System Security Plan

<System Name>

<Plan Version #.#>

<Date>

Company Sensitive and Proprietary

For Authorized Use Only

LEVEL 3, RESTRICTED INFORMATION

DISTRIBUTION FOR OFFICIAL USE ONLY

When system specific information is detailed within this document, all Level 3 statewide information security standards must be met. All copies must follow statewide protection and handling standards. Destroy by shredding.

EXECUTIVE SUMMARY

The objective of system security planning is to improve protection of information system resources. All State of Oregon systems have some level of sensitivity and require protection as part of good management practice.

The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place, or planned, for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system.

Management authorization should be based on an assessment of management, operational, and technical controls.

SECURITY PLAN BENEFITS

Accurate documentation of an organization's security programs, processes and procedures, and documentation of compliance with them, provides five key benefits. Security plans:

- Facilitate adequate, cost-effective security protection by assessing the security controls during the development phase of systems and documenting the authorization given by management.
- Lead to institutionalization of security activities for consistency as employees leave the organization. Good documentation is a change management tool and helps effective practices outlast the person who developed them.
- Increase compliance with security measures. Rules are generally followed more closely when someone is looking and keeping records.
- Help IT staff determine where various security measures may need to be strengthened.
- Provide an important step in quality control.

SYSTEM OVERVIEW

[*Provide a high-level summary of the system*]

IDENTIFIED SYSTEM RISKS

[*Provide a summary of the risk identified in the table below. Describe any residual risks, the likelihood of occurrence, and (using the impact table on page 3) the impact of a security event to the business or system. When assigning an impact rating to a risk, assign the rating corresponding to the most serious consequence that could result should the vulnerability be exploited.*]

Provide the top 5 risks associated with the system:

Likelihood	Impact	Risk Description

{A summary table is provided for the Executive review. Although not required, it is recommended as an overview of the control implementation status for each control family.}

Controls Status Summary Table

Control Family	In Place	Partially In Place	Not In Place	Not Applicable
3.1 – Access Control (15)	0	0	0	0
3.2 – Awareness and Training (1)	1	0	0	0
3.3 – Audit and Accountability (6)	0	0	0	0
3.4 – Configuration Management (8)	0	0	0	0
3.5 – Identification and Authentication (4)	0	0	0	0
3.6 – Incident Response (2)	0	0	0	0
3.7 – Maintenance (4)	0	0	0	0
3.8 – Media Protection (6)	0	0	0	0
3.9 – Personnel Security (2)	0	0	0	0
3.10 – Physical and Environmental Protection (2)	0	0	0	0
3.11 – Risk Assessment (3)	0	0	0	0
3.12 – Security Assessment and Authorization (3)	0	0	0	0
3.13 – System and Communications Protection (6)	0	0	0	0
3.14 – System and Information Integrity (7)	0	0	0	0
Totals	0	0	0	**0**

1 GENERAL SYSTEM INFORMATION

This System Security Plan provides an overview of the security requirements for the <**system name**> and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our state security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the <**system name**> information system.

Note: Once the name and abbreviation for the system and all the system's components is established in this section, use the exact same name and abbreviation throughout the SSP.

The security safeguards implemented for the <**system name**> system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Those items in square brackets (e.g. [ ]) are intended for fill-in purposes. Those items in braces (e.g. { }) are for references purposes.

SYSTEM FUNCTION OR PURPOSE

Get from charter or business case.

The purpose of the <system name> system is to

CONTACT INFORMATION

AUTHORIZING OFFICIAL

The authorizing official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. The authorizing official has the following responsibilities related to system security plans:

- Approves system security plans,
- Authorizes operation of an information system,
- Issues an interim authorization to operate the information system under specific terms and conditions, or
- Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

Name	
Title	
Company / Organization	
Address	

Phone Number	
Email Address	

INFORMATION SYSTEM OWNER

The following individual is identified as the information system owner or functional proponent/advocate for this system. The system owner is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. The system owner has the following responsibilities related to system security plans:

• Develops the system security plan in coordination with information owners, the system administrator, and functional "end users,"

• Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements,

• Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior),

• Updates the system security plan whenever a significant change occurs, and

• Assists in the identification, implementation, and assessment of the common security controls.

Name	
Title	
Company / Organization	
Address	
Phone Number	
Email Address	

INFORMATION OWNER (A.K.A. DATA OWNER)

The following individual(s) identified below is the agency official with the statutory or operational authority for the information processed, stored, or transmitted as part of this system and/or its functions and operation. The information owner has the following responsibilities related to system security plans:

• Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),

• Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides,

• Decides who has access to the information system and with what types of privileges or access rights, and

• Assists in the identification and assessment of the common security controls where the information resides.

Name	
Title	
Company / Organization	
Address	
Phone Number	
Email Address	

Information Owner

SYSTEM ADMINISTRATION

This system is managed by [*both ETS and the <ORGANIZATION> Team*]. List the Agency Primary and Secondary Administrators and the [*ETS Primary and Secondary Administrators*]. Additionally list all groups, or individuals not in groups, that have administrative access to the system or its application.

Identify groups or individuals, if possible, responsible for administrative functions of the system:

- *Group Name*
- *Name*
- *Name*

INFORMATION SYSTEM BUSINESS IMPACT ASSESSMENT

A potential impact assessment must be performed to determine the system categorization. An impact assessment considers the data sensitivity and system mission criticality to determine the potential impact that would be caused by a loss of confidentiality, integrity, or availability of the information system and/or its data. This section describes how the information system is categorized for confidentiality, integrity, and availability.

{Working with the Authorizing Official, the Information System Owner, and the Information Owner, rate the potential impact to the business or system in the event of unauthorized disclosure, modification, or unavailability of this information and/or information system.}

The tables (below) identifies the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adv effect on organizationa erations, organizational assets, or individuals. [1]	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. [1]	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. [1]	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Answers to the following questions will help in the evaluation process:

- How can a malicious adversary use the unauthorized disclosure, disruption of access, modification, or destruction of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- Would unauthorized disclosure, disruption of access, modification/destruction of elements of the information type violate Federal or State laws, executive orders, OAR's, or agency regulations?

[1] Adverse effects on individuals may include, but are not limited to, loss of privacy to which individuals are entitled under law.

	SYSTEM-WIDE POTENTIAL IMPACT		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality	☐	☐	☐
Integrity	☐	☐	☐
Availability	☐	☐	☐

Information System-wide Impact Assessment

Does this system require a disaster recovery plan? ☐ No ☐ Yes

Please provide a reference to related documents or a brief description of your disaster recovery requirements; including recovery time objective/recovery point objective requirements:

Click here to enter text.

Does the Business Continuity Plan need to be updated to include this system?

☐ No ☐ Yes

Please provide a reference to related documents or a brief description of your business continuity requirements:

Click here to enter text.

DATA CLASSIFICATION

What level of data will the system be processing, storing, or transmitting – according to the Statewide Information Asset Classification Policy?

	Data Classification
☐	Level 1 - Published
☐	Level 2 - Limited
☐	Level 3 – Restricted
☐	Level 4 - Critical

If Level 3 or Level 4 data classifications are checked, please indicate the type of data the information system will be processing, transmitting, or storing that requires this classification:

Click here to enter text.

REGULATORY COMPLIANCE

☐ Oregon Consumer Identity Theft Protection Act (As defined in ORS 646A.602)

☐ Criminal Justice Information System (CJIS)

☐ Health Insurance Portability and Accountability Act (HIPAA)

☐ Payment Card Industry-Data Security Standard (PCI-DSS)

☐ Federal Information Security Management Act (FISMA)

☐ Federal Tax Information (FTI)

☐ Social Security Administration (SSA)

☐ Other regulatory compliance _____

If any regulatory compliance boxes were checked, refer to the appropriate regulatory document to determine if information types are required to be documented (otherwise, N/A). Information types are defined by the organization or in some instances, by a specific law. Examples of specific categories of information include privacy, medical, proprietary, financial, investigative, contractor sensitive, and security management.

Information Type	Confidentiality	Integrity	Availability
Privacy (PII)	Moderate	Moderate	Low

Is the system subject to GDPR regulation? ☐ No ☐ Yes

{Provide definition of GDPR and Anthony will forward the language RE: contacting DOJ for an opinion}

WEB SERVER QUESTIONS

Yes	No	Server Questions
☐	☐	Do users connect to the system from over the Internet?
☐	☐	Does the system require authentication over the Internet?
☐	☐	Besides authentication, is Level-3 or higher data being transmitted over the Internet via browsers?
☐	☐	Will mobile applications be developed for use with the system?
☐	☐	Will the system require server-side Java or Flash as a supporting application?
☐	☐	Will clients connecting to the system require Java or Flash installation?

Server Function Determination Questions

INFORMATION SYSTEM OPERATIONAL STATUS

The system is currently in the life-cycle phase noted in the table that follows. (Only operational systems can be granted an ATO).

System Status		
☐	Operational	The system is operating and in production.
☐	Under Development	The system is being designed, developed, or implemented
☐	Major Modification	The system is undergoing a major change, development, or transition.
☐	Other	Explain:

Table 7- 1. System Status

2 TECHNICAL SYSTEM DESCRIPTION

This section includes a general description of the <system name>.

TYPES OF USERS

Employees (or contractors) of [ORGANIZATION] are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in the table that follows.

Role	Internal or External	Authorized Privileges and Functions Performed	Approximate # of users
Admins	Internal	Admin	5
Users	Internal/External	User	100

Table 9- 1. User Roles and Privileges

SOFTWARE INVENTORY

The following table lists the principle software components for <**system name**>**.**

Hostname	Function	Version	Patch Level	IP Address	Virtual (Yes / No)
<system name>.oregon.gov	Operating System	Windows Server 2012 R2	Service Pack 1	255.255.255.255	Yes
<system name>.oregon.gov	IIS	ASP .Net 4.5		255.255.255.255	Yes
<system name>.oregon.gov	Application Software	<system name>		255.255.255.255	Yes
<system name>.oregon.gov	Database SQL Server	MS SQL 2016		123.45.678	Yes
<system name>-testing.oregon.gov	Operating System	Windows Server 2012 R2	Service Pack 1	123.45.678/23	Yes

Hostname	Function	Version	Patch Level	IP Address	Virtual (Yes / No)
<system name>-testing.oregon.gov	IIS	ASP .Net 4.5		123.45.678/23	Yes
<system name>-testing.oregon.gov	Application Software	<system name>		123.45.678/23	Yes
<system name>-testing.oregon.gov	Database SQL Server	MS SQL 2016		123.45.678	Yes

Table 10- 1. Software Components

REMOTE SERVICES (OTHER THAN WEB SERVICES)

Will users or administrators connect to the system using any of the following services?

	Remote Management Services Questions		
☐	FTP	☐	VNC
☐	SFTP	☐	RDP
☐	Telnet	☐	Citrix
☐	SSH	☐	Other: Click here to enter text.

Hardware, Network, and Data Flow Diagram

<Insert Network and Data Flow Diagram>

PORTS, PROTOCOLS AND SERVICES

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential company operations. Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations should limit component functionality to a single function per device (e.g., email servers or web servers, but not both). (See 3.4.6)

In the table below, lists the Ports, Protocols, and Services enabled in this information system.

{On the Hardware, Network, and Data flow diagram are ports and protocols documented and color coded?}

Ports (TCP/UDP)	Protocols	Services	Purpose	Used By (Function or System Name)
80/TCP	HTTP		IIS	<system name>
443/TCP	HTTPS		IIS	<system name>
389/636	LDAP/LDAPS		LDAP	<system name>
22	SFTP		SFTP	<system name>
1433	TCP		MS SQL database	<system name>
25	SMTP		email	<system name>

Ports, Protocols, and Services

SYSTEM INTERCONNECTIONS

Instruction: List all interconnected systems – these are systems external to the System in this plan. Provide the IP address and interface identifier (eth0, eth1, eth2) that provides the connection to the external system. Name the external organization and the IP address of the external system. Indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted.

<System name> Environment

IP Address and Interface on the System	External Organization Name and IP Address of External System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer etc.)	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Ports or Circuit #

System Interconnections

OPERATIONAL RACI

Legend: **"R" – Responsible** **"A" – Approve** **"C" – Consulted** **"I" – Informed** **"S" – Sign**	***Teams***								
	Help Desk	***Agency IT***	***Field Tech***	***Web Team***	***System Owner***	***ETS***	***ESO***	***Agency IT Steering Committee***	***Third Party Provider***
Operational Tasks									
Server Maintenance (OS Patching)		I		I	I	R			
Server Maintenance (IIS Patching)		R		I	I				
Application patching/upgrade		R		I	I				
Server Configuration		R		I	I				
Backups		I		I		R			
Data Restore (e.g. Logs and files)		R				I/C			
Application Break/Fix	I	I		R		I			
Hardware Break/Fix	I					R			
Application/Systems Integrations				R					
Security- F5 Firewall Maintenance/Monitoring				C			R		

Example

BENCHMARKS, CONFIGURATION, AND INSTALLATION GUIDE

{Check the box that the agency has in possession}

Installation Guide

☐ <System> Installation Guide

CIS Compliance Reports (examples)

☐ *<System> Test Webserver - CIS Microsoft IIS 8 L1 Benchmark*
☐ *<System> Test Webserver - CIS Windows Srvr 2012 R2 L1 Benchmark*

☐ *<System> Production Webserver - CIS Microsoft IIS 8 L1 Benchmark*
☐ *<System> Production Webserver - CIS Windows Srvr 2012 R2 L1 Benchmark*

Baseline Configuration Reports (examples)

☐ <System> Test Webserver - System Configuration
☐ <System> Production Webserver - System Configuration

Other artifacts:

FTI Security Guidelines Report (example)

☐ *<System> Server – FTI Security Guidelines Report*

CJIS Security Audit Report (example)

☐ *<System> Server – CJIS Security Audit Report*

3 MINIMUM SET OF CONTROLS

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

This section provides the minimum security controls using NIST SP 800-171 based on system categorization. For each of the controls, unless otherwise stated, the information system owner or designate is responsible for the control implementation. This section summarizes the implementation of the minimum management, operational, and technical controls, their requirements for the system, the status of implementation, usage of common control (if applicable), and the specific implementation details.

Organizations should not assume that satisfying the minimum control requirements listed below will automatically satisfy the necessary security requirements and controls to maintain confidentiality, integrity, or availability of the system. It is highly recommended that the latest revision of NIST SP800-53 be reviewed to determine if additional controls are necessary to secure the system. For example, in addition to the security objective of confidentiality, the objectives of integrity and availability may remain a high priority for organizations that are concerned with establishing and maintaining a comprehensive information security program.

Control Implementation Details, highlighted in BLUE, are for example purposes and can be use/modified/deleted at discretion.

Table 1 summarizes the management, operational and technical control requirements for the system and shows their status (in place, planned or not applicable and type of control).

There are three types of security controls for information systems that can be employed by an organization:

System-specific controls—controls that provide a security capability for a particular information system only;

Common controls—controls that provide a security capability for multiple information systems; or

Hybrid controls—controls that have both system-specific and common characteristics.

http://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf

3.1 ACCESS CONTROL

How does the system limit access to only authorized users, processes acting on behalf of authorized users, or devices (including other information systems)? – AC-2; AC-3; AC-17

Control Description:

☐ Common Control based on Statewide Standards ☐System Specific ☐ Hybrid or ☐ N/A

Limits information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Describe the set of procedures by which authorized users are provisioned/de-provisioned access to the system and the procedure by which authorized users access the system. If there is a procedure, note it as a common control (above). Additional questions: Does the system require passwords? Does the system have an authentication mechanism? Does the system require users to logon to gain access? Are account requests authorized before system access is granted? Does the organization maintain a list of authorized users, defining their identity and role and sync with system, application, and data layers?

Does the organization allow remote access to the controlled network? Does the organization use firewalling? Does the organization use end-to-end encryption with appropriate access? Are all the methods of remote access to the system authorized, monitored and managed?

SP 800-171 Ref: 3.1.1

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By utilizing written policies and/or procedures, It is not necessary to detail the steps in this block.

This control is inherited from the Statewide Standards, [*Cite reference # from Standards*]. Common Control is checked, cite reference from the Statewide Standards in the Control Implementation Details Section.

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (**EXAMPLE BELOW**):

Access overview: The system uses RBAC to authorize users for system level administration. It is integrated with the organization's Active Directory infrastructure. Users of the system are controlled through group membership in Active Directory.

<who reviews the accounts and how frequently?>

<Changes or re-authorization to accounts> The responsible managers facilitates any requested changes or re-authorization to the user accounts via the Help Desk request. If re-authorization is not obtained, the user accounts are disabled and subjected to removal according to organizational policies

System Administration: Upon receipt of an approved request, the Help Desk sends an authorization request to the System Owner. Upon approval from the System Owner, the Help Desk creates the user account on the Active Directory Server and adds the user account to the appropriate group. Active Directory automates the authorization of registered users by verifying the expiration date, approved password aging status, and proper password length, associated with the user account.

Application Authorization (if applicable) : <Describe how users of the application are provided access and how the authorization is performed.>

Microsoft Remote Desktop is configured for Administrator remote access when they are working remotely. The F5 perimeter firewall is configured to allow and forward IP xxx.xxx.xxx.xxx on port 32154 to connect and translate to the internal IP and standard remote desktop port (3389). All remote desktop connections are logged on the system. See Information Security Plan, para 6.2.2

How are functions, features, and transactions for authorized users limited? – AC-2; AC-3; AC-17

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Limits information system access to the types of transactions and functions that authorized users are permitted to execute.

Describe how the system restricts users to those parts of the system that they are explicitly permitted to use. This should be based on user "need-to-know" and their role within the system. Additional questions: Does the system use access control lists to limit access to applications and data based on role and/or identity? (e.g. RBAC)

This security requirement is also intended to limit the use of remote access to perform privileged actions on the system. Privileged commands are human initiated and involve the control, monitoring or administration of the system and security functions. Additional questions: Is remote access for privileged actions (such as software installation) only permitted for necessary operational functions? Is remote access for privileged commands and security-relevant information authorized only for compelling operational needs and is the rationale for such access documented?

Statewide Information Security Standards:

1.7.1. Server administrators shall use named user accounts that tie actions back to a specific individual for performing administrative work. Generic name and shared accounts shall not be used.
1.7.3 Each server shall have a firewall installed and securely configured.
1.7.7 All guest accounts shall be disabled.
2.3.2 Access shall be specifically granted to provide explicit access to objects within any information system.
2.3.3 Access shall be reviewed and modified in accordance with security policies prior to production deployment.
2.3.4 Access shall be removed immediately upon departure or change in employee job duties.
2.3.5 Administrative rights to information systems shall be tied to identified unique individuals.
2.3.6 Administrative rights shall be limited to only staff whose duties require it.

SP800-171 Ref: 3.1.2

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By utilizing written policies and/or procedures, It is not necessary to detail the steps in this block.

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

Access overview: The system uses RBAC to authorize users to the system. It is integrated with the organization's Active Directory infrastructure. Users of the system are controlled through group membership in Active Directory. Group roles are configured within the system that provide separation of access control rights.

The following groups are configured to control access:

Administrator – Provide for administration of the system/application. Administrators have access to all system components.

Guest – Allow users to logon to view training material

All changes to the system must be documented and approved through a change management process. Privileged commands and security-relevant administration (e.g. Host-based firewall changes, group policy changes that affect the system) through remote access must be approved by the System Owner.

Describe the control of data flow- AC-4

Control Description:

☒System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Controls the flow of information in accordance with approved authorizations.

The solutions may include firewalls, proxies, encryption, and other security technologies. Information flow control regulates where information can travel within an information system and between information systems. Examples of flow control restrictions include: blocking outside traffic that claims to be from within the organization, restricting web requests to the internet that are not from the internal web proxy server, and limiting information transfers between organizations. Additional questions: Are there architectural solutions to control the flow of system data? Do you document information flow control enforcement to assist in flow control decisions?

SP800-171 Ref: 3.1.3

Control Implementation Status (select only one):

☒In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

See the network and data flow diagrams attached to pages 9-11.

See the System Interconnections Table on page 13

Does the system audit privileged functions? – AC-6(9)

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Audit the execution of privileged functions.

Statewide Information Security Standards:

5.3.3 Logs shall be configured to capture security-related information in sufficient detail to recreate activity in support of incident investigations including, but not limited to, start up and shut down of audit functions, account logon and logoff activity, access to security relevant files, activities that modify, bypass, or negate security controls, failed attempts to access resources, and the use of privileged accounts.

SP800-171 Ref: 3.1.7

Control Implementation Status (select only one):

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Audit the execution of privileged functions.

Statewide Information Security Standards:

5.3.3 Logs shall be configured to capture security-related information in sufficient detail to recreate activity in support of incident investigations including, but not limited to, start up and shut down of audit functions, account logon and logoff activity, access to security relevant files, activities that modify, bypass, or negate security controls, failed attempts to access resources, and the use of privileged accounts.

SP800-171 Ref: 3.1.7

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By utilizing written policies and/or procedures, It is not necessary to detail the steps in this block.

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

System, security, and application logs are collected and retained on the system. All privileged access is removed from all standard user accounts, including local administrator access, thereby preventing users from executing privileged functions. This is governed by the implementation of CIS hardening standards and enforced by Active Directory Group Policies.

How are unsuccessful logon attempts managed? – AC-7

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Limit unsuccessful logon attempts.

This requirement seeks to limit the number of logon attempts. Multiple of unsuccessful logon attempts may indicate malicious attacks on the information system. Additional questions: Is the system configured to limit the number of invalid logon attempts? Is the system configured to lock the logon mechanism for a predetermined time after a predetermined number of invalid logon attempts? Does the system enforce a limit of a defined number of consecutive invalid access attempts during a defined time?

Statewide Information Security Standards:

2.1.13 Controls shall be implemented to protect information systems from brute force password guessing attacks (e.g. lock out after predetermined number of incorrect attempts.). Controls shall be commensurate with the associated risk to the information system and information.

2.5.1 All information systems shall support logging of access including logins to the information system, and granted and denied access to resources.

SP800-171 Ref: 3.1.8

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By utilizing written policies and/or procedures, It is not necessary to detail the steps in this block. (e.g. Unsuccessful logon attempts to the system are defined and governed by a domain-wide group policy standard - which includes unsuccessful logon attempts, password length, aging, and expiration requirements.

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

Group policy (or application configuration) enforces this standard by limiting the number of invalid logon attempts to <X>, after which the attempted account is locked for <XX> minutes.)

-or-

System has built in technical controls that include limiting unsuccessful logon attempts. After <X> attempts, the user account attempted is locked for a period of <X> minutes.

Does the system display privacy notices at logon? – AC-8

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Provide privacy and security notices consistent with applicable Controlled Unclassified Information (CUI) rules.

System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Additional questions: Does the logon screen display notices upon initial logon? Does the system display the system use information before granting access? Does the system ensure that any references to monitoring, recording, or auditing are consistent with privacy accommodations? Does the system include a description of the authorized uses of the system?

SP800-171 Ref: 3.1.9

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By utilizing written policies and/or procedures, It is not necessary to detail the steps in this block.

<If 'N/A' is selected> <System Name> does not include privacy notices for users using the system.

How are external systems that access the system controlled and verified? – AC-20

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Terminate (automatically) a user session after a defined condition.

This control does not apply to external systems used to access public interfaces. Additional questions: Are only authorized systems permitted external access? Are guidelines and restrictions placed on the use of external system access? Do those systems meet the security standards set by State Standards?

SP800-171 Ref: 3.1.20

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

See System Interconnections on page 13

3.2 AWARENESS AND TRAINING

Are managers, system administrators, and users of the system made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organization information systems? – AT-2; AT-3

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Information security-related duties and responsibilities are not just IT related or wholly the responsibility of the ESO. All personnel within the organization are to be trained and understand information security as it relates to their job duties. Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems. Additional questions: Do all users, managers, and system administrators receive initial and annual training commensurate with their roles and responsibilities? Does the training provide a basic understanding of the need for information security, applicable policies, standards, and procedures related to the security of the information system, as well as user actions to maintain security and respond to suspected security incidents? Does the training also address awareness of the need for operations security? Is basic security awareness training provided to all system users before authorizing access to the system and at least annually thereafter?

Statewide Acceptable Use of Information Assets:

The division administrator is responsible to enforce this policy and informing employees of this policy and obtaining employee signature on Acceptable Use Agreement for all employees using state information assets in the scope of employment.

The Manager of the Authorized User is responsible for ensuring that the Authorized User has received training on acceptable use, understands their responsibilities and signs an Acceptable Use Agreement and knows the importance of protecting confidential and sensitive information contained on information assets that can be released during voice/data transmissions or with the loss or theft of a MCD, and receives a copy of the policies.

The Authorized User is responsible for taking reasonable steps to ensure the physical security of state information assets, use the state information assets in a manner consistent with the Acceptable Use Agreement, and taking reasonable steps to prevent the release of confidential or sensitive information.

SP800-171 Ref: 3.2.1

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Statewide Acceptable Use of State Information Assets, policy number 107-004-0110, commonly applied.

Are personnel adequately trained in the area of information security to carry out their assigned duties and responsibilities? – AT-2; AT-3

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals, and the specific security requirements of the organization and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, software developers, acquisition/ procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security requirement assessors, and other personnel having access to system-level software, adequate security- related technical training specifically tailored for their assigned duties. Additional questions: Does Information Systems personnel receive security training on initial and annual training on their operational, managerial, and technical roles and responsibilities? Does the training cover physical, personnel, and technical safeguards and countermeasures? Does the training address required security requirements related to environmental and physical security risks? Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on a periodic basis?

SP800-171 Ref: 3.2.2

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are personnel provided security awareness training on recognizing and reporting potential indicators of insider threat? – AT-2(2)

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Security and privacy awareness training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through organizational channels in accordance with established policies and procedures. Additional questions: Do users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threat, e.g., long-term job dissatisfaction, attempts to gain unauthorized access to information, unexplained access to resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of company policies? Does security training include how to communicate employee and management concerns regarding potential indicators of insider threat?

SP800-171 Ref: 3.2.3

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

3.3 AUDIT AND ACCOUNTABILITY

Are system audit records created, protected, and retained to enable monitoring, analysis, investigation and reporting? – AU-2; AU-3; AU-4; AU-6; AU-11; AU-12

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. In addition, allocating sufficient audit storage capacity reduces the likelihood of storage capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

It is important for organizations to create audit records, protect the integrity of audit records and retain audit records. Good audit records will allow the organization to monitor system activities, perform analysis on system activities, and provide evidence for use during an investigation and reporting. Additional questions: Does the system provide alert functions? Does the organization perform audit analysis and review? Does the organization create, protect, and retain information system audit records to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity? Are mechanisms used to integrate audit review, analysis, and reporting to processes for investigation and response to suspicious activity?

Statewide Information Security Standards:

2.5.1 All information systems shall support logging of access including logins to the information system, and granted and denied access to resources.
2.5.2 Audit logs shall be tamper-resistant. In all cases, access to the logs shall be limited only to those with a need to access.
5.3.1 Log data from servers, network components (firewalls, switches, routers, etc.) and other devices/services shall be collecting on an ongoing basis. Events shall be logged as they occur.
5.3.2 Log data shall be collected in its original form but also may be normalized for log aggregation.
5.3.3 Logs shall be configured to capture security-related information in sufficient detail to recreate activity in support of incident investigations including, but not limited to, start up and shut down of audit functions, account logon and logoff activity, access to security relevant files, activities that modify, bypass, or negate security controls, failed attempts to access resources, and the use of privileged accounts.
5.3.4 Logs shall be regularly reviewed and analyzed for indications of unauthorized or unusual activity. Suspicious activity shall be investigated, findings reported to appropriate management, and necessary follow-up actions taken.
5.3.5 Log data shall, by default, be considered Level 3 until Level 3 information has been removed for public disclosure. Privacy of the log information shall be protected in accordance with the most restrictive applicable regulations and laws.
5.3.6 Logs shall be retained in accordance with the state retention requirements for the information and information systems they are logging. Where no specific retention rules apply, logs shall be kept for six months to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Logs pertaining to ongoing information security incidents shall be preserved as long as necessary to complete and close the investigations

SP800-171 Ref: 3.3.1

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block. (E.g. Statewide Information Security Standards, para 2.5 & 5.3, commonly applied.)

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

STORAGE CAPACITY: Each system component has been allocated enough disk space to retain 6 months' worth of logged events.

ACCESS TO LOGS: Access to log files is limited to named administrators only.

Operating system level auditing: All security, system, and application events are logged within the windows environment. Logs are retained for a period of <X> days.

The System Administrator (SA), in coordination with System Owners (SO), shall:

a) Configure the system to audit for the following events:
    a. The following events shall be identified within server audit logs:
        i. Server startup and shutdown

ii. Loading and unloading of services
iii. Installation and removal of software
iv. System alerts and error messages
v. Successful and unsuccessful account logon events
vi. account management events
vii. policy change
viii. privilege functions
ix. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;

Application level auditing: The <system name> application logs the following events:

- User logon/logoff

Can system users be uniquely traced or will shared or system accounts be used? – AU-2; AU-3; AU-6; AU-11; AU-12

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Companies obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Additional questions: Does the organization correlate network activity to individual user information? Can the organization uniquely trace and hold accountable users responsible for unauthorized actions? Does the system protect against an individual denying having performed an action (non-repudiation)?

Statewide Information Security Standards:

1.7.1. Server administrators shall use named user accounts that tie actions back to a specific individual for performing administrative work. Generic name and shared accounts shall not be used.
2.1.2 Policy shall be established directing users not to reveal passwords to anyone, including supervisors, family members or co-workers.
2.1.3 Management approval shall be required for establishing each user ID and a process shall be in place to remove or suspend user IDs that are no longer required to perform an assigned job function.
2.3.5 Administrative rights to information systems shall be tied to identified unique individuals.

SP800-171 Ref:3.3.2

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block. (E.g. Statewide Information Security Standards, para 1.7.1, 2.1.2, 2.1.3, & 2.3.5, commonly applied.)

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

For system access: Users are assigned unique AD accounts and all privileged access requires the use of a .priv account that is uniquely assigned to the individual. The use of generic or shared accounts are prohibited.

For Application access: All users are assigned a unique username and required to provide a unique password.

Do audit process failure events trigger an alert? – AU-5

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Alert in the event of an audit process failure. An accurate and current audit trail is essential for maintaining a record of system activity. If the system fails, the SA must be notified and must take prompt action to correct the problem. Minimally, the system must log this event and the SA will receive this notification during the daily system log review. If feasible, active alerting (such as e-mail or paging) should be employed consistent with the organization's established operations management systems and procedures. Additional questions: Will the system alert the SA in the event of an audit processing failure? Does the system maintain audit records on host servers until log delivery to central repositories can be re-established? Is there real-time alert when any defined event occurs? **SP800-171 Ref: 3.3.4**
Control Implementation Status (select only one): ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW): The System Administrator will configure the system to alert the [Assignment: organization-defined personnel or roles or email distribution group] in the event of an audit failure. Additionally, real-time alerts will be configured when the following audit events occur: 1) recording of authentication attempts, and/or escalation of privileges. These events will be considered a potential security event and be responded to as outlined in the Incident Response Policy.

Is the systems internal clock synchronized with an authoritative source? – AU-8

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. This provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. Additional questions: Does the system use internal system clocks to generate time stamps for audit records? Can the records time stamps be mapped to UTC (Coordinated Universal Time), compare system clocks with authoritative NTP servers, and synchronize system clocks when the time difference is greater than 1 second? Does the system synchronize internal system clocks on a defined frequency? **SP800-171 Ref: 3.3.7**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW): The System Administrator will configure the system to utilize an authoritative time source for time synchronization.

Is audit information protected from unauthorized access, modification, and deletion? – AU-9

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Protect audit information and audit tools from unauthorized access, modification, and deletion.

This security requirement seeks to prevent a malicious user from erasing all evidence of their activities in the audit information. Only authorized users should have access to audit information and audit tools. Additional questions: Does the system protect audit information and audit tools from unauthorized access, modification, and deletion?

Statewide Information Security Standards:

2.5.4 Audit logs shall be tamper-resistant. In all cases, access to the logs shall be limited only to those with a need to access.
5.3.5 Log data shall, by default, be considered Level 3 until Level 3 information has been removed for public disclosure. Privacy of the log information shall be protected in accordance with the most restrictive applicable regulations and laws.
5.3.6 Logs shall be retained in accordance with the state retention requirements for the information and information systems they are logging. Where no specific retention rules apply, logs shall be kept for six months to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Logs pertaining to ongoing information security incidents shall be preserved as long as necessary to complete and close the investigations

SP800-171 Ref: 3.3.8

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The organization authorizes access to management of audit functionality to only authorized system administrators and designated security officials.

3.4 CONFIGURATION MANAGEMENT

Are baseline configurations established and maintained? – CM-2; CM-6; CM-8

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles

The effective integration of security requirements into enterprise architecture helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizations processes. Additional questions: Are baseline configurations developed, documented, and maintained for each information system type? Do baseline configurations include software versions and patch level, configuration parameters, network information including topologies, and communications with connected systems? Are baseline configurations updated as needed to accommodate security risks or software changes? Are deviations from baseline configurations documented?

SP800-171 Ref: 3.4.1

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure

and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <organization>.

ETS manages all server baseline configurations. ETS has partially hardened the server OS according to the CIS Server 2012 R2 Level 1 benchmark standards. Additionally, ETS has partially hardened the IIS application according to the CIS IIS 10 Level 1 benchmark standards. Compliance reports are attached to this security plan.

A baseline configuration report is attached to this SSP.

Are security configuration settings established and enforced? – CM-2; CM-6; CM-8

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Additional questions: Are security settings included as part of baseline configurations? Do security settings reflect the most restrictive settings appropriate? Are changes or deviations to security settings documented?

SP800-171 Ref: 3.4.2

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <organization>.

ETS has partially hardened the server OS according to the CIS Server 2012 R2 Level 1 benchmark standards. Additionally, ETS has partially hardened the IIS application according to the CIS IIS 10 Level 1 benchmark standards. Compliance and configuration reports are attached to this security plan.

<Organization> will need to review and configure Level 1 items not configured by ETS. Where Level 1 items will not be configured according to CIS recommendations, <organization> will need to document rationale within the CIS Benchmark XLS worksheet and attach it to this SSP.

Are the impact of changes to the system security analyzed prior to implementation? – CM-4

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Analyze the security impact of changes prior to implementation.

System Administrators analyze changes to information systems and any associated security ramifications. Additional questions: Are changes tested prior to implementation? Are configuration changes tested, validated, and documented before installing them on the operational system? Has testing been ensured to not interfere with system operations?

SP800-171 Ref: 3.4.4

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

All hardware or firmware changes are documented and approved through the ETS change management procedure. The ETS team will apply all OS system updates on a regularly scheduled basis.

<system name> application software will be updated following the <ORGANIZATION> change management procedure.

Changes or deviations that affect system security controls will be tested prior to implementation to test their effectiveness. Only those changes or deviations that continue to meet compliance requirements will be approved and implemented.

Are logical access controls defined, documented, approved, and enforced? – CM-5

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Organizations should permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Additional questions: Are only employees who are approved to make physical or logical changes on systems allowed to do so? Are authorized personnel approved and documented? Does all change documentation include the name of the authorized employee making the change?

SP800-171 Ref: 3.4.5

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

All physical access restrictions are managed by the ETS teams.

Logical access for system administration is controlled through group policy (applied by the ETS team). Once joined to the domain, AD groups (that contain both ETS technicians and <ORGANIZATION> technicians) are added to the local administrator group for system administration. Membership to the AD groups are controlled by each department.

Logical access for application administration is controlled by the ETS team. Requests by the <ORGANIZATION> team to add a technician to the application administration group is made to the ETS team. The ETS team will then add the technician to the "LA" group.

Does the system employ the principle of least functionality? – CM-7

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Employ the principle of least functionality by configuring the information system to provide only essential capabilities.

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential company operations. Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations should limit component functionality to a single function per device (e.g., email servers or web servers, but not both).

Statewide Information Security Standards:
1.7.3 Each server shall have a firewall installed and securely configured.
1.7.5 Servers shall be configured to run only required services. All unnecessary services shall be disabled.

SP800-171 Ref: 3.4.6

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished. List (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

(a) The system must be configured to provide only essential capabilities – e.g. email server or web server, but not both.
(b) Ports, protocols, and/or services, must be specifically prohibited or restricted:
- (1) Domain Name System be (DNS)
  - Port 53 / Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
- (2) File Transfer Protocol (FTP)
  - Ports 20, 21 / TCP
- (3) Internet Message Access Protocol (IMAP)
  - Port 143 / TCP, UDP
- (4) Internet Relay Chat (IRC)
  - Port 194 / UDP
- (5) Network Basic Input Output System (NetBIOS)
  - Port 137 / TCP, UDP
- (6) Post Office Protocol 3 (POP3)
  - Port 110 / TCP
- (7) Session Initiation Protocol (SIP)
  - Port 5060 / TCP, UDP
- (8) Simple Mail Transfer Protocol (SMTP)
  - Port 25 / TCP (Inbound)
- (9) Simple Network Management Protocol (SNMP)
  - Port 161 / TCP, UDP
- (10) Structured Query Language (SQL)
  - Port 118 / TCP, UDP
  - Port 156 / TCP, UDP
- (11) Telnet
  - Port 23 / TCP

(c) See Table 10-4, page 10, "Ports, Protocols and Services" table for the list of ports that are required to be left open.

Does the system control and monitor user-installed software? Is the use of software in accordance with contract agreements and copyright laws? – CM-10; CM-11

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Control and monitor user-installed software. Approaches to meeting this requirement to control and monitor software installed by users can include policies and procedures. Policies should fully describe what is allowed and procedures should be in place to check that the policy is not violated. Additional questions: Are user controls in place to prohibit the installation of unauthorized software? Is all software in use on the information systems approved? Does the organization follow good practices which require that user-installed software execute in confined physical or virtual machine environment with limited privileges? **SP800-171 Ref: 3.4.9**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW): Controls are be in place to prohibit the unintentional installation of unauthorized or unwanted software. All software for the system must be approved through the <ORGANIZATION> change management procedure.

3.5 IDENTIFICATION AND AUTHENTICATION

How does the system identify users? – IA-2; IA-5

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Identify information system users, processes acting on behalf of users, or devices.

Identification of users is a prerequisite for granting access to resources within the system. It prevents unauthorized individuals or processes from entering the system. Identification and authentication of users is the basis for many types of access control and user accountability. Additional questions: Does the system make use of organization-assigned accounts for unique access by individuals? If administrator service accounts are necessary for device or process authentication, are the accounts created by the central identity management team and assigned to a member of the team using the account (separation of duties)? Are organization and administrator service accounts managed centrally and deleted automatically when an individual leaves the organization?

Statewide Information Security Standards:

1.7.1. Server administrators shall use named user accounts that tie actions back to a specific individual for performing administrative work. Generic name and shared accounts shall not be used.
2.1.1 The combination of a unique User ID and a valid password shall be the minimum requirement for granting access to information except for that which is publicly viewable.
2.1.2 Policy shall be established directing users not to reveal passwords to anyone, including supervisors, family members or co-workers.
2.1.3 Management approval shall be required for establishing each user ID and a process shall be in place to remove or suspend user IDs that are no longer required to perform an assigned job function.

SP800-171 Ref: 3.5.1

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

System level accounts are managed individually by ETS and the <ORGANIZATION> team. Each team centrally manages and assigns accounts to groups. When an administrator leaves the organization, each team is responsible for deleting the account from the system.

Application level accounts are managed by the <system name> Administrator.

How does the system authenticate (or verify) user identities? – IA-2; IA-5

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. Additional questions: Are the accounts in use assigned and managed by a central identity management system? Are accounts provisioned as part of the established account creation process? Are accounts provisioned as part of the established account creation process? Are accounts uniquely assigned to new employees, contractors, or subcontractors upon hire? Are initial passwords randomly generated strings provided via a password reset mechanism to each employee? Is the password reset upon first use? Do all passwords follow the statewide standard?

Statewide Information Security Standards:

2.1.1 The combination of a unique User ID and a valid password shall be the minimum requirement for granting access to information except for that which is publicly viewable.
2.1.2 Policy shall be established directing users not to reveal passwords to anyone, including supervisors, family members or co-workers.

2.1.3 Management approval shall be required for establishing each user ID and a process shall be in place to remove or suspend user IDs that are no longer required to perform an assigned job function.
2.1.4 The construction and specifications of a password shall be defined in agency policy and shall be of a complexity consistent with the information classification level the user has access to.
2.1.5 Passwords shall be a minimum length of 10 characters.
2.1.6 Non expiring user account passwords are not permitted.
2.1.9 Vendor supplied passwords for information systems shall be changed immediately upon installation.
2.1.10 Passwords shall be changed periodically determined by the information classification level the user has access to and the password length and complexity. Passwords shall be changed immediately whenever there is a chance that the password or information system has been compromised.

SP800-171 Ref: 3.5.2

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The system authenticates users at the system level, as well as the application level, through the use of user ID and passwords. System user accounts for both ETS and <ORGANIZATION> administrators are centrally managed through their respective active directory environments.

<ORGANIZATION> AD password requirements do not currently meet statewide standards of 10 characters.

<System name> passwords do not currently meet statewide standards of 10 characters.

Is multi-factor authentication used for local or network access to privileged accounts? – IA-2(1)

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

Additional questions: Does the system uniquely identify and authenticate users? Is multifactor authentication used for local access to privileged accounts? Is multifactor authentication used for network access to privileged accounts?

Statewide Information Security Standards:

2.1.14 Special Access Privileges: Procedures shall be established to maintain documentation of special access privileges, including high-level privileges (e.g.: root access, administrator), system utilities requiring high-level privileges, and privileges that provide access to sensitive network devices, operating systems, or software application capabilities. Procedures shall include:

2.1.14.6 Requiring multifactor authentication.

SP800-171 Ref: 3.5.7

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished.

Does the system enforce a minimum password complexity? – IA-5(1)

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Enforce a minimum password complexity and change of characters when new passwords are created. Additional questions: Does the organization specify a degree of complexity and follow statewide standards?

Statewide Information Security Standards:

2.1.4 The construction and specifications of a password shall be defined in agency policy and shall be of a complexity consistent with the information classification level the user has access to.
2.1.5 Passwords shall be a minimum length of 10 characters.
2.1.6 Non expiring user account passwords are not permitted.

SP800-171 Ref: 3.5.7

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, it is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The system inherits the control from <ORGANIZATION> group policy. The password policy is configured to accept the following: <INSERT CONFIGURATION ITEMS HERE>

(For Windows based systems, obtain a GPResult HTML report and attach to this SSP)

<ORGANIZATION> AD password requirements do not currently meet statewide standards of 10 characters.

<system name> passwords do not currently meet statewide standards of 10 characters.

Is authentication information obscured? – IA-6

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Obscure feedback of authentication information.

Do the authentication mechanisms obscure feedback of authentication information during the authentication process? Do the authentication mechanisms not return any system specific information such as “wrong password” or “wrong username”?

Statewide Information Security Standards:

2.1.8 Passwords shall be redacted on login to all information systems so the password cannot be read off of the screen.

SP800-171 Ref: 3.5.11

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

User passwords are obfuscated by * when entered by the user via the <system name> application.

3.6 INCIDENT RESPONSE

Is an operational incident-handling capability established? – IR-2; IR-4; IR-5; IR-6; IR-7

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

<ORGANIZATION> and the SDC follow the Statewide Incident Response Policy and Statewide Incident Response Plan
http://www.oregon.gov/<organization>/Policies/107-004-120.pdf
http://www.oregon.gov/<organization>/OSCIO/Documents/InformationSecurityIncidentResponsePlan.pdf

SP800-171 Ref: 3.6.1

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

ETS and <ORGANIZATION> will follow their respective IR procedures. Where IR procedures don't exist, the organization will follow the statewide IR policy and statewide IR plan.

Are incidents tracked, documented, and reported? – IR-2; IR-4; IR-5; IR-6; IR-7

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

<ORGANIZATION> and the SDC follow the Statewide Incident Response Policy and Statewide Incident Response Plan
http://www.oregon.gov/<organization>/Policies/107-004-120.pdf
http://www.oregon.gov/<organization>/OSCIO/Documents/InformationSecurityIncidentResponsePlan.pdf

SP800-171 Ref: 3.6.2

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

ETS and <ORGANIZATION> will follow their respective IR procedures. Where IR procedures don't exist, the organization will follow the statewide IR policy and statewide IR plan.

3.7 MAINTENANCE

How is maintenance on the system performed? – MA-2

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Perform maintenance on organizational information systems. Additional questions: Are IT system maintenance tools (e.g., tools used for diagnostics, scanner and patching tools) managed? Is there a list of approved tools and their access and location is controlled? Are all systems, devices, and supporting systems for the company maintained per manufacturer recommendations or company defined schedules? Who performs maintenance on the information system? Who approves maintenance activities? Is the equipment sanitized prior to removal for maintenance or at EOL?

SP800-171 Ref: 3.7.1

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

<ORGANIZATION> performs patch management on a 30 day cycle *{see patching policy}*, and maintain 7x24 hr. hardware and software maintenance for its systems. All server hardware is on a 3 year depreciation cycle after which the hardware is refreshed with new state of the art systems. See <ORGANIZATION> Patch Management policy, no 3.01.06.01.001.POL

How are maintenance controls provided effectively? – MA-2

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance. Controls may include lists of authorized tools, authorized employees, and authorized techniques and mechanisms. Additional questions: Are controls in place that limit the tools, techniques, mechanisms, and employees used to maintain information systems, devices, and supporting systems? Is the equipment sanitized prior to removal for maintenance or at EOL?

Statewide Information Security Standards:

2.1.14 Special Access Privileges: Procedures shall be established to maintain documentation of special access privileges, including high-level privileges (e.g.: root access, administrator), system utilities requiring high-level privileges, and privileges that provide access to sensitive network devices, operating systems, or software application capabilities. Procedures shall include:
2.1.14.1 Specifying and documenting the purpose and acceptable use of special access privileges;
2.1.14.2 Management approval for granting special access privileges;
2.1.14.3 Requiring different accounts or different authentication tokens than those used with the individual's regular user account;
2.1.14.4 Specifying and documenting a procedure to remove special access privileges;
2.1.14.5 Continual monitoring;
2.1.14.6 Requiring multifactor authentication.

SP800-171 Ref: 3.7.2

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

Are maintenance activities of personnel not having normal access supervised (e.g. contractors)? – MA-5

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Supervise the maintenance activities of maintenance personnel without required access authorization. Additional questions: Are all activities of maintenance personnel (who do not normally have access to a system) monitored? Has the company defined approved methods for supervision?

SP800-171 Ref: 3.7.6

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

The system inherits the control from the Organizational Security Policies and Procedures. Refer to the P&P's for additional information.

3.8 MEDIA PROTECTION

Is information system media securely stored in protected areas? – MP-2; MP-6

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Protect (i.e., physically control and securely store) information system media containing Level 2 or higher information, both paper and digital. For media containing information determined by companies to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the company or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

Statewide Information Security Standards:

1.1.1 **Level 1:** Access control shall be in place to prevent unauthorized changes. Access logging shall be in place to identify what was changed and who changed it in accordance with the Access Control standards in Section 2.
1.1.2 **Level 2**: All Level 1 standards apply. Access control shall be in place to prevent unauthorized viewing. Access logging shall be in place to identify unauthorized attempts.
1.2.1 **Level 1:** Level 1 information stored on electronic media shall be protected from unauthorized changes to, or deletion of, the original "published" document.
1.2.2 **Level 2:** All Level 1 standards apply. Information stored on paper shall not be left unattended in open or public areas.

SP800-171 Ref: 3.8.1

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, it is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

The data classification of the <system name> system is Level 2. Physical access controls provide adequate protection.

Per the Statewide Information Security Standards document, media containing Level 3 and Level 4 information is controlled while at rest on digital and paper form.

Is access to the system media limited to only authorized users and managed under least access rules? – MP-2; MP-6

Control Description:

☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A

Limit access to Level 2 or higher information on information system media to authorized users. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media.

Statewide Information Security Standards:

1.1.1 **Level 1:** Access control shall be in place to prevent unauthorized changes. Access logging shall be in place to identify what was changed and who changed it in accordance with the Access Control standards in Section 2.
1.1.2 **Level 2**: All Level 1 standards apply. Access control shall be in place to prevent unauthorized viewing. Access logging shall be in place to identify unauthorized attempts.
1.2.1 **Level 1:** Level 1 information stored on electronic media shall be protected from unauthorized changes to, or deletion of, the original "published" document.
1.2.2 **Level 2:** All Level 1 standards apply. Information stored on paper shall not be left unattended in open or public areas.

SP800-171 Ref: 3.8.2

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

The data classification of the <system name> system is Level 2. Physical access controls provide adequate protection.

Per the Statewide Information Security Standards document, media containing Level 3 and Level 4 information is controlled while at rest on digital and paper form.

Is system media sanitized or destroyed? – MP-2; MP-6

Control Description:

☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A

Sanitize or destroy information system media, containing Level 3 or higher information, before disposal or release for reuse.

Statewide Information Security Standards:

1.1.3 Disposal of media storing Level 3 data shall be sanitized in accordance with the Sustainable Acquisition and Disposal of Electronic Equipment (e-Waste/Recovery) Policy #107-009-0050. Agencies may elect to destroy media rather than sanitize.

SP800-171 Ref: 3.8.3

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

Prior to disposal via the State's disposal process, all media is either sanitized in accordance with statewide policy #107-009-0500 or destroyed.

How is the use of removable media controlled? – MP-7

Control Description:

☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A

Control the use of removable media on information system components. Restrict or prohibit the use of removable media on the system and prohibit the use of portable storage devices when devices have no identifiable owner.

Statewide Acceptable Use of Information Systems Policy:

Hardware devices shall not be attached to a state provided computer that the user does not employ in the user's assigned work. Privately owned devices shall not be connected to state networks, computers (including remotely used computers) or other equipment without approval of the agency prior to connection. All hardware attached to state systems shall be appropriately configured, protected and monitored so it will not compromise state information assets.

Statewide Information Security Standards:

1.5.2 Agencies that choose to allow portable devices (cameras, I-phones, USB drives, etc.) not owned by the agency to connect to agency owned equipment shall provide an exception and approval process by which the agency grants and documents approval to attach the equipment.

SP800-171 Ref: 3.8.7

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

Are there written and signed policies and/or procedures that provide instruction covering this control? If so, reference the policy and/or procedure and remove the remainder of this narrative. By enforcing written policies and/or procedures, It is not necessary to detail the steps in this block

If no policy and/or procedure exists, then provide enough detail to describe how this control is accomplished (EXAMPLE BELOW):

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

The use of removable media is governed and monitored per Statewide Acceptable Use of Information Systems policy and the Statewide Information Security Standards.

How is the confidentiality of backups protected? – CP-9

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Protect the confidentiality of backup at storage locations.

Statewide Information Security Standards:

5.5.1 Information systems and the classification levels of the data stored upon them, time-criticality of business processes, business continuity plans, legal, regulatory, contractual obligations and retention requirements shall be analyzed to determine the frequency with which backups need to be made, the backup media types, and encryption requirements.

5.5.1.1 The analysis process shall define a backup cycle and document it as well as determining backup media selection and requirements.

5.5.1.2 The analysis process shall include the evaluation of security threats and mitigation to restore data.

SP800-171 Ref: 3.8.9

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The Hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

Backups of the <system name> application are transmitted to the ETS backup facility, located out of the state of Oregon. Access to <system name> system backups are controlled by ETS personnel and encrypted while at rest and, if necessary, in transport and at the off-site storage facility. Access to backup media is limited to only a few identified ETS personnel.

3.9 PERSONNEL SECURITY

Are individuals screened prior to authorizing access? – PS-3; PS-4; PS-5

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Screen individuals prior to authorizing access to information systems containing level 2 or higher information. **SP800-171 Ref: 3.9.1**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: <ORGANIZATION> performs background checks on all FTE's prior to being hired, and requires contractor companies, with which it deals with, to perform similar background checks on all contractors working for the agency.

How is the system protected during or after personnel terminations and transfers? – PS-3; PS-4; PS-5

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Ensure that systems are protected during and after personnel actions such as terminations and transfers. **SP800-171 Ref: 3.9.2**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Planned Control: Access to systems are protected by removing the user's access via <ORGANIZATION> Active Directory infrastructure, thereby protecting systems in the event of terminations and transfers.

3.10 PHYSICAL AND ENVIRONMENTAL PROTECTION

How is physical access to organizational information systems limited? – PE-2; PE-6

Control Description:

☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A

Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

Statewide Information Security Standards:
4.1.1 All facilities shall have, at a minimum, a single physical security control protecting it from unauthorized access, damage, or interference.
4.1.2 All facilities that process or store information classified at level 3 or 4 shall have multiple layers of physical security controls.

SP800-171 Ref: 3.10.1

Control Implementation Status:

☒In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

The agency's information systems reside in the ETS data center. Access to the data center is controlled by proximity ID cards. Access to the data center server room floor is further restricted to essential employees only. Non ETS or ESO staff are required to obtain visitor badges and be escorted. All non-essential server room staff are required to be escorted at all times while in the data center server room.

How is physical access authorized? – PE-2; PE-6

Control Description:

☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A

Protect and monitor the physical facility and support infrastructure for those information systems.

Statewide Information Security Standards:
4.1.1 All facilities shall have, at a minimum, a single physical security control protecting it from unauthorized access, damage, or interference.
4.1.2 All facilities that process or store information classified at level 3 or 4 shall have multiple layers of physical security controls.

SP800-171 Ref: 3.10.2

Control Implementation Status:

☒In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

ETS protects and monitors the physical facility and support infrastructure for the <system name> system.

3.11 RISK ASSESSMENT

Will the organization periodically asses the risk of this system (e.g. impact to operations if confidentiality, integrity, or availability is compromised) to the agency? – RA-3

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Periodically assess the risk of the system to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of information.

SP800-171 Ref: 3.11.1

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

System risk assessments will be completed, at least annually, using Tenable SecurityCenter compliance scans, as well as vulnerability reports, and an internal review of compliance to standards and procedures.

Last assessment completed: January 2018

Are there scans performed periodically for vulnerabilities? – RA-5

Control Description:

☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A

Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.

Statewide Information Security Standards:

5.9.7 Custom developed applications shall be tested on a defined schedule for vulnerabilities and updated to correct identified vulnerabilities.
5.9.8 If no patch is available, other controls shall be implemented, such as turning off services or capabilities related to the vulnerability; adapting or adding access controls, e.g. firewalls, at network borders; increased monitoring to detect or prevent actual attacks; raising awareness of the vulnerability; keeping an audit log of all procedures undertaken; evaluating the technical vulnerability management process in order to ensure its effectiveness; and addressing high-risk information systems first.

SP800-171 Ref: 3.11.2

Control Implementation Status (select only one):

☒In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

The ESO performs frequent scans using the Tenable vulnerability scanning system. Vulnerabilities and recommendations for remediation are reported to the ETS and <ORGANIZATION> teams. Additionally, ETS and <ORGANIZATION> designated individuals have logon access to the Tenable SecurityCenter application to review reported vulnerabilities on the system.

How are vulnerabilities remediated? – RA-5

Control Description:

☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A

Remediate vulnerabilities in accordance with assessments of risk.

Statewide Information Security Standards:

5.9.1 All operating systems and commercial off-the-shelf/open source software shall be patched and maintained at current vendor supported levels unless there is a documented business reason for not applying a specific patch.
5.9.2 Agencies shall immediately deploy security patches to operating systems and applications upon release unless the agency follows a documented procedure for testing and deploying security patches within an identified timeframe.
5.9.3 Operating System and commercial off-the-shelf/open source software for which the vendor/open source community no longer provides security patches is considered deprecated and shall be remediated with documented controls or removed from production.
5.9.4 Wherever possible, automated patching systems shall be implemented to automatically update operating systems and applications.
5.9.5 Automated patching systems shall log which information systems have received the patches and audit for information systems that have been missed.
5.9.6 An application update management process shall be implemented to ensure the most up-to-date approved patches and application updates are installed for all software.
5.9.7 Custom developed applications shall be tested on a defined schedule for vulnerabilities and updated to correct identified vulnerabilities.
5.9.8 If no patch is available, other controls shall be implemented, such as turning off services or capabilities related to the vulnerability; adapting or adding access controls, e.g. firewalls, at network borders; increased monitoring to detect or prevent actual attacks; raising awareness of the vulnerability; keeping an audit log of all procedures undertaken; evaluating the technical vulnerability management process in order to ensure its effectiveness; and addressing high-risk information systems first.

SP800-171 Ref: 3.11.3

Control Implementation Status (select only one):

☐In Place ☒Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

ETS, working with <ORGANIZATION>, performs patch management, on a 30-day cycle, for both security and system patches. Other vulnerabilities which have patches released from the vendor, are applied according to the ETS patch management procedure.

Vulnerabilities requiring configuration changes (e.g. registry edits, file/folder edits) will be assessed for risk, configuration changes approved through the change management process, and tested before being applied by <ORGANIZATION> to production servers.

As of February 2018, initial CIS Level 1 configuration benchmark reports have delineated gaps in numerous configuration items. <ORGANIZATION> has listed these on the system risk register for risk assessment and possible remediation plans.

3.12 SECURITY ASSESSMENT AND AUTHORIZATION

Will the organization periodically assess the security controls? – CA-2; CA-5; CA-7; PL-2

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application. Additional questions: Has a periodic (e.g., annual) security assessment been conducted to ensure that security controls are implemented correctly and meet the security requirements? Does the assessment scope include all information systems and networks, including all security requirements and procedures necessary to meet the compliance requirements of the environment? Does the assessment include, but is not limited to, vulnerability scanning, penetration testing, security control testing and reviews, configuration testing and reviews, log reviews, and talking with company employees? Is the assessment conducted by company employees? Is the assessment conducted by an independent security auditor/consultant? Is a final written assessment report and findings provided to company management after the assessment? **SP800-171 Ref: 3.12.1**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: None. There are no policies or procedures in place to periodically assess the security controls of the <system name> system.

Are weaknesses and deficiencies identified? Is there an action plan to remediate weaknesses or deficiencies? – CA-2; CA-5; CA-7; PL-2

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems. Additional questions: Is there an action plan to remediate identified weaknesses or deficiencies? Is the action plan maintained as remediation is performed? Does the action plan designate remediation dates and milestones for each item? Are deficiencies and weaknesses identified in security requirements assessments added to the action plan within a specified timeframe (e.g., 30 days) of the findings being reported? **SP800-171 Ref: 3.12.2**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: None. There is no POA&M document to remediate identified weaknesses or deficiencies.

Are the system security controls monitored and alerted for modifications? – CA-2; CA-5; CA-7; PL-2

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. Additional questions: Are continuous monitoring tools deployed for front internet facing systems (computers with IP addresses that can be reached from the internet) or those used to store or transmit sensitive data? At a minimum, are these systems monitored for privileged access, permission changes, kernel modifications, and binary changes against a control and system baseline? Are continuous monitoring reports and alerts reviewed frequently (e.g., daily)? Are unauthorized changes or unauthorized access reported to company management, and information system owner within a certain time frame (e.g., 24 hours) of it being discovered? Is there an assessor or assessment team to monitor the security requirement in the system on an ongoing basis? **SP800-171 Ref: 3.12.3**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: None. <ORGANIZATION> does not have the monitoring or alerting tools for system security control modifications.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Are organizational communications controlled and monitored? – SC-7; SA-8

Control Description: ☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. **SP800-171 Ref: 3.13.1**
Control Implementation Status: ☒In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: ESO provides firewall and IDS protection services at the state network perimeter. ETS provides networking services for the data center and <ORGANIZATION> networks. All network communications are monitored, controlled and protected by ESO and ETS.

Are architectural designs, software development techniques, and systems engineering principles that promote effective information security within company information systems? – SA-8

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A Organizations should apply security engineering principles primarily to new development of information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. For COTS systems, does the vendor include system security engineering principles in the specification, design, development, and implementation of the system during the system development lifecycle? For in-house systems: Is the system managed using a system development life-cycle methodology that includes security considerations? Additional questions: Are the company's information security policies (including architectural design, software development, and system engineering principles) designed to promote information security? Are system security engineering principles applied in the specification, design, development, and implementation of the system? Statewide Information Security Standards: 8.1.1 All relevant information security requirements shall be documented and agreed upon with each supplier or vendor that may access, process, store, communicate, or provide IT services or infrastructure. **SP800-171 Ref: 3.13.2**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details:

How are user and system management functionality separated? – SC-2

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

This is different from the above question regarding "How are separation of duties managed?"

Separate user functionality from information system management functionality. Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Companies implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. Additional questions: Are physical or logical controls used to separate user functionality from system management-related functionality (e.g., to ensure that administration [e.g., privilege] options are not available to general users)? Is user functionality separated from system management functionality?

Statewide Information Security Standards:

2.1.14 Special Access Privileges: Procedures shall be established to maintain documentation of special access privileges, including high-level privileges (e.g.: root access, administrator), system utilities requiring high-level privileges, and privileges that provide access to sensitive network devices, operating systems, or software application capabilities. Procedures shall include:
2.1.14.1 Specifying and documenting the purpose and acceptable use of special access privileges;
2.1.14.2 Management approval for granting special access privileges;
2.1.14.3 Requiring different accounts or different authentication tokens than those used with the individual's regular user account;
2.1.14.4 Specifying and documenting a procedure to remove special access privileges;
2.1.14.5 Continual monitoring;

SP800-171 Ref: 3.13.3

Control Implementation Status:

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

ETS separates all 3 servers (web server (user facing application server), the LMS server, the database server) in the virtual environment. Access to database server is not directly accessible by standard users. User functionality is separated in the system level environment through RBAC's.

Are publicly accessible system components physically or logically separated from internal networks? – SC-7

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

In cybersecurity, a demilitarized zone (DMZ), sometimes referred to as a perimeter network, is a physical or logical subnetwork that contains and exposes a company's external-facing services to an untrusted network, usually a larger network such as the internet. The purpose of a DMZ is to add an additional layer of security to a company's LAN, an external network node can access only what is exposed in the DMZ, and can be intensely managed and audited, while the rest of the company's network is firewalled. Additional questions: Does the company implement DMZs? Are they adequate to meet the needs of the company? Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?

SP800-171 Ref: 3.13.5

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The <system name> web application server is not separated from other AD servers. It does not reside in a DMZ.

Does the system terminate network connections after a period of inactivity? – SC-10

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A **This is different from the above question regarding "Is the system configured to terminate sessions?"** Where AC-12 addresses website/web-based services (e.g. logging a user off from a web session after a period of inactivity), this control addresses the de-allocation of associated TCP/IP address or port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Statewide Information Security Standards: 2.1.17 Access to password-protected information systems shall be timed out after an inactivity period of 15 minutes. **SP800-171 Ref: 3.13.9**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: <System name> terminates the network connection associated with a communications session at the end of the session or after [120 minutes] of inactivity.

Is data encrypted at rest? – SC-13

Control Description: ☐System Specific ☐ Common Control ☐ Hybrid or ☒ N/A Protect the confidentiality of level 3 information or higher at rest. **SP800-171 Ref: 3.13.11**
Control Implementation Status: ☐In Place ☐Partially In Place ☐ Not in Place
Control Implementation Details: The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>. The <system name> information has been assigned Level 2 data classification by the data owner.

3.14 SYSTEM AND INFORMATION INTEGRITY

Does the organization identify, report and correct information flaws on the system in a timely manner? – SI-2; SI-3; SI-5

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Is the system kept updated as vendors/organizational developers supply patches, updates, and upgrades? Does remediation of all flaws incorporate testing prior to production?.

Identify, report, and correct information and information system flaws in a timely manner. Additional questions: Are system flaws identified, reported, and corrected within company-defined time periods? Does the company perform all security-relevant software updates (patching, service packs, hot fixes, and anti-virus signature additions) in response to identified system flaws and vulnerabilities within the timeframe specified in policy or within the system security plan? When available, do managers and administrators of the system rely on centralized management of the flaw remediation process, to include the use of automated update software, patch management tools, and automated status scanning? Is the time between flaw identification and flaw remediation measured and compared with benchmarks?

Statewide Information Security Standards:

5.9.1 All operating systems and commercial off-the-shelf/open source software shall be patched and maintained at current vendor supported levels unless there is a documented business reason for not applying a specific patch.
5.9.2 Agencies shall immediately deploy security patches to operating systems and applications upon release unless the agency follows a documented procedure for testing and deploying security patches within an identified timeframe.
5.9.3 Operating System and commercial off-the-shelf/open source software for which the vendor/open source community no longer provides security patches is considered deprecated and shall be remediated with documented controls or removed from production.
5.9.4 Wherever possible, automated patching systems shall be implemented to automatically update operating systems and applications.
5.9.5 Automated patching systems shall log which information systems have received the patches and audit for information systems that have been missed.
5.9.6 An application update management process shall be implemented to ensure the most up-to-date approved patches and application updates are installed for all software.
5.9.7 Custom developed applications shall be tested on a defined schedule for vulnerabilities and updated to correct identified vulnerabilities.
5.9.8 If no patch is available, other controls shall be implemented, such as turning off services or capabilities related to the vulnerability; adapting or adding access controls, e.g. firewalls, at network borders; increased monitoring to detect or prevent actual attacks; raising awareness of the vulnerability; keeping an audit log of all procedures undertaken; evaluating the technical vulnerability management process in order to ensure its effectiveness; and addressing high-risk information systems first.

SP800-171 Ref: 3.14.1

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

ETS is responsible for performing frequent scans using the Tenable vulnerability scanning system. Vulnerabilities and recommendations for remediation are reported to the ETS and <ORGANIZATION> teams. Additionally, ETS and <ORGANIZATION> designated individuals have logon access to the Tenable SecurityCenter application to review reported vulnerabilities on the system. ETS, working with <ORGANIZATION>, performs patch management, on a 30-day cycle, for both security and system patches. Other vulnerabilities which have patches released from the vendor, are applied according to the ETS patch management procedure.

<ORGANIZATION> is responsible for the <system name> application update process.

Does the organization employ malicious code protection mechanisms on the system as well as all devices connecting to (or transmitting data to) the system? – SI-2; SI-3; SI-5

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Provide protection from malicious code at appropriate locations within organizational information systems. Additional questions: Does the organization employ malicious code protection mechanisms (e.g. anti-virus, anti-malware, and anti-spyware) at system entry and exit points to minimize the presence of malicious code? System entry and exit points may include firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Does the system automatically update malicious code protection mechanisms?

Statewide Information Security Standards:

5.1.1 All workstations and Windows based servers shall have current antivirus/anti-malware software installed upon them.
5.1.2 All information systems with antivirus software shall undergo, at a minimum, a weekly full system scan for viruses and malware.
5.1.3 Any information system with malware shall be assessed for removal from the network, and handled in accordance with incident response procedures.
5.1.4 Portable devices shall also have antivirus protection.
5.1.5 Antivirus/anti-malware software shall be centrally managed with ongoing updates and reporting.
5.1.6 All antivirus/anti-malware signatures shall be updated and maintained at current vendor supported and recommended levels
5.1.7 Users shall not be able to disable the antivirus/anti-malware software on their workstation or portable device.

SP800-171 Ref: 3.14.2

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

Anti-virus agents and definition files are updated by ETS regularly. ETS and <ORGANIZATION>-IT will monitor and communicate anti-virus activity to ensure required services and software remain operational and up to date.

Additional questions: Are there written procedures for monitoring and communicating? Who's responsible for monitoring/communicating/troubleshooting?

Does the organization receive system alerts and advisories from the vendor or other peer or supporting organizations (e.g. US-CERT) and are the alerts and advisories disseminated and any directives implemented in accordance with established time frames? – SI-2; SI-3; SI-5

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Monitor information system security alerts and advisories and take appropriate actions in response.

SP800-171 Ref: 3.14.3

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

<ORGANIZATION> receives and monitors alerts from various organizations, including MS-ISAC, Microsoft Security Slate, and the ESO. All are used to evaluate the potential vulnerabilities and exposure to <ORGANIZATION> core applications and infrastructure.

<ORGANIZATION> will configure the web servers to forward selected events to the ESO SEIM server. If ESO identifies a threat, ESO will send alerts to <ORGANIZATION> contacts for investigation. <ORGANIZATION> will create a program to monitor selected events and alert the interim ISO for possible investigation.

Are malicious code protection mechanisms updated regularly? How often? – SI-3

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Update malicious code protection mechanisms when new releases are available.

Statewide Information Security Standards:
5.1.5 Antivirus/anti-malware software shall be centrally managed with ongoing updates and reporting.
5.1.6 All antivirus/anti-malware signatures shall be updated and maintained at current vendor supported and recommended levels

SP800-171 Ref: 3.14.4

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

ETS configures the malicious coded protection systems to receive automatic updates from their respective manufactures, which ensures the system is utilizing the latest signature files.

Are real-time and periodic scans of malicious code of the information systems performed? – SI-3

Control Description:

☐System Specific ☒ Common Control ☐ Hybrid or ☐ N/A

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. Additional questions: Does the organization perform periodic scans of the information system for malware? Are scans performed within the timeframe specified in policy or within the system security plan? Does the organization perform real-time scans of files from external sources as the files are downloaded, opened, or executed? Does the system disinfect and quarantine infected files?

Statewide Information Security Standards:
5.1.1 All workstations and Windows based servers shall have current antivirus/anti-malware software installed upon them.
5.1.2 All information systems with antivirus software shall undergo, at a minimum, a weekly full system scan for viruses and malware.
5.1.3 Any information system with malware shall be assessed for removal from the network, and handled in accordance with incident response procedures.
5.1.4 Portable devices shall also have antivirus protection.
5.1.5 Antivirus/anti-malware software shall be centrally managed with ongoing updates and reporting.
5.1.6 All antivirus/anti-malware signatures shall be updated and maintained at current vendor supported and recommended levels
5.1.7 Users shall not be able to disable the antivirus/anti-malware software on their workstation or portable device.
5.1.8 All e-mail shall be scanned at the e-mail gateway and upon arrival at the workstation. Infected e-mail messages shall be isolated and remediated.

SP800-171 Ref: 3.14.5

Control Implementation Status (select only one):

☒In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

Periodic scans of the information system are scheduled by ETS to occur regularly. All systems have anti-malware installed, which scans all files before being opened or executed. The configured behavior for the anti-virus/anti-malware program is to disinfect and quarantine infected files.

Are information systems continuously monitored? – SI-4; SI-4(4)

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. Additional questions: Does the organization monitor the information system to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections? Will the organization strategically deploy monitoring devices within the information system to collect essential information? Is the information gained from these monitoring tools protected from unauthorized access, modification, and deletion? Does the system monitor inbound and outbound communications for unusual or unauthorized activities or conditions?

Statewide Information Security Standards:

5.7.1 IDS shall be deployed to monitor network traffic to provide timely alerts and notification.
5.7.2 Intrusion detection signatures shall be updated and maintained at current vendor supported levels.
5.7.3 IDS shall perform packet and protocol analysis.
5.7.4 IDS shall perform fragmented and packet stream reassembly.
5.7.5 IDS shall detect attacks in real time.
5.7.7 Evidence and alerts of intrusion shall be handled in accordance with incident response plans and the statewide incident response policy. Incident response plan/procedure shall include response to IDS alerts.

SP800-171 Ref: 3.14.6

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

All inbound and outbound traffic at the state perimeter is monitored by the ESO to detect attacks and indicators of potential attacks, using the state perimeter firewall and IDS. Evidence and alerts are sent to <ORGANIZATION> security contacts to assess, analyze, and remediate, if necessary. <ORGANIZATION> will follow the agency incident response plan, should an event be classified as an incident.

Is unauthorized use of the information system identifiable? – SI-4

Control Description:

☐System Specific ☐ Common Control ☐ Hybrid or ☐ N/A

Identify unauthorized use of the information system. Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Additional questions: Does the company monitor the information system to identify unauthorized access and use? Does the company monitor the information for potential misuse? Is unauthorized use of the system identified (e.g., log monitoring)?

Statewide Information Security Standards:

5.7.1 IDS shall be deployed to monitor network traffic to provide timely alerts and notification.
5.7.2 Intrusion detection signatures shall be updated and maintained at current vendor supported levels.
5.7.3 IDS shall perform packet and protocol analysis.
5.7.4 IDS shall perform fragmented and packet stream reassembly.
5.7.5 IDS shall detect attacks in real time.
5.7.7 Evidence and alerts of intrusion shall be handled in accordance with incident response plans and the statewide incident response policy. Incident response plan/procedure shall include response to IDS alerts.

SP800-171 Ref: 3.14.7

Control Implementation Status (select only one):

☐In Place ☐Partially In Place ☐ Not in Place

Control Implementation Details:

The physical protection, hardware, VM, OS, installed OS roles, anti-virus, backup, and patching of the system are managed by Enterprise

Technology Services (ETS). The <system name> application and system configuration are managed by <ORGANIZATION>.

All inbound and outbound traffic at the state perimeter is monitored by the ESO to detect attacks and indicators of potential attacks, using the state perimeter firewall and IDS. Evidence and alerts are sent to <ORGANIZATION> security contacts to assess, analyze, and remediate, if necessary. <ORGANIZATION> will follow the agency incident response plan, should an event be classified as an incident.

There currently is no internal monitoring for unauthorized use of the system.

DEFINITIONS

{}

[]