progressing of work that has been mutually agreed to.

3.2.2 Change Management

The Master Project Management Plan must document the method used for Change Management work that has been mutually agreed to. This includes Scope, Cost, and Schedule Changes that will be documented, and tracked.

Note: Depending on the Change the effort may need to be escalated to the DOH IT Governance Sub Committee for review. Significant Schedule and Budget Changes may require additional turnaround time, especially for changes that require financial approval.

3.2.3 Risk Management

The Master Project Management Plan must document the method used for Risk Management identification, tracking and resolutions that has been mutually agreed to. This includes identification and ranking/prioritizing of any known risks, assumptions, constraints that occur or have been identified for this project.

Document what method will be used for tracking and how the process for assignment of work through resolution will be handled as well as resolving any impacts to the schedule.

3.2.4 Issue Management

The Master Project Management Plan must document the method used for Issue Management identification, tracking and resolutions that has been mutually agreed to. This includes addressing concerns that may not appear to be issues.

Document what method will be used for tracking and how the process for assignment of work through resolution will be handled as well as resolving any impacts to the schedule.

3.2.5 Review of the Project Closeout Handoff Checklist

The Master Project Management Plan must include the review of the Project Handoff Checklist to add any additional tasks/activities to the schedule that must be completed to ensure proper close out.

3.2.6 Implementation and Rollout Plan

The activities for Implementation and rollout need to be part of the Master Project Work Schedule. The Implementation and Rollout plan may be very high level at the beginning of the project. This section will be updated in more detail as the project moves forward and prior to rollout. This includes the environment and any data conversion/migration activities and documentation review.
The planned activities for rollout must include the notifications for impacted stakeholders.

3.2.7 Post-Production Support Plan

The identification of activities for Post-Production Support along with any licensing agreements must be part of the Master Project Work Schedule. This information must be provided at a high level at the beginning of the project. Prior to the implementation rollout plan this information must be updated to support production use. It is recommended that this section be updated in more detail as the project moves forward and not wait until just prior to rollout. This includes the environment, skill levels, resources needed and may also include contractual agreements.

As part of that plan items that must be included are:

- Helpdesk support.
- Assisting users with understanding the functionality and practical use of the system.
- Identifying errors in the system.
- Provide action plan(s) and resolution timeline for all issues.
- Evaluating system effectiveness against the established go live criteria.
- Monitoring performance of the new system.
- Modification process and knowledge necessary.

The post-production support plan must include all impacted support stakeholders, and any operation level agreements that need to be reviewed and approved.

3.3 Project Quality Planning

3.3.1 Project Qualitative Progress

The Master Project Management Plan must document the method and frequency to be used for the Quality Management assessment to ensure the project processes are being followed and to keep the project within scope, on schedule, and within budget. Any risk, issues, or concerns will be addressed through the Change, Risk, and Issue Management processes.

3.3.2 Project Test Planning

The Master Project Management Plan must document the method for Test Planning and Test Acceptance, how this work will be managed and progressed and how the traceability of the testing is tied to the requirements acceptance and milestones.

The deliverables are test planning, test scripts, and the test results process that must be documented and must be mutually agreed to by both contractor and DOH project managers. The Test Management Plan should include not only the methodology of how testing will be handled, but all responsibilities for contractor staff, DOH program staff and DOH IT.

3.3.3 System Test Plan

While there may be individual testing (smoke testing, unit/module testing) there should be an overarching System Test Plan that describes each type of testing that will be performed and how it will be handled for traceability of requirements. The plan will include the sequence and resources for each type of testing (for both Contractor, and State resources), provide exit criteria for each testing type, and criteria for system acceptance.

The plan will include any required equipment setup, application installations, and software setup for each type of test. The plan should also provide the schedule for User Acceptance Testing (UAT).

The test plan will identify the process for reporting, tracking, and resolving identified issues/defects in the application during development, UAT, and after application rollout.

Note: This testing and defect tracking should also be consistent with the management of Test deliverables.

If an Agile methodology is used and testing is incorporated into the iteration rollouts, there must be traceability for the feature acceptance and for the final system acceptance to ensure all features and functions have been met and accepted.

3.3.4 Testing

Testing consists of all activities that occur to create, test, and deliver the finished application. The state understands that there may be a significant overlap in activities during the project life cycle that cover testing depending on which project methodology and application development methodology is used. Responsibilities for who performs development of test cases and scripts, sets up the environment, tests, and how to handle defects must be defined.

The contractor will provide testing results and progress reporting at the weekly project status meeting. Upon successful completion of the user acceptance testing, the contractor will finalize all components of the system including:

- System Finalization.
- Demonstrate the backup and restore capability.
- Provide a roll-back procedure for use in the event of a system failure.
- Resolve all critical issues prior to placing the system in production.
- Establish Support and Help Desk Procedures.

The contractor will provide the DOH Project Manager with a formal assessment of the system's readiness for production implementation.

3.3.5 UAT Test Scripts

The contractor shall provide test cases, test scripts and/or scenarios that provide step-by-step instructions for testers to follow to test all system functionality. Location and documentation of test scripts and testing scenarios will be provided and must be sufficiently detailed to allow untrained staff to carry out testing and determine the accuracy of results.

The contractor shall schedule testing based on their project and application development plans and adjust the test environment appropriately.

All Test Plans, test results, test scripts must be maintained and available for future Audit requirements.

3.3.6 Support UAT and System Revision

Prior to making the system available for UAT, the contractor shall perform internal testing and certify that the system is ready for UAT. If errors are identified in the internal testing, the system should not be certified and UAT will not proceed until the errors are resolved. The system, as delivered by the contractor for UAT, is expected to be fully functional, and contain no known critical errors. The UAT is expected to use actual client data from the legacy system as some test data.

The UAT must include tests of all system functions resulting in minimal errors as defined in the accepted test plan of this RFP. Errors in this context include errors identified in any portion of the new application (in the code, process functionality, documentation, and/or online help).

UAT shall include a test of data conversion/data migration and confirmation of transaction performance. It is assumed that the UAT can be completed in two rounds: one to uncover any errors and a second after modification and internal contractor testing to verify that any errors identified have been fixed and that no new errors have been introduced. This requires that the contractor not only fix the errors identified in round one, but also run the resulting system through their system qualification test prior to delivering it for the second round of UAT.

UAT will continue until the above process is completed successfully. The contractor will be available at their development facilities for consultation and problem resolution for the duration of the test. The contractor shall make all required corrections and revisions to the system resulting from the acceptance testing process. System retesting shall be conducted as required. If the UAT exhibits any failures, the system will be returned to the contractor for revisions.

During UAT, the user manuals and online help will also be evaluated. Reference materials must reflect system configurations appropriate to the product. The UAT procedures will instruct the testers to reference the user manuals and/or online help for directions regarding how to perform the required actions. Any inadequacies or omissions in the manuals must be corrected prior to final acceptance of the system by the State.

3.3.7 Training Planning

The Master Project Management Plan must document the method used for Training Management. This includes identification of the training needed, set up of training, and execution of training that has been mutually agreed to.

There are different types of training that may be identified:

- Skills deficit needed for support of the product.
- Knowledge transfer for support.
- Training to use the new product.

The Contractor shall train the state staff – including IT staff and Data Center staff prior to the Implementation rollout. This includes knowledge transfer for support.
The Training Plan should include the methodology used to complete knowledge transfer and training of the system, responsibilities and be consistent with the overall Project Management Plan.

The outcomes of training include:

- Recommended skill deficit training and costs and recommended vendor.
- Training materials for the product usage.
- Knowledge transfer documentation for support.

3.4 Project Communication, Staff, and Stakeholder Management

The Master Project Management Plan must document the method used for Communication Management between Contractor team, DOH Division team, and DOH IT support team as well as any impacted stakeholders affected by the project, or the new product. The communication method must be mutually agreed to by both Contractor Project Manager and DOH Project Manager.

3.4.1 Communication Management

To help with communication management the SharePoint project site also provides an initial IT Commitment Charter that contains an initial identification of the stakeholders that may be impacted by or be a part of the project team.

The Communication plan must document how communication will be managed between contractor, project resources, and impacted project stakeholders for notifications and escalation. This includes notifications for assignments, meetings, meeting minutes, requests for information, decisions, and documentation management.

The escalation tree for issues and concerns must also be mutually agreed to and documented.

The communication plan must include the process for bringing new staff up to speed so that they are aware of the agreed upon communication process. This process must be documented to handle staff turnover that may occur during the course of the project.

3.4.2 Project Meetings and Reporting

The Contractor will be responsible for scheduling, meeting agendas, minutes and final reports. It is anticipated that most status meetings will occur via web and/or video conference; onsite status meetings shall take place in conjunction with other onsite activities.

3.4.3 Project Initiation/Kick Off meeting

As part of their response, the Contractor will hold a project kick off meeting to set project expectations and agreement for role definitions and responsibilities for both contractor and Division staff surrounding the project. The Contractor will coordinate with the DOH Project Manager for who needs to be at this meeting.

The contractor shall be prepared to provide an overview of how they intend to accomplish the tasks of the project, discuss the project schedule, and begin discussing the system modifications desired by the State.

In advance of the meeting the contractor shall provide a memorandum documenting required decisions and outcomes of the meeting. The meeting will address:

- Deliverable review and approval process.
- Agreement on the format and protocol for project status meetings.
- Agreement on the format for project status reports.
- Setting the schedule for meetings between representatives from the State and the contractor to develop the detailed project plan.
- Defining lines of communication and reporting relationships.
- Reviewing the project mission, scope, approach, timeline, and resource Commitments

- Pinpointing high-risk or problem areas; and
- Change management and Issue resolution process.

3.4.4 Weekly/Bi-Weekly Reporting

The contractor shall provide a single page weekly/Bi-Weekly status report summary to the DOH Project Manager. The frequency and format should be a standard that is mutually agreeable between the Contractor and DOH Project Managers.

The contents of the report shall include at a minimum:

- Project progress and accomplishments for the reporting period.
- Items/ tasks to be completed during the next reporting period.
- Items/ tasks that are behind schedule
  - Impact and risk to the project.
  - Mitigation.
  - Trends for items/tasks that are not yet overdue but need attention to keep the schedule on track.
- Heads up for any external dependency activities that are needed to complete to keep the schedule on track.
- Open Issues
  - Impact and risk to the project.
  - Mitigation.
- Any obstacles to progress.
- Housekeeping.
- Site visit schedules if applicable.
- Team activities and availability.

3.4.5 Monthly Reporting Meeting

The contractor shall lead the monthly status meeting to provide updates:

- on project progress.
- to discuss issues.
- to review project risks.

Attendees will include the Project Sponsors, DOH Project Manager, DOH IT Lead representative and core team members as appropriate.

3.4.6 Monthly Report

A formal monthly report will be submitted to the State within five (5) working days of the meeting. It will contain a monthly summary of the information in a weekly report. In addition, it will include:

- Work plan review.
- Task information updated to reflect percentage completion.
- Project Management metrics.
- Actual effort vs Planned.
- Cost to date vs Planned.
- Estimates to complete both effort and cost on a major task basis.
- Staffing changes.
- Change Orders.

- Other business as necessary.

3.4.7 Staffing Management

Staffing management is part of the communication plan and must not only identify the project staff but include their anticipated roles and responsibilities that have been agreed to. This must include the expectations and responsibilities during meetings and any information dissemination to their represented groups. This includes contractor as well as DOH Division and IT staff.

An understanding of what DOH resource dependent activities are needed for the contractor effort to be successful must be delineated along with any assumptions about skills and support needs so expectations can be clarified or adjusted.

Note: DOH IT standard operation support hours are 7:00 AM to 5:00 PM Alaska Time Zone. If there are expectations for after work hour support for the project, including Rollout, and post support these must also be agreed to and documented.

3.4.8 Stakeholder Management

As part of the communication plan, there must be information taken back to interdependent support teams, and external stakeholders to the project team. The responsibilities for this communication notification and solicitation process must be documented.

Impacted stakeholders outside of the project team need to be identified as well as the expectations for keeping them informed of decisions, impacts and obtaining information from them. This must also be documented.

4 Project Execution and Monitoring

Project Execution and Monitoring will follow the Master Project Management Plan and Master Project Work Schedule defined.

5 Project Closing and Handoff

5.1 Project Closeout Handoff Checklist

Prior to the close of the project the DOH IT Project Management Office must be notified to schedule the IT Project Handoff Checkoff list meeting. This should be requested at the commencement of Implementation and Rollout Planning. This meeting ensures that required activities have been completed prior to close out of the project. Any additional uncovered activities that need to be completed prior to project close out need to be reviewed and addressed to ensure completion.

5.2 Implementation and Rollout Plan

The implementation and rollout of the product requires a plan and notification of the appropriate stakeholders with enough lead time to ensure the environment and support are ready. Any after-hours support for DOH IT Staff and Division staff must be cleared in advance.
Only after final approval, the application will be placed in production.

5.2.1 Final Deliverable Acceptance

The contractor will submit a final document for the formal acceptance of all system development, modification, and implementation activities. The document will include a list of all known issues with the application and a plan for their resolution.

5.2.2 Delivery of Final Documents

Within 30 days of the completion of rollout, the contractor shall deliver a Post Implementation Evaluation to the State Project Manager. The contractor shall deliver all materials developed during the course of the project. This will include complete documentation, source code, and other materials, as well as client/program data to the DOH Project Manager. The contractor shall provide verification and certification that specifies all software, policies, security requirements, procedures, reporting, and equipment are functioning as planned and that all documentation is complete has been received and approved by the DOH Project Manager.

6 Post Implementation Support

6.1 Warrantee Support

The contractor warrantee must be documented, and it must spell out what is covered. The process for how defects and issues will be handled must be addressed during the Project Planning Process and should be included in the proposal.

The turnaround expectations for defects and issues that are covered must include the response time and process for handling the defects. Items that are not covered by warrantee must be spelled out. The duration of the warrantee must also be spelled out and must be addressed at the beginning of the project and not wait until implementation rollout.

The contractor must provide during the warranty period support services that include:

- (a) Application support
  - i. Support must be available Monday through Friday 8 AM – 4 PM Alaska time for all State of Alaska workdays (email notification is sufficient).
  - ii. Contractor will respond to any critical issues within 24 hours.
  - iii. Contractor will respond to any non-critical issue within 48 hours.
- (b) Issue response will include
  - i. Assessment of the impact of the issue to the application.
  - ii. Workarounds if available.
  - iii. An estimate of the time to resolve the issue.
- (c) Contractor will be responsible for all cost for the licensing, purchase, application, and testing of all updates, upgrades, and patches to the software packages used to deploy, operate, and maintain the application during the warrantee period.
- (d) Updated Documentation
  - i. The contractor will update documentation to reflect all changes to the function and operation of the system within 30 days of any change.
  - ii. Online documentation will be updated to reflect all changes to the system processes within 30 days.

6.2 Post Implementation Contract Support

The post implementation support plan needs to be executed prior to or during the implementation rollout to provide support to the DOH during the implementation to assist with the turnover for postproduction support.

Reference D
Information Technology Standards

State of Alaska
Department of Health

1 Introduction

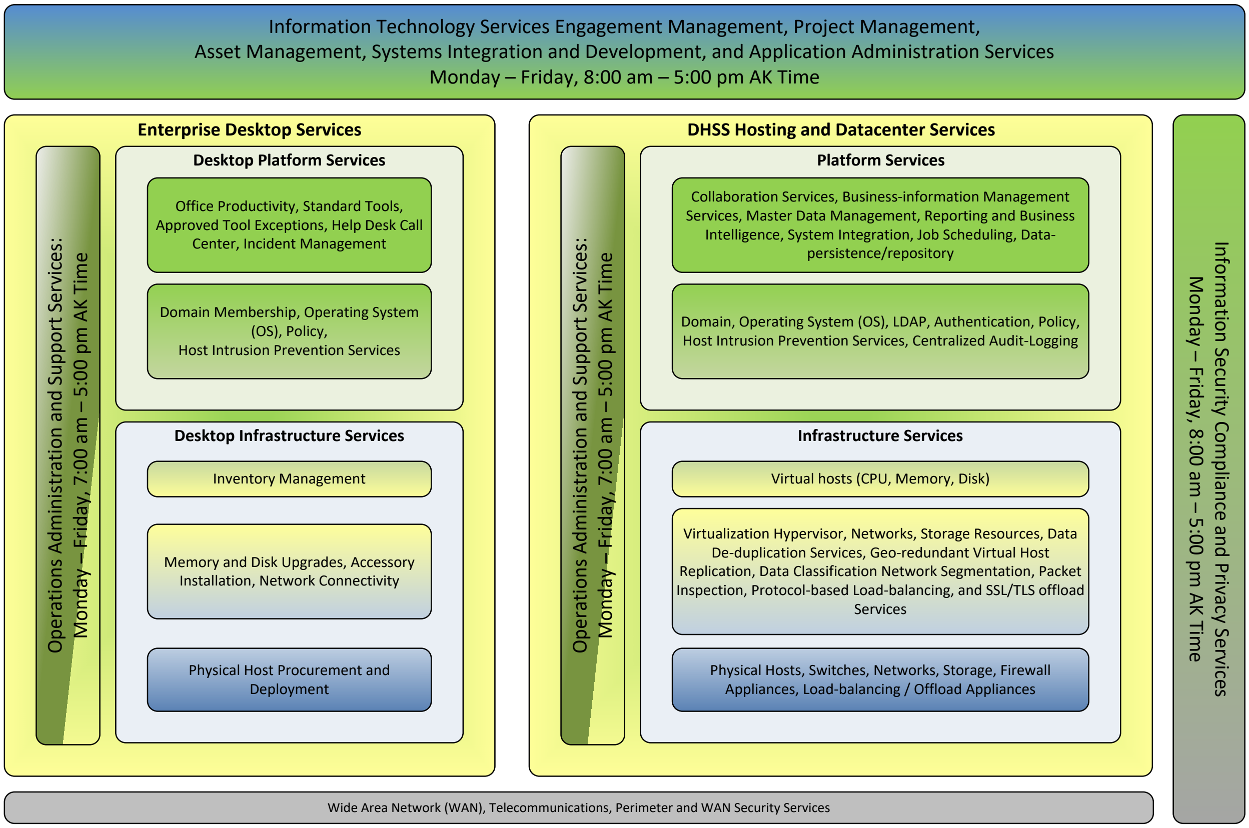
This document presents software, hardware, and other Information Technology product standards for Alaska Department of Health (DOH). This document is a reference companion to other documents, such as the DOH RFP IT Requirements template, that clarifies the current IT standards. This IT Standards document is structured according to the service-line/area for the applicable standard.

1.1 State of Alaska Statewide IT Standards

In addition to the DOH IT Standards identified in this document, the State of Alaska Department of Administration (DOA) Office of Information Technology (OIT) may have state standards that are not represented in this document. Please see their services website at Home, Office of Information Technology, State of Alaska.

1.2 DOH Service Lines

The DOH following IT service lines apply:



Information Technology Services Engagement Management, Project Management,
Asset Management, Systems Integration and Development, and Application Administration Services
Monday – Friday, 8:00 am – 5:00 pm AK Time

Enterprise Desktop Services

Operations Administration and Support Services:
Monday – Friday, 7:00 am – 5:00 pm AK Time

Desktop Platform Services

Office Productivity, Standard Tools, Approved Tool Exceptions, Help Desk Call Center, Incident Management

Domain Membership, Operating System (OS), Policy,
Host Intrusion Prevention Services

Desktop Infrastructure Services

Inventory Management

Memory and Disk Upgrades, Accessory Installation, Network Connectivity

Physical Host Procurement and Deployment

DHSS Hosting and Datacenter Services

Operations Administration and Support Services:
Monday – Friday, 7:00 am – 5:00 pm AK Time

Platform Services

Collaboration Services, Business-information Management Services, Master Data Management, Reporting and Business Intelligence, System Integration, Job Scheduling, Data-persistence/repository

Domain, Operating System (OS), LDAP, Authentication, Policy, Host Intrusion Prevention Services, Centralized Audit-Logging

Infrastructure Services

Virtual hosts (CPU, Memory, Disk)

Virtualization Hypervisor, Networks, Storage Resources, Data De-duplication Services, Geo-redundant Virtual Host Replication, Data Classification Network Segmentation, Packet Inspection, Protocol-based Load-balancing, and SSL/TLS offload Services

Physical Hosts, Switches, Networks, Storage, Firewall Appliances, Load-balancing / Offload Appliances

Information Security Compliance and Privacy Services
Monday – Friday, 8:00 am – 5:00 pm AK Time

Wide Area Network (WAN), Telecommunications, Perimeter and WAN Security Services

1.3 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
S Taylor	2/10/2017	Re-organized document, added change log
T Kisner	10/16/2018	Removed ETS reference and link to their IT Standards document
C Boom	09/27/2021	Updated link to OIT services catalog website. Updated lists of standard software. Added DOH Logo, formatted header. Added document date and page number.
D. Garcia	08/02/2022	Corrected basic grammar & formatting problems and inconsistencies, commented on a number of technologies, removed SharePoint 2010 as a standard.
IT Leadership Review	08/18/2022	Reviewed updated document and addressed remaining contents

2 Standards

This section contains the standards for each service-line. Standards are established for:

- Software
- Hardware
- Other IT products (e.g., other referenced standards)

Standards must be followed for all IT software, hardware, and other products. Deviation from standards requires a completed Security Policy Waiver for each individual using the deviant product, as established by DOH information security policies and standard operating procedure.

2.1 Engagement and Service Delivery Management Service Standards

Engagement and Service Delivery Management Services focus on how DOH IT interacts with our DOH customers, vendors, grantees, and other partners. The following standards apply.

2.1.1 Hardware

No unique hardware standards for Engagement and Service Delivery Management Services.

2.1.2 Software

Standard	Function	Uses
Microsoft SharePoint 2019	Enterprise Content and Document Management, Intranet and Social Network, Collaboration, Custom Web Applications and Workflow	IT Matrix Inventory of initiatives (projects, systems, services), Reference document libraries
Azure DevOps Server Azure DevOps Services	Version control, Agile project management, Continuous integration, Release management, Package mgmt., DevSecOps, Testing	Service delivery management tracking and reporting
SolarWinds Web Help Desk	Help Desk Ticketing System	Service delivery management tracking and reporting

2.1.3 Other Products

No unique other product standards for Engagement and Service Delivery Management Services.

2.2 Project Portfolio Management Service Standards

Project Portfolio Management Services focus on how DOH IT supports project management enterprise process development and execution. The following standards apply.

2.2.1 Hardware

No unique hardware standards for Project Portfolio Management Services.

2.2.2 Software

Standard	Function	Uses
Microsoft SharePoint 2019	Enterprise Content and Document Management, Intranet and Social Network, Collaboration, Custom Web Applications and Workflow	IT Matrix Inventory of initiatives (projects, systems, services), Project management and chartering sites, Reference document libraries, activity lists
Azure DevOps Server Azure DevOps Services	Version control, Agile project management, Continuous integration, Release management, Package mgmt., DevSecOps, Testing	Work management tracking and capacity allocation reporting

2.2.3 Other Products

No unique other product standards for Project Portfolio Management Services.

2.3 Asset Management Service Standards

Asset Management Services focus on how DOH IT supports managing software licensing and other software assets. The following standards apply.

2.3.1 Hardware

No unique hardware standards for Asset Management Services.

2.3.2 Software

Standard	Function	Uses
Ivanti Inventory Scanner SCCM Inventory Tracking	Software inventory scanning	Licensing support, enterprise standards enforcement
Microsoft Team Foundation Server 2018 (on prem) Azure DevOps (SaaS)	Documentation and code management and repository.	Version control, code, and documentation management.
IRIS/Alder	State asset management system/reporting	State procurement asset tagging and tracking
Dell Asset Management	Hardware wipe and recycle	Hardware wipe and recycle

2.3.3 Other Products

No unique other product standards for Asset Management Services.

2.4 Systems Integration and DDI Service Standards

Systems Integration and DDI Services focus on how DOH IT supports system architecture development, integration between DOH systems and information system design, development, and implementation. The following standards apply.

2.4.1 Hardware

No unique hardware standards for Systems Integration and DDI Services.

2.4.2 Software

Standard	Function	Uses
Mainstream supported Microsoft Visual Studio	Development IDE	Information systems and software development and maintenance
Microsoft Visual Studio Code	Development IDE	Information systems and software development and maintenance
Supported versions of C# language	Development language	Information systems and software development and maintenance
Microsoft Team Foundation Server 2018	Work management, SDLC support	Work management, requirements definition, design, implementation, and test management and execution artifacts
Mainstream support versions of Microsoft Visio	Diagramming and modeling	Diagramming and modeling various architectural views
Mainstream support versions of Microsoft PowerShell	Automation and DevSecOps	Automate various processes via PowerShell
Mainstream support versions of .NET Framework and .NET Core (preferred)	Development language	Information systems and software development and maintenance.
Microsoft Dynamics 365, on prem	Development IDE	Information systems and software development and maintenance.

2.4.3 Other Products

Standard	Function	Uses
Microsoft Azure PaaS	Auto-scaling custom information system application containers in the cloud	Hosting information systems and services in the cloud

2.5 Systems Operations and Administration Service Standards

Systems Operations and Administration Services focus on how DOH IT supports technical system operations and system administration. The following standards apply.

2.5.1 Hardware

No unique hardware standards for System Operations and Administration Services.

2.5.2 Software

Standard	Function	Uses
Microsoft Windows Remote Desktop Client, Ivanti, SCCM, VMWare vSphere, Citrix Access Gateway, Cisco AnyConnect, OpenConnect for Mainframe	Remote desktop access	Remote server access
F5 Proxy Services	Reverse proxy	Web application delivery
Mainstream support versions of Microsoft Internet Information Services Manager	System administration	Manage IIS sites and applications
Mainstream support versions of Microsoft SQL Server Management Studio	System administration	Manage SQL Server databases and servers
Mainstream support versions of Microsoft BizTalk Server Administration Console	System administration	Manage BizTalk servers and server groups, Enterprise Service Bus (ESB)
Mainstream support version of Visionware MultiVue Administration Console	System administration	Manage MultiVue Configuration, Master Client Index (MCI)
Mainstream support versions of Microsoft PowerShell	System administration	Manage various services via PowerShell

2.5.3 Other Products

Standard	Function	Uses
Microsoft Azure Portal	Management for all Azure resources and services allocated with a tenant subscription	Administering Azure hosted resources and services

2.6 Information Security Compliance and Privacy Service Standards

Information Security Compliance and Privacy Services focus on how DOH IT supports legal compliance with information security, privacy, and ongoing development/maintenance of security policy and practice. The following standards apply.

2.6.1 Hardware

No unique hardware standards for Information Security Compliance and Privacy Services.

2.6.2 Software

Standard	Function	Uses
RSA Archer	Information security risk and compliance	Risk and compliance management

Standard	Function	Uses
Splunk	Enterprise log indexing and reporting	Audit-logging, reporting
Veracode	Software vulnerability scanning	Scan source code, identify software vulnerabilities for remediation, per policy
Varonis	Enterprise confidential data audit-logging	File system-based access audit logging

2.6.3 Other Products

Standard	Function	Uses
NIST 800-53 v4	Standardized security controls	Reference for security plan control set
NIST 800-66	Standard subset of NIST 800-53 controls for HIPAA	Selection criteria for security plan control set for HIPAA systems

2.7 Enterprise Desktop Service Standards

Enterprise Desktop and Mobility Services focus on how DOH IT supports defining, deploying and supporting the DOH enterprise desktop and mobility endpoints. The following standards apply.

2.7.1 Hardware

Standard	Function	Uses
Dell Precision 3540 Mem 32GB HD M.2 512 SSD Processor 15-11500	PC workstation	Desktop, non-mobile
Dell Precision 3650 Mem 32GB HD M.2 512 SSD Processor i7	PC workstation	Power Desktop, non-mobile
Dell Latitude 5310 Mem 16GB HD M.2 256 SSD Proc i5-1021OU	PC workstation	Small Laptop, mobile
Dell Precision M3551 Mem 32GB HD M.2 512 SSD Proc i7	PC workstation	Regular Laptop, mobile
Dell Precision M7750 Mem 32GB HD M.2 512 SSD Proc i7	PC workstation	Large Laptop, mobile

Standard	Function	Uses
Dell Latitude 7210 2 in 1 Mem 16 GB HD M.2 256 SSD Proc i5	Mobile endpoint	Productivity capable, extended use mobile device
Dell WD19DC Docking Station	Docking station	17" laptops
Dell WD19TBS Docking Station	Docking station	Less than 17" laptops

2.7.2 Software

Standard	Function	Uses
Microsoft Systems Center Configuration Manager (SCCM)	Systems management	Desktop deployment
Ivanti	Systems management	Desktop software install, upgrade, patching, security scanning
SolarWinds Web Help Desk	Help Desk Ticketing	Incident and service request management. Interface between customers using DOH systems/IT services and the operational support team for those systems/IT services
Mainstream supported Microsoft Windows on Desktops	Desktop operating system (OS)	Standard DOH desktop operating system
Microsoft BitLocker	Disk encryption	Fixed and removable disk encryption
Cybereason Migrating to Windows Defender for Endpoint in H2 of 2022	Antivirus, host intrusion prevention, policy management	Antivirus, host intrusion prevention, policy management
Microsoft Edge current version, Chrome (current version), Firefox (current version). Browser support only	Web browser	Browsing web
Edge in IE 11 mode	Web-application client	DOH IT internal application development browser. IE 11 mode is deprecated and not preferred. Must have plans to update to modern browser compatibility
Microsoft Office 365	Desktop productivity suite	Document authoring, spreadsheets, presentations, information system integration (e.g., notice processing or other document merge processing)

2.7.3 Other Products

No unique other product standards for Enterprise Desktop Services.

2.8 DOH Hosting and Datacenter Service Standards

DOH Hosting and Datacenter Service Standards focus on how DOH IT supports designing, implementing and operating standard infrastructure and platform offerings. The following standards apply.

2.8.1 Hardware

Standard	Function	Uses
Cisco UCS Blade Server	Physical host	Datacenter virtualization resources
Dell PowerEdge Server	Physical host	Datacenter virtualization resources or remote location physical server
NetApp Storage Area Network	Enterprise storage	Datacenter disk storage
Checkpoint Firewall	Data center firewall/IPS	Data center protection against unauthorized access

2.8.2 Software

Standard	Function	Uses
F5	Load balancing, proxy, protocol optimization, SSL/TLS offload appliance	Load balancing, SSL/TLS offload
VMWare ESXi Hypervisor Virtualization	Hypervisor	Datacenter hypervisor for host virtualization
NFS for VMware Network Attached Storage (NAS)	Storage management protocol	Allocate/manage/use storage, printers, etc.
iSCSI for VMware Storage Area Network (SAN)	Storage management protocol	Allocate/manage/use storage
Mainstream supported Microsoft Windows Server	Server operating system	Access and manage server hosts
Mainstream supported Microsoft .NET	Underlying enterprise services platform API	Support 3rd party and custom .NET components and services
.NET Core	Underlying enterprise services platform API	Support 3rd party and custom .NET Core components and services
Mainstream supported Microsoft Active Directory	Domain, LDAP, authentication, policy	Manage domain, LDAP, authentication (Kerberos, Integrated) and policy
Mainstream supported Microsoft Active Directory Federation Services	Federated authentication	Manage authentication in federated identity scenarios

Standard	Function	Uses
Mainstream supported Microsoft SQL Server	Information persistence / data repository	Online Transaction Processing / Information system database storage
Splunk	Enterprise log indexing and reporting	Audit-logging, reporting
Mainstream Microsoft Internet Information Services	Application server and web content delivery	Support IIS hosted applications and content
Mainstream supported Microsoft SQL Server Reporting Services	Reporting and business intelligence	Report authoring, scheduling, and subscription services
Mainstream supported Microsoft SQL Server Analysis Services	Reporting and business intelligence	Online Analytical Processing / Information and metrics trend reporting
Mainstream supported Microsoft SharePoint 2019	Enterprise Content and Document Management, Intranet and Social Network, Collaboration, Custom Web Applications and Workflow	Collaborative self-service business productivity, including: intranet, document libraries, simple data lists, and simple workflows. Approved applications.
Mainstream supported Microsoft BizTalk	System integration, Enterprise Service Bus	Master Client Index, line of business system integration
Mainstream supported version Microsoft Dynamics CRM, on prem	Extensible relationship/case management, rapid design, and scalable business information systems platform	Case management, registries, grants management
Mainstream supported version Visionware MultiVue	Master data management	Master Client Index
DOH Master Client Index	Line of business system client cross-reference	System integration support, Client Services Dashboard

2.8.3 Other Products

Standard	Function	Uses
Microsoft Azure PaaS	Auto-scaling custom information system application containers in the cloud	Hosting information systems and services in the cloud

2.9 DOH Wide Area Network, Telecommunications and Perimeter and WAN Security Service Standards

DOH Wide Area Network, Telecommunications and Perimeter Security Services focus on how DOH IT supports integrating the DOH LAN with the State of Alaska (SOA) wide area network, telecommunications and perimeter security is managed by Department of Administration (DOA) Office of Information Technology (OIT). The following standards apply.

2.9.1 Hardware

No unique hardware standards for DOH Wide Area Network, Telecommunications and Perimeter Security Services.

2.9.2 Software

Standard	Function	Uses
AlaskaNow (ServiceNow)	Incident and service request management tracking	Interface between DOH and OIT for addressing OIT supported service incidents and requesting changes or other services

2.9.3 Other Products

Standard	Function	Uses
PureCloud	Interactive Voice Response	Cloud call center solution

Reference F
Data Destruction Information and References

State of Alaska
Department of Health

This is an overview of the State of Alaska and Federal Sources data destruction requirements for confidential information, as applicable to the State of Alaska, Department of Health (DOH). The department recognizes confidential information, information that identifies or could identify an individual, as personally identifiable information (PII) as defined in OMB Memorandum M-07-1616.

> PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual. (GSA.gov)

A DOH applicable example of this would be a data set that includes an individual's name and one other identifier such as, a social security number, date of birth, driver's license number, account number, password, employee id, or other access codes.

There are many laws and regulations defining PII. Here are just a few examples:

- Alaska Personal Information Protection Act (APIPA)
- Electronic Protected Health Information (ePHI)
- Personally Identifiable Information (PII)
- Criminal Justice Information (CJI)
- Criminal History Record Information (CHRI)

To meet the department's required standards for destruction of Electronic Protected Health Information (ePHI), Personally Identifiable Information (PII), Criminal Justice Information (CJI), or Criminal History Record Information (CHRI) staff must comply with the most current NIST guidance (currently NIST Special Publication 800-88 Revision 1). (Kissel, Regenscheid and Scholl) As outlined in NIST Special Publication 800-88 Revision 1, Appendix A—Minimum Sanitization Recommendations, DOH requires that staff comply with the appropriate Clear, Purge, or Destroy mechanisms for all media.
Additionally, Alaska Statute 45.48 (State of Alaska) Section 45.48.500 -.590 addresses the Disposal of Records by stating:

> When disposing of records that contain personal information, a business and a governmental agency shall take all reasonable measures necessary to protect against unauthorized access to or

> use of the records.
>
> Notwithstanding (a) of this section, if a business or governmental agency has otherwise complied with the provisions of AS 45.48.500 — 45.48.590 in the selection of a third party engaged in the business of record destruction, the business or governmental agency is not liable for the disposal of records under AS 45.48.500 — 45.48.590 after the business or governmental agency has relinquished control of the records to the third party for the destruction of the records.
>
> A business or governmental agency is not liable for the disposal of records under AS 45.48.500 — 45.48.590 after the business or governmental agency has relinquished control of the records to the individual to whom the records pertain.

In the HIPAA Disposal FAQ (HHS.gov) the Department of Health and Human Services reiterates that PHI must be sanitized using specific means; see:

> For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

Additionally, the HIPAA Security Series – Topic 3, Security Standards: Physical Safeguards (HHS.gov), outlines the following criteria for device reuse:

> Are policies and procedures developed and implemented that address disposal of EPHI, and/or the hardware or electronic media on which it is stored?
>
> Do the policies and procedures specify the process for making EPHI, and/or the hardware or electronic media, unusable and inaccessible?

References

GSA.gov. *https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act*. 12 01 2020. Web. 19 02 2020.

HHS.gov. *https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html*. 18 02 2009. Web. 19 02 2020.

—. *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf*. 03 2007. Web. 19 02 2020.

Kissel, Richard, et al. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf*. 12 2014. Web. 19 02 2020.

State of Alaska. *http://www.akleg.gov/basis/statutes.asp#45.48*. 2019. Web. 19 02 2020.

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.