Security Control Standards Catalog

Version 1.2

Texas Department of
Information Resources

April 3, 2015

Contents

About the Security Control Standards Catalog 1

Document Life Cycle 1
Revision History 2
Scope 2
Exceptions 2
Control Details and Sample Format 2
Notes on the Control Details and Sample Format 3

Security Controls Standards 5

AC–Access Control 5
AP–Authority and Purpose 22
AR–Accountability, Audit, and Risk Management 24
AT–Awareness and Training 30
AU–Audit and Accountability 33
CA–Security Assessment and Authorization 44
CM–Configuration Management 50
CP–Contingency Planning 58
DI–Data Quality and Integrity 67
DM–Data Minimization and Retention 69
IA–Identification and Authentication 72
IP–Individual Participation and Redress 80
IR–Incident Response 83
MA–Maintenance 90
MP–Media Protection 95
PE–Physical and Environmental Protection 101
PL–Planning 114
PM–Program Management 119
PS–Personnel Security 132
RA–Risk Assessment 138
SA–System and Service Acquisition 142
SC–System and Communication Protection 156
SE–Security 182
SI–System and Information Integrity 184
TR–Transparency 196
UL–Use Limitation 199

Appendix A. NIST Control Families 201

Appendix B. Acronyms and Abbreviations 212

Appendix C. Glossary of Terms 214

About the Security Control Standards Catalog

The purpose of this Security Control Standards Catalog (control catalog) is to provide state agencies and higher education institutions (subsequently referred to as *state organizations*) specific guidance for implementing security controls in a format that easily aligns with the National Institute of Standards and Technology Special Publication 800-53 Version 4 (NIST SP 800-53 Rev. 4).

The control catalog specifies the minimum information security requirements that state organizations must use to provide the appropriate levels of information security according to risk levels. The control catalog specifies the purpose, levels of risk, implementation overview, and implementation examples for each control activity. See the *Control Details and Sample Format* section for further detail.

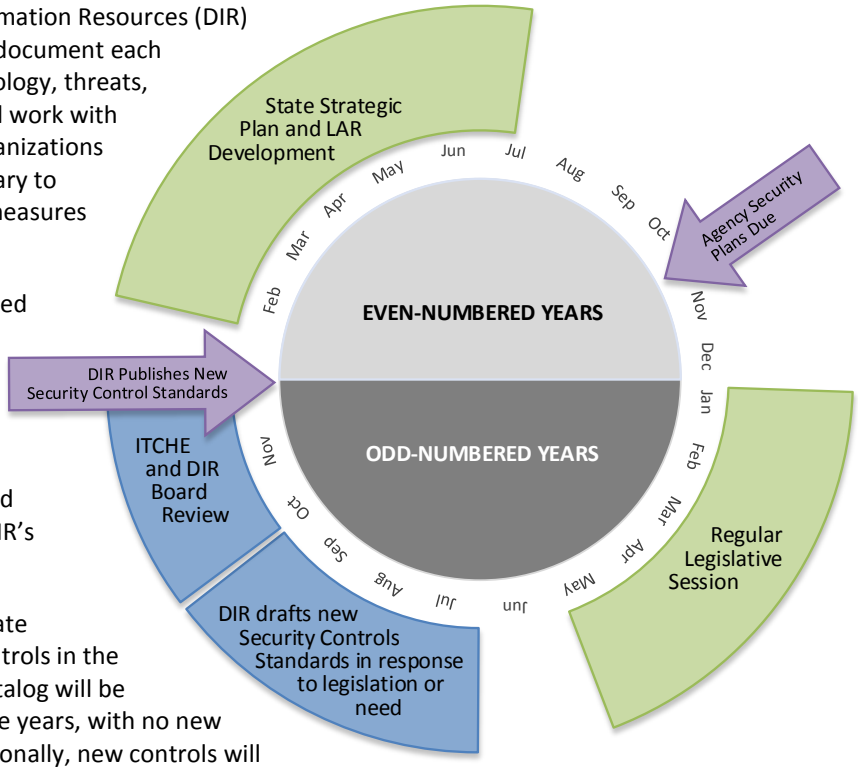
For more information related to information security requirements for state organizations, refer to Texas Administrative Code (1 TAC 202).

Document Life Cycle

The Texas Department of Information Resources (DIR) will review the controls in this document each biennium. As changes in technology, threats, and risks are identified, DIR will work with representatives from state organizations to develop the controls necessary to maintain reasonable security measures to protect state resources.

Prior to publishing new or revised standards, DIR will solicit comments on new controls from Information Resources Managers and Information Security Officers at state organizations. All recommended changes will be presented to DIR's board for approval.

To minimize their impact on state organizations, the required controls in the Security Controls Standards Catalog will be phased in over a period of three years, with no new controls in the first year. Additionally, new controls will be implemented with a "required by date not to exceed 18 months," after which, all state organizations must adhere to the new standard.



Revision History

VERSION	UPDATED BY	DATE	CHANGE DESCRIPTION
0.1	DIR Office of the Chief Information Security Officer	3/23/14	Released Draft Version 0.1
1.0	DIR Office of the Chief Information Security Officer	10/22/14	Released Draft Version 1.0
1.1	DIR Office of the Chief Information Security Officer	3/17/15	Released Final Version 1.0
1.2	DIR Office of the Chief Information Security Officer	4/3/15	Corrected date on cover; added missing legacy TAC references in Appendix A; ensured resulting pdf is fully searchable."

Scope

Below is the inventoried list of NIST controls groups that are included in this catalog. See the *Controls Details and Sample Format* section for a description of how information on each control is presented.

NIST CONTROL GROUPS/ABBREVIATIONS

AC Access Control
AP Authority and Purpose
AR Accountability, Audit, Risk Management
AT Awareness and Training
AU Audit and Accountability
CA Security Assessment and Authorization
CM Configuration Management
CP Contingency Planning
DI Data Quality and Integrity
DM Data Minimization and Retention
IA Identification and Authentication
IP Individual Participation and Redress
IR Incident Response
MA Maintenance
MP Media Protection
PE Physical and Environmental Protection
PL Planning
PM Program Management
PS Personnel Security
RA Risk Assessment
SA System and Services Acquisition
SC System and Communications Protection
SE Security
SI System and Information Integrity
TR Transparency
UL Use Limitation

Exceptions

Any exception to the following controls shall be approved, justified and documented in accordance with 1 TAC 202.21/71(c), 1 TAC 202.22/72(a.1), and 1 TAC 24/74(a6).

Control Details and Sample Format

Each control group is organized under its group identification code and title, *e.g.,* **AC – ACCESS CONTROL** ([NIST Domain Name abbreviation] – [Unabbreviated NIST control family description, e.g., *Access Control*]).

Information about each control in a group is presented in the following format.

Control ID-# Title	**[NIST 800-53 Rev. 4 Control (MOD) Control Number]-[Control Name]**

RISK STATEMENT

[A high level statement of the potential risk present by not addressing the control activity]

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

[Date which requirement will become effective. Note: Only "Low" baseline controls are mandatory for all systems. Other controls may be applicable based on the state organization risk assessment]

CONTROL DESCRIPTION

[Detailed NIST 800-53 Rev. 4 Control (MOD) control description]

IMPLEMENTATION

STATE

[State-level requirements for the implementation of information security controls]

STATE ORGANIZATION

[To be determined for each organization; to include organization-specific components as applicable, e.g., if an organization has a specific mapping requirement under the Health Insurance Portability and Accountability Act (HIPAA; or other regulatory driver) this relative control could be included here]

COMPARTMENT

[To be determined for each state organization; to include organization-specific compartment or divisional level components as applicable, e.g., if an organization's department has a specific requirement under HIPAA, as an example, this relative control could be included here]

EXAMPLE

[This section includes example only considerations of how the control identified above may be applicable in a state organization security environment]

BACK TO CONTENTS

Notes on the Control Details and Sample Format

- GROUP ID, GROUP TITLE, CONTROL ID, CONTROL TITLE
  The Group ID, Group Title, Control ID, and Control Titles are brought in directly from NIST SP 800-53, Rev 4. By maintaining this consistent mapping, state organizations can more easily map their controls to other regulatory schemes. DIR will also maintain a mapping on its website for many of the common security and regulatory systems.

- PRIORITY/BASELINE
  The PRIORITY/BASELINE is imported from NIST SP 800-53 and used for two distinct purposes. The BASELINEs are used to select which controls to implement and relate to the three impact levels—LOW, MODERATE, or HIGH—of a system. For the purposes of this version of the catalog only LOW controls will be required. When those LOW controls will be required is based on their priority.

  PRIORITY is useful for ensuring that more fundamental controls are implemented first. Controls that existed in the previous version of TAC 202 are required upon adoption by the DIR Board of the new rule and catalog. Other NIST controls that were not required under the previous TAC 202 will be prioritized for implementation over the next two years.

  There are four PRIORITY levels—P1, P2, P3, and P0—within NIST. LOW/P1 controls *not* in current TAC are required to be implemented one year after adoption by the DIR board. LOW/P2 and LOW/P3 controls *not* in current TAC 202 will be required two years after adoption by the DIR Board.

  P0 controls are not required, but are provided for consistent mapping with NIST 800-53 and to offer state organizations that choose to implement a P0 control a location to store that information.

- IMPLEMENTATION

  A REQUIRED BY date is provided for each required control. By phasing in requirements, DIR aims to minimize disruption to state organizations, while providing clear guidance on the minimums required to protect state resources.

  The catalog also provides an IMPLEMENTATION/STATE for each control that is or will be required. IMPLEMENTATION/STATE is meant to align the NIST 800-53 control with the minimum security required by the state.

  For state organizations that have stronger control requirements, either dictated by third-party regulation or required by the organizations' own risk assessment, the catalog also provides a space for the agency to specify both an IMPLEMENTATION/AGENCY and an IMPLEMENTATION/COMPARTMENT. As an example, an organization may have a specific type of data that requires a specific handling procedure. Thus, its IMPLEMENTATION/AGENCY would be more stringent than the state's minimum requirement. That same organization may also have a business unit or specific program area that also deals with a third type of data that has a specific breach notification requirement, thus that IMPLEMENTATION/COMPARTMENT would have a requirement that may not apply to the whole organization.

Security Controls Standards

AC–Access Control

AC-1 Access Control Policy and Procedures

RISK STATEMENT

Access provided is not consistent with job function as Access Control Policy is not documented, communicated, and understood.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates the current:
   1. Access control policy [Assignment: organization-defined frequency]; and
   2. Access control procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

Each state organization shall create, distribute, and implement an account management policy which defines the rules for establishing user identity, administering user accounts, and establishing and monitoring user access to information resources.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a documented, accepted written policy and procedure.

BACK TO CONTENTS

AC-2 Account Management

RISK STATEMENT

To prevent unauthorized access to information systems.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
g. Monitors the use of, information system accounts;
h. Notifies account managers:
    1. When accounts are no longer required;
    2. When users are terminated or transferred; and
    3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

IMPLEMENTATION

STATE

Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety. Information resources assigned from one state organization to another or from a state organization to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing state organization.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

The organization has:

a. Implemented role-based access to help in identifying and selecting only those accounts that enable organization mission/ business function.
b. Formulated process flow for approval of access request to information systems.
c. Defined policies and procedures for creating, modifying, disabling and removing user accounts in the system.

BACK TO CONTENTS

AC-3 Access Enforcement

RISK STATEMENT

Misconfigured access controls provide unauthorized access to information held in application systems.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization enforces approved authorizations for logical access to the system in accordance with applicable policy.

IMPLEMENTATION

STATE

1. Access to state information resources shall be appropriately managed.
2. Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

The organization has Implemented role-based access control to determine how users may have access strictly to those functions that are described in job responsibilities.

BACK TO CONTENTS

AC-4 Information Flow Enforcement

RISK STATEMENT

Users gain access to information that is beyond their appropriate level of privilege.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

IMPLEMENTATION

STATE

No statewide requirement

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization issues individual, separate user IDs between access control systems.

BACK TO CONTENTS

AC-5 Separation of Duties

RISK STATEMENT

The lack of user segregation of duties may result in unauthorized or unintentional modification or misuse of the organization's information assets.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Separates [Assignment: organization-defined duties of individuals];
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

IMPLEMENTATION

STATE

State organizations shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

a. Programmers are not the same individuals as approvers when a change is made to an application system.
b. Programming controls ensure that the person who enters a financial transaction is not the same as the person who authorizes a payment be made from that transaction.

BACK TO CONTENTS

AC-6 Least Privilege

RISK STATEMENT

Information in applications is accessed by users and other personnel outside of defined business requirements.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Only authorized users have authorized accounts to establish system accounts, configure access authorizations, filter firewall rules, manage cryptographic keys, and access control lists.

BACK TO CONTENTS

AC-7 Unsuccessful Logon Attempts

RISK STATEMENT

Unauthorized access is gained to operating systems.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The information system:

a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and
b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

IMPLEMENTATION

STATE

1. As technology permits, state organizations should enforce account lockouts after, at minimum, 10 failed attempts. This threshold may be lowered for Moderate or High risk systems.
2. Accounts locked out due to multiple incorrect logon attempts should stay locked out for a minimum of 15 minutes. Accounts for Moderate or High risk systems should remain locked until reset by an administrator.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An account is locked out of use after a predetermined number of attempts.

BACK TO CONTENTS

AC-8 System Use Notification

RISK STATEMENT

Unauthorized users log on to information systems.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The information system:

a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems:
   1. Displays system use information [Assignment: organization-defined conditions], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

IMPLEMENTATION

STATE

System Identification/Logon Banner. System identification/logon banners shall have warning statements that include the following topics:

- Unauthorized use is prohibited;
- Usage may be subject to security testing and monitoring;
- Misuse is subject to criminal prosecution; and
- Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Organizational information systems should display an accepted system use notification message or banner before granting access to the information system.

BACK TO CONTENTS

AC-9 Previous Logon (Access) Notification

RISK STATEMENT

Users are not notified when their account was used to access the resource.

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users are notified of the date, time, and IP address of their last access.

BACK TO CONTENTS

AC-10 Concurrent Session Control

RISK STATEMENT

Multiple sessions could be run under the same user account, allowing an attacker to launch a concurrent session without the user's knowledge.

PRIORITY/BASELINE

P3 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

AC-11 Session Lock

RISK STATEMENT

Unauthorized users access operating systems by physically or logically accessing valid inactive and/or unattended sessions.

PRIORITY/BASELINE

P3 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system:

a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

User sessions are locked after a period of user inactivity (e.g., 15 minutes for example).

BACK TO CONTENTS

AC-12 Session Termination

RISK STATEMENT

Inadequate session limit mechanisms may expose sensitive information or operating systems to unauthorized access.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users account are logged out have a defined period.

BACK TO CONTENTS

AC-13 Withdrawn

BACK TO CONTENTS

AC-14 Permitted Actions without Identification or Authentication

RISK STATEMENT

Systems which allow for unauthenticated access will disclose information to unauthorized parties.

PRIORITY/BASELINE

P3 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

IMPLEMENTATION

STATE

The state organization identifies, documents, and provides supporting rationale in the security plan for any actions that may be performed on an information system without identification or authentication.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Emergency IDs have only selective administrative ability.

BACK TO CONTENTS

AC-15 Withdrawn

BACK TO CONTENTS

AC-16 Security Attributes

RISK STATEMENT

When security attributes are not bound to data/information, enforcement of information security policies for access control and information flow control, either through organizational processes or information system functions or mechanisms is difficult.

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment: organization-defined security attribute values] with information in storage, in process, and/or in transmission;
b. Ensures that the security attribute associations are made and retained with the information;
c. Establishes the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined information systems]; and
d. Determines the permitted [Assignment: organization-defined values or ranges] for each of the established security attributes.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

AC-17 Remote Access

RISK STATEMENT

Users of corporate information systems expose business information to exploitable vulnerabilities when teleworking.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

IMPLEMENTATION

STATE

The state organization establishes, documents, and reviews usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed

All remote access connections must be authorizes prior to allowing such connections

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

a. Remote access is not permitted without explicit approval.
b. Access to corporate network is only provided when using VPN while working remotely

BACK TO CONTENTS

AC-18 Wireless Access

RISK STATEMENT

Unauthorized parties gain access to resources by exploiting vulnerabilities in unsecured wireless networks.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b. Authorizes wireless access to the information system prior to allowing such connections.

IMPLEMENTATION

STATE

State organizations shall establish the requirements and security restrictions for installing or providing access to the state organization information resources systems. The wireless policy shall address the following topic areas:

1. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting. Some networks should not include organizational or location information in the SSID. Additional equipment configuration recommendations are included in the Wireless Security Guidelines.

2. Types of information that may be transmitted via wireless networks and devices with or without encryption including mission critical information or sensitive personal information.

State organizations shall not transmit confidential information via a wireless connection to, or from a portable computing device unless encryption methods, such as a Virtual Private Network (VPN), Wi-Fi Protected Access, or other secure encryption protocols that meet appropriate protection or certification standards, are used to protect the information.

3. Prohibit and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state organizational IT systems by individuals without the approval of the state organization information resources manager.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Wireless access (guest or local) is locked with a password mechanism.

BACK TO CONTENTS

AC-19 Access Control for Mobile Devices

RISK STATEMENT

Mobile computing and teleworking expose systems and information to exploitable vulnerabilities.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems.

IMPLEMENTATION

STATE

State organizations shall establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, whether owned by the state organization or the employee.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Mobile devices are password restricted.

BACK TO CONTENTS

AC-20 Use of External Information Systems

RISK STATEMENT

The security of the organizations information processing facilities is compromised by external parties.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from external information systems; and
b. Process, store, or transmit organization-controlled information using external information systems.

IMPLEMENTATION

STATE

1. State organizations shall develop policies governing the use of external information systems and resources including the type and classification of data that can be stored outside of the state organization.
2. State organizations shall establish terms and conditions for contracting with external information resources providers.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

External information systems are not permitted to the internal network without appropriate monitoring and/or approval.

BACK TO CONTENTS

AC-21 Information Sharing

RISK STATEMENT

Processes which do not restrict access to information, information processing systems or applications and sensitive business processes based on a need to know basis, may result in accidental or deliberate misuse of access privileges.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for

[Assignment: organization-defined information sharing circumstances where user discretion is required]; and

b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

User login credentials are provided based on job responsibilities and periodically reviewed for appropriateness.

BACK TO CONTENTS

AC-22 Publicly Accessible Content

RISK STATEMENT

Laws and regulations are violated due to inappropriate disclosure of personal information.

PRIORITY/BASELINE

P3 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.

IMPLEMENTATION

STATE

State organizations shall develop policies governing the procedures to post information on publicly accessible information systems.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Only select state organization personnel have access to publicly post content.

BACK TO CONTENTS

AC-23 Data Mining Protection

RISK STATEMENT

Confidential data could be exposed to unauthorized viewers.

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to adequately detect and protect against data mining.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization issues individual, separate user IDs between access control systems.

BACK TO CONTENTS

AC-24 Access Control Decisions

RISK STATEMENT

Users gain access to information that is beyond their appropriate level of privilege.

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization establishes procedures to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization issues individual, separate user IDs between access control systems.

BACK TO CONTENTS

AC-25 Reference Monitor

RISK STATEMENT

The access controls of subjects with certain privileges (i.e., access permissions) are not restricted from being passed to any other subjects, either directly or indirectly.

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system implements a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization issues individual, separate user IDs between access control systems.

BACK TO CONTENTS

AP–Authority and Purpose

AP-1 Authority to Collect

RISK STATEMENT

Laws and regulations are violated due to inappropriate collection of personal information.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Legal authority is explicitly defined.

BACK TO CONTENTS

AP-2 Purpose Specification

RISK STATEMENT

Laws and regulations are violated due to an organization failing to provide notices on usage of customer data.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION
[To be determined]
COMPARTMENT
[To be determined]

EXAMPLE

Data classification (sensitive, non-sensitive, etc.) is conducted and the location or repositories of such is clearly defined.

BACK TO CONTENTS

AR–Accountability, Audit, and Risk Management

AR-1 Governance and Privacy Program

RISK STATEMENT

Lack of a privacy program may result in the compromise of sensitive information due to loss of integrity or confidentiality.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;
b. Monitors federal privacy laws and policy for changes that affect the privacy program;
c. Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program;
d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
f. Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A privacy officer is assigned and/or designated for the organization.

BACK TO CONTENTS

AR-2 Privacy Impact and Risk Assessment

RISK STATEMENT

Laws and regulations are violated as a result of customers' data being modified.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Privacy impact assessment methodology and programs are defined for the organization.

BACK TO CONTENTS

AR-3 Privacy Requirements for Contractors and Service Providers

RISK STATEMENT

Customer information is improperly disclosed when transmitted to a third party.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and
b. Includes privacy requirements in contracts and other acquisition-related documents.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Service providers are subject to agency privacy requirements and held accountable for such.

BACK TO CONTENTS

AR-4 Privacy Monitoring and Auditing

RISK STATEMENT

Critical business processes and sensitive data are compromised due to a flawed monitoring and inspection process.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Privacy controls are subject to periodic review and inspection by a neutral internal department or other.

BACK TO CONTENTS

AR-5 Privacy Awareness and Training

RISK STATEMENT

Employees, contractors or third party users breach privacy because they are not aware or trained on information privacy requirements.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;
b. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and
c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Employees and other agency personnel received periodic information security training.

BACK TO CONTENTS

AR-6 Privacy Reporting

RISK STATEMENT

Privacy laws and regulations cannot be enforced due to ill-defined policy.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Reporting mechanism and responsibilities to regulatory bodies are defined.

BACK TO CONTENTS

AR-7 Privacy-Enhanced System Design and Development

RISK STATEMENT

Laws and regulations are violated as a result of poor integration of privacy controls into system design and development.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization designs information systems to support privacy by automating privacy controls.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Privacy controls are made automated, where possible.

BACK TO CONTENTS

AR-8 Accounting of Disclosures

RISK STATEMENT

Laws and regulations are violated as a result of inaccurate accounting practices of disclosures of information.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
   (1) Date, nature, and purpose of each disclosure of a record; and
   (2) Name and address of the person or agency to which the disclosure was made;

b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and
c. Makes the accounting of disclosures available to the person named in the record upon request.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Potential records are maintained, and a custodian of these records is identified.

BACK TO CONTENTS

AT–Awareness and Training

AT-1 Security Awareness and Training Policy and Procedures

RISK STATEMENT

Applications and technology alternatives are not effectively and efficiently used since a training curriculum for employees has not been established or regularly updated.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
   1. Security awareness and training policy [Assignment: organization-defined frequency]; and
   2. Security awareness and training procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

State organizations shall establish the requirements to ensure each user of information resources receives adequate training on computer security issues

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has written and documented policy and procedure supporting a training and awareness program.

BACK TO CONTENTS

AT-2 Security Awareness Training

RISK STATEMENT

Employees, contractors or third party users breach security because they are not aware or trained on information security requirements.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;
b. When required by information system changes; and
c. [Assignment: organization-defined frequency] thereafter.

IMPLEMENTATION

STATE

State organizations shall:

- Provide an ongoing information security awareness education program for all users.
- Use new employee orientation to introduce information security awareness and inform new employees of information security policies and procedures.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

a. The organization has established a security training program to improve the awareness of the impact that a security breach can have on the organization as well as the individual users, employees, contractors and third parties.
b. The organization uses security awareness techniques such as displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

BACK TO CONTENTS

AT-3 Role-Based Security Training

RISK STATEMENT

Failure to conduct suitable and relevant security training and to publish notifications to enhance awareness of organizational policies and procedures may expose the operational environment to potential security breach by employees, contractors and third parties.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. [Assignment: organization-defined frequency] thereafter.

IMPLEMENTATION

STATE

State organizations shall provide role-based information security training to staff with information security responsibilities.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Employees are trained in information security based on their role and job responsibilities.

BACK TO CONTENTS

AT-4 Security Training Records

RISK STATEMENT

Service Management objectives are not achieved since personnel performing work within service management have inappropriate education, training, skills, and experience.

PRIORITY/BASELINE

P3 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
b. Retains individual training records for [Assignment: organization-defined time period].

IMPLEMENTATION

STATE

State organizations shall maintain information security awareness and training records

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization maintains records of information security training and monitored them for compliance.

BACK TO CONTENTS

AT-5 Withdrawn

BACK TO CONTENTS

AU–Audit and Accountability

AU-1 Audit and Accountability Policy and Procedures

RISK STATEMENT

Critical business processes and sensitive data are compromised due to flawed inspection process.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
b. Reviews and updates the current:
   1. Audit and accountability policy [Assignment: organization-defined frequency]; and
   2. Audit and accountability procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization develops, disseminates, and periodically reviews/updates formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has written and documented audit and accountability procedures in place.

BACK TO CONTENTS

AU-2 Audit Events

RISK STATEMENT

Unauthorized access and activity is undetected due to incomplete log information.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

IMPLEMENTATION

STATE

Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information.

Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules.

Based on the risk assessment, a sufficiently complete history of transactions shall be maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization monitors the use of information systems, maintains security related system logs, and retains logs in accordance with the organization's records retention schedules.

BACK TO CONTENTS

AU-3 Content of Audit Records

RISK STATEMENT

The lack of logging mechanisms to record and store user activities, exceptions, and information security events may result in unauthorized access or activity going undetected.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

IMPLEMENTATION

STATE

Audit record content includes, for most audit records:

- date and time of the event;
- the component of the information system (e.g., software component, hardware component) where the event occurred;
- type of event;
- user/subject identity; and
- the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization utilizes logging mechanisms, including the generation of audit reporting records.

BACK TO CONTENTS

AU-4 Audit Storage Capacity

RISK STATEMENT

Logging facilities and log information is compromised due to inadequate capacity to maintain necessary logs.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

IMPLEMENTATION

STATE

The state organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Data storage space is available to accommodate audit records.

BACK TO CONTENTS

AU-5 Response to Audit Processing Failures

RISK STATEMENT

Unauthorized system activities are undetected because of inconsistent log monitoring.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system:

a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and
b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

IMPLEMENTATION

STATE

The information system alerts appropriate organizational officials in the event of an audit processing failure

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Automated alerts are generated and provided to state organization personnel in the event of an audit failure.

BACK TO CONTENTS

AU-6 Audit Review, Analysis, and Reporting

RISK STATEMENT

Audit findings are not effectively communicated or resolved by management.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
b. Reports findings to [Assignment: organization-defined personnel or roles].

IMPLEMENTATION

STATE

The state organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A reporting structure is defined and records are periodically promoted to specific management personnel for review, as applicable.

BACK TO CONTENTS

AU-7 Audit Reduction and Report Generation

RISK STATEMENT

Information security events are not reported.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system provides an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Audit records cannot be altered by administrators.

BACK TO CONTENTS

AU-8 Time Stamps

RISK STATEMENT

The lack of operational control to synchronize system clocks with an authoritative time source may hinder the ability to monitor timestamps from logs which could affect the incident response process.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system:

a. Uses internal system clocks to generate time stamps for audit records; and
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

IMPLEMENTATION

STATE

Whenever technically possible, information systems should provide time stamps for use in audit record generation.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The internal clock of an application system is active, which synchs to a global time reporting system.

BACK TO CONTENTS

AU-9 Protection of Audit Information

RISK STATEMENT

Failure to restrict access to logging facilities and log information may result in unauthorized access, log information tampering and loss of user activity evidence.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

IMPLEMENTATION

STATE

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Logging mechanisms and tools are not available to general users for modification.

BACK TO CONTENTS

AU-10 Non-Repudiation

RISK STATEMENT

Individuals can falsely deny having performed actions on information systems.

PRIORITY/BASELINE

P2 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

AU-11 Audit Record Retention

RISK STATEMENT

Laws and regulations are violated due to data not being retained for the required duration of time or inappropriate data being stored.

PRIORITY/BASELINE

P3 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

IMPLEMENTATION

STATE

The state organization retains audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Data retention policies and procedures define the pre-determined period of time that records are maintained.

BACK TO CONTENTS

AU-12 Audit Generation

RISK STATEMENT

Failure to plan and execute IT logging activities may result in potential compromise of critical business processes and sensitive data to go undetected.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system:

a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];
b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and
c. Generates audit records for the events defined in AU-2 with the content defined in AU-3.

IMPLEMENTATION

STATE

State organizations shall configure information systems to generate audit records to support AU-2 and AU-3

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization defines auditable events per application/operating system.

BACK TO CONTENTS

AU-13 Monitoring and Information Disclosure

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization monitors [Assignment: organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization monitors public sources for evidence of unauthorized disclosure of organizational information.

BACK TO CONTENTS

AU-14 Session Audit

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

AU-15 Alternate Audit Capability

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [Assignment: organization-defined alternate audit functionality].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

AU-16 Cross-organizational Auditing

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

CA–Security Assessment and Authorization

CA-1 Security Assessment and Authorization Policy and Procedures

RISK STATEMENT

Management does not set a clear policy direction in line with business objectives and demonstrate a commitment to information security.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Reviews and updates the current:
   1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and
   2. Security assessment and authorization procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization shall establish a security assessment procedure.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has published a policy setting information security expectations for communicating to faculty, staff, business, IT, and other users.

BACK TO CONTENTS

CA-2 Security Assessments

RISK STATEMENT

Objective reviews of information security are not regularly performed to determine the continuing suitability, capability, and effectiveness of the organization's information security program.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
c. Produces a security assessment report that documents the results of the assessment; and
d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].

IMPLEMENTATION

STATE

A review of the state organization's information security program for compliance with these standards will be performed at least annually, based on business risk management decisions, by individual(s) independent of the information security program and designated by the state organization head or his or her designated representative(s).

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a defined information security program that includes:

a. Developing a plan and executing periodic assessments of security control effectiveness;
b. Identifying objective and qualified assessors; and
c. Reporting results of such assessment(s) to the appropriate stakeholders.

BACK TO CONTENTS

CA-3 System Interconnections

RISK STATEMENT

Security breaches occur due to risks related to external parties not being identified and controlled.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The organization authorizes all connections from internal/organization information system to other information systems outside of organization through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Interconnections to application systems are defined; a dataflow of information is available.

BACK TO CONTENTS

CA-4 Withdrawn

BACK TO CONTENTS

CA-5 Plan of Action and Milestones

RISK STATEMENT

Identified risks are not accepted, mitigated or responded to with actionable plans and decisions.

PRIORITY/BASELINE

P3 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

IMPLEMENTATION

STATE

The state organization develops and updates, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An organization tracks and reports on control deficiencies through a defined plan of action and milestone document.

BACK TO CONTENTS

CA-6 Security Authorization

RISK STATEMENT

Responsibility for the IT program has not been defined.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization authorizes the information system for processing before operations or when there is a significant change to the system.

A senior organizational official signs and approves the security accreditation.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Each application system has a defined authorizing official.

BACK TO CONTENTS

CA-7 Continuous Monitoring

RISK STATEMENT

Known violations of security policy are not properly mitigated due to ineffective compliance and/or self-assessment activities.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [Assignment: organization-defined metrics] to be monitored;
b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization monitors the security controls in the information system on an ongoing basis.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A continuous monitoring strategy such as automated and other periodic manual checkpoints is defined.

BACK TO CONTENTS

CA-8 Penetration Testing

RISK STATEMENT

Vulnerabilities will not be validated or confirmed. The organization will be unable to assess their ability to withstand an attack directed at their information resources.

PRIORITY/BASELINE

P2 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Internal interfaces between application systems are accepted for usage.

BACK TO CONTENTS

CA-9 Internal System Connections

RISK STATEMENT

Failure to establish formal authorization processes for restricting user access to internal system connections may result in unauthorized or unsecure connections to the network exposing sensitive or critical business applications.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and
b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

IMPLEMENTATION

STATE

The state organization has a procedure for authorizing internal information resource connections.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a process for accepting internal interfaces between application systems.

BACK TO CONTENTS

CM–Configuration Management

CM-1 Configuration Management Policy and Procedures

RISK STATEMENT

The change management process in place does not adequately protect the environment from disruptive changes in production.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
b. Reviews and updates the current:
   1. Configuration management policy [Assignment: organization-defined frequency]; and
   2. Configuration management procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The organization establishes the process for controlling modifications to hardware, software, firmware, and documentation to ensure the information resources are protected against improper modification before, during, and after system implementation

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has written, documented configuration management policies and procedures in place

BACK TO CONTENTS

CM-2 Baseline Configuration

RISK STATEMENT

Changes to systems and applications are executed inconsistently in the production environment due to ill-defined procedures.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

IMPLEMENTATION

STATE

The state organization develops, documents, and maintains a current baseline configuration of the information system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization uses configuration policies and procedure to manage the change lifecycle.

BACK TO CONTENTS

CM-3 Configuration Change Control

RISK STATEMENT

Changes to the production environment that are inadequately tested disrupt production environment. Management does not accept changes to the operating environment prior to implementation into production.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

IMPLEMENTATION

STATE

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Configuration changes are accepted prior to implementation.

BACK TO CONTENTS

CM-4 Security Impact Analysis

RISK STATEMENT

Effects from changes to systems or applications are undetected in the production environment.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

IMPLEMENTATION

STATE

- All security-related information resources changes shall be approved by the information owner through a change control process.
- Approval shall occur prior to implementation by the state organization or independent contractors

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization considers and documents consideration of the potential impact to information security prior to the completion of a change.

BACK TO CONTENTS

CM-5 Access Restrictions for Change

RISK STATEMENT

Operations handle emergency situations that require a change to the production environment consistently.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

IMPLEMENTATION

STATE

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Access control restrictions for the purposes of change are defined.

BACK TO CONTENTS

CM-6 Configuration Settings

RISK STATEMENT

Changes to the production environment are not operating as expected disrupt the production environment.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

IMPLEMENTATION

STATE

The state organization:

- establishes mandatory configuration settings for information technology products employed within the information system;
- configures the security settings of information technology products to the most restrictive mode consistent with operational requirements;
- documents the configuration settings; and
- enforces the configuration settings in all components of the information system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization maintains a baseline of configuration settings.

BACK TO CONTENTS

CM-7 Least Functionality

RISK STATEMENT

Configuration standards do not exist for systems being implemented.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

IMPLEMENTATION

STATE

The state organization configures information system to provide only essential capabilities.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization applies the concept of least privilege when providing access to application systems.

BACK TO CONTENTS

CM-8 Information System Component Inventory

RISK STATEMENT

Information and assets associated with information processing facilities are not owned by a designated part of the organization.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

The organization has a defined information security program that includes:

a. developing a plan and executing periodic assessments of security control effectiveness;
b. identifying objective and qualified assessors; and
c. reporting results of such assessment(s) to the appropriate stakeholders.

BACK TO CONTENTS

CM-9 Configuration Management Plan

RISK STATEMENT

IT assets and configurations are managed ineffectively due to the lack of a configuration management process.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Written, document configuration plan is available relevant to application systems.

BACK TO CONTENTS

CM-10 Software Usage Restrictions

RISK STATEMENT

Improper use of information or assets occurs inside an information processing facility.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

IMPLEMENTATION

STATE

The state organization:

- uses software and associated documentation in accordance with contract agreements and copyright laws;
- tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
- controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization utilizes periodic monitoring sweeps to catch inappropriate peer-to-peer file sharing.

BACK TO CONTENTS

CM-11 User-Installed Software

RISK STATEMENT

Users expose information systems by not correctly executing their access control responsibilities.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Establishes [Assignment: organization-defined policies] governing the installation of software by users;
b. Enforces software installation policies through [Assignment: organization-defined methods]; and
c. Monitors policy compliance at [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization establishes and enforces a policy governing the installation of software by users.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Unauthorized software installation is either not allowed, or limited based on access privileges.

BACK TO CONTENTS

CP–Contingency Planning

CP-1 Contingency Planning Policy and Procedures

RISK STATEMENT

The Continuity of Operations Program is ineffective since the COOP documentation has not been created and maintained.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and updates the current:
   1. Contingency planning policy [Assignment: organization-defined frequency]; and
   2. Contingency planning procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

State organizations shall maintain written Continuity of Operations Plans that address information resources so that the effects of a disaster will be minimized, and the state organization will be able either to maintain or quickly resume mission-critical functions.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Written, documented COOP documentation is in place.

BACK TO CONTENTS

CP-2 Contingency Plan

RISK STATEMENT

Critical activities are not recovered rapidly at the time of a disruption since the organization has not categorized its activities according to their priority for recovery.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops a contingency plan for the information system that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
g. Protects the contingency plan from unauthorized disclosure and modification.

IMPLEMENTATION

STATE

The plan shall be distributed to key personnel and a copy stored offsite. Elements of the plan for information resources shall include:

a. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis shall identify the following elements:
   1. Mission-Critical Information Resources (specific system resources required to perform critical functions) to include:
      A. Internal and external points of contact for personnel that provide or receive data or support interconnected systems.
      B. Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.
   2. Disruption impacts and allowable outage times to include:
      A. Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.
      B. Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.
   3. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:
      A. Preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms.
      B. Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.
b. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.
c. Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan.
d. Disaster Recovery Plan--Each state organization shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:

1. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;
2. Identify recovery resources and a source for each;
3. Contain step-by-step implementation instructions;
4. Include provisions for annual testing.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A written, documented, accepted contingency plan is in place.

BACK TO CONTENTS

CP-3 Contingency Training

RISK STATEMENT

An organization is unable to resume its activities following a disruption since it has not considered strategic options for its critical activities and the resources that each activity will require on its resumption.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. [Assignment: organization-defined frequency] thereafter.

IMPLEMENTATION

STATE

The state organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides periodic refresher training.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization trains applicable personnel for contingency roles and responsibilities.

BACK TO CONTENTS

CP-4 Contingency Plan Testing

RISK STATEMENT

Disaster recovery plans fail because they were not tested, maintained or re-assessed.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

IMPLEMENTATION

STATE

Each state organization's written disaster recovery plan will include provisions for annual testing.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

The organization:

a. Tests, reassesses and maintains the disaster recovery plans regularly to determine that they are up to date and effective.
b. Conducts regular sessions analyze the disaster recovery plan's test results for further upgrades.

BACK TO CONTENTS

CP-5 Withdrawn

BACK TO CONTENTS

CP-6 Alternate Storage Site

RISK STATEMENT

The organization has not devised Information strategies which determine that information vital to the organization's operation is adequately protected and recoverable at the time needed.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

IMPLEMENTATION

STATE

Mission-critical information shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized state organization representatives.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

a. The organization has established procedures to perform and maintain backup copies of information in accordance with organization's business continuity and disaster recovery requirements.
b. The organization stores media back-ups in a secure location, preferably at an off-site facility, such as an alternate or back-up site, or a commercial storage facility.

BACK TO CONTENTS

CP-7 Alternate Processing Site

RISK STATEMENT

An organization is unable to recover its technology services since it has not devised a technology strategy according to its size, nature and complexity of business.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An offsite, alternative processing site is available. The alternative site should not be subject to the same natural disasters of the primary site (i.e. not in proximity).

BACK TO CONTENTS

CP-8 Telecommunications Services

RISK STATEMENT

The agreed service continuity and availability commitment to customers are not met in specific circumstances.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An offsite, alternative telecommunication site is available. The alternative site should not be subject to the same natural disasters of the primary site (i.e. not in proximity.

BACK TO CONTENTS

CP-9 Information System Backup

RISK STATEMENT

Data is not recoverable due to inadequate or undefined backup and restoration procedures.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

IMPLEMENTATION

STATE

The state organization conducts backups of system-level information (including system state information) and critical user-level information contained in the information system and protects backup information at the storage location.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization performs periodic, regular data backups of application sensitive/critical information.

BACK TO CONTENTS

CP-10 Information System Recovery and Reconstitution

RISK STATEMENT

Information systems fail due to improper fault tolerant or redundant architectures.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

IMPLEMENTATION

STATE

The state organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has redundant processing mechanisms available in the event of natural disaster.

BACK TO CONTENTS

CP-11 Alternate Communications Protocols

RISK STATEMENT

Resiliency will be reduced if a single protocol is relied on during an business interruption

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system provides the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.

IMPLEMENTATION

STATE

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Switching from Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4 to TCP/IP Version 6

BACK TO CONTENTS

CP-12 Safe Mode

RISK STATEMENT

Systems may be overloaded if unnecessary functionality is allowed during emergencies

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system, when [Assignment: organization-defined conditions] are detected, enters a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].

IMPLEMENTATION

STATE

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Allowing only certain functions that could be carried out under limited power or with reduced communications bandwidth

BACK TO CONTENTS

CP-13 Alternative Security Mechanisms

RISK STATEMENT

Mission critical systems may be unavailable, if the primary security mechanisms fail.

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.

IMPLEMENTATION

STATE

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An organization may issue to senior executives and system administrators one-time pads in case multifactor tokens, the organization's standard means for secure remote authentication, is compromised

BACK TO CONTENTS

DI–Data Quality and Integrity

DI-1 Data Quality

RISK STATEMENT

Security exploits and errors exist in systems that are implemented due to a lack of information security practices.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;
b. Collects PII directly from the individual to the greatest extent practicable;
c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and
d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

PII data is automatically sourced for information security repositories, and if not is analyzed for appropriateness as applicable.

BACK TO CONTENTS

DI-2 Data Integrity and Data Integrity Board

RISK STATEMENT

Laws and regulations are violated as a result of customers' data being modified.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and
b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A committee is in place (legal) to disseminate and discern the computer matching agreements.

BACK TO CONTENTS

DM–Data Minimization and Retention

DM-1 Minimization of Personally Identifiable Information

RISK STATEMENT

Laws and regulations are violated as a result of lack of controls over collection of personally identifiable information (PII).

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A privacy impact assessment determines the extent and nature of PII in the organization, and appropriate handling mechanisms are defined.

BACK TO CONTENTS

DM-2 Data Retention and Disposal

RISK STATEMENT

Laws and regulations are violated due to data not being retained for the required duration of time or inappropriate data being stored.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law;
b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
c. Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A privacy impact assessment determines the extent and nature of PII in the organization, and appropriate handling mechanisms are defined.

BACK TO CONTENTS

DM-3 Minimization of PII Used In Testing, Training, And Research

RISK STATEMENT

Laws and regulations are violated as a result of lack of controls over use of personally identifiable information (PII) in testing, training and research.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:
a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and
b. Implements controls to protect PII used for testing, training, and research.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A privacy impact assessment determines the extent and nature of PII in the organization, and appropriate handling mechanisms are defined.

BACK TO CONTENTS

IA–Identification and Authentication

IA-1 Identification and Authentication Policy and Procedures

RISK STATEMENT

The lack of acceptable policies and procedures to control access to information resources may expose the information to unauthorized access.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
b. Reviews and updates the current:
   1. Identification and authentication policy [Assignment: organization-defined frequency]; and
   2. Identification and authentication procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization establishes the policies for verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in an information system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has written, documented identification and authentication policies and procedures are in place.

BACK TO CONTENTS

IA-2 Identification and Authentication (Organizational Users)

RISK STATEMENT

Failure to assign individual user identification and a relevant authentication mechanism to confirm the claimed identity of a user may result in potential fraud and/or falsification of user identities.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

IMPLEMENTATION

STATE

Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users have individual identification and login credentials.

BACK TO CONTENTS

IA-3 Device Identification and Authentication

RISK STATEMENT

Unidentified equipment is allowed to gain access to the network.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users' equipment is uniquely identified prior to login.

BACK TO CONTENTS

IA-4 Identifier Management

RISK STATEMENT

Unauthorized users are able to gain access to information systems by claiming to be an authorized user.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization manages information system identifiers by:

a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and
e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].

IMPLEMENTATION

STATE

A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the state organization change.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

The organization manages information system identifiers for users and devices by receiving authorization from a designated official to assign an individual user identifier (user-id), preventing reuse of user-ids, and disabling user-ids to information resources and data under their authority.

BACK TO CONTENTS

IA-5 Authenticator Management

RISK STATEMENT

Unauthorized users gain access through user accounts based on a password that was disclosed during communication to the authorized users.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

IMPLEMENTATION

STATE

The state organization manages information system authenticators by:

- defining initial authenticator content;
- establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and
- changing default authenticators upon information system installation.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Password, token, biometric, etc. is utilized for access to information systems.

BACK TO CONTENTS

IA-6 Authenticator Feedback

RISK STATEMENT

Lack of controls to obscure feedback of authentication information may expose the authentication information to possible exploitation.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IMPLEMENTATION

STATE

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

a. Passwords are masked upon keyed entry.
b. Failed login boxes do not indicate which part of the username/password combination is incorrect

BACK TO CONTENTS

IA-7 Cryptographic Module Authentication

RISK STATEMENT

Laws and regulations are inadvertently violated due to illegal use of cryptographic controls.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

IMPLEMENTATION

STATE

Encryption used by the state organization meets the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Encryption mechanisms used on information systems that must comply with federal standards use FIPS 140-2 approved algorithms.

BACK TO CONTENTS

IA-8 Identification and Authentication (Non-Organizational Users)

RISK STATEMENT

Unauthenticated and/or unauthorized users access networks by exploiting vulnerabilities in external connections.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

IMPLEMENTATION

STATE

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Non-organizational users (guests) are subject to authorization to information systems prior to access.

BACK TO CONTENTS

IA-9 Service Identification and Authentication

RISK STATEMENT

Information systems are not able to determine in a dynamic manner, if external providers and associated services are authentic

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization identifies and authenticates [Assignment: organization-defined information system services] using [Assignment: organization-defined security safeguards].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.

BACK TO CONTENTS

IA-10 Adaptive Identification and Authentication

RISK STATEMENT

Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users.

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

IA-11 Re-authentication

RISK STATEMENT

Authentication may become stale, allowing a no longer authenticated user access

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT
[To be determined]

EXAMPLE

Organization may require re-authentication of individuals and/or devices:

a. when authenticators change;
b. when roles change;
c. when security categories of information systems change;
d. when the execution of privileged functions occurs;
e . after a fixed period of time; or
f. periodically.

BACK TO CONTENTS

IP–Individual Participation and Redress

IP-1 Consent

RISK STATEMENT

Laws and regulations are violated as a result of individuals not having the ability to choose how their personal information is to be used.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;
b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users sign-off on acceptable usage guidelines for PII.

BACK TO CONTENTS

IP-2 Individual Access

RISK STATEMENT

Laws and regulations are violated as a result of individuals not having the ability to access their personal information as stored by the company.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;
b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
c. Publishes access procedures in System of Records Notices (SORNs); and
d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users signoff on acceptable usage guidelines for PII, and have access to relevant information

BACK TO CONTENTS

IP-3 Redress

RISK STATEMENT

Violations to privacy laws, and regulations cannot be enforced due to ill-defined policy.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and
b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users may access applicable information through the concept of least privilege.

BACK TO CONTENTS

IP-4 Complaint Management

RISK STATEMENT

The extent of a security breach of personal information and possible damage(s) may not be identified.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An anonymous incident “hot-line” or similar should be available to employees for complaints, questions, and concerns.

BACK TO CONTENTS

IR–Incident Response

IR-1 Incident Response Policy and Procedures

RISK STATEMENT

Information security incidents are not responded to in a quick, effective and orderly manner.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
b. Reviews and updates the current:
   1. Incident response policy [Assignment: organization-defined frequency]; and
   2. Incident response procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

State organizations shall assess the significance of a security incident based on the business impact on the affected resources and the current and potential technical effect of the incident, e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has documented policies and procedures and trained personnel to identify, prioritize, report, and resolve information security incidents as required by federal and state rules.

BACK TO CONTENTS

IR-2 Incident Response Training

RISK STATEMENT

Failure to train personnel on the incident response roles and responsibilities may result in inadequately coordinated processes in response to a security incident.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. [Assignment: organization-defined frequency] thereafter.

IMPLEMENTATION

STATE

The state organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization provides training to employees relevant to how to handle an information security incident.

BACK TO CONTENTS

IR-3 Incident Response Testing

RISK STATEMENT

Incidents are mishandled due to lack of defined and tested incident management plans.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The agency conducted periodic testing of the incident reporting mechanisms.

BACK TO CONTENTS

IR-4 Incident Handling

RISK STATEMENT

Security incidents continue to occur due to lack of learning from past security incidents.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IMPLEMENTATION

STATE

The state organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The incident management process evolves based on testing, usage, and feedback.

BACK TO CONTENTS

IR-5 Incident Monitoring

RISK STATEMENT

Rules for evidence handling are not followed by when evidence is collected, retained, or presented.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization tracks and documents information system security incidents.

IMPLEMENTATION

STATE

The state organization tracks and documents information system security incidents on an ongoing basis.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization utilizes an automated mechanism to record and track information security incidents.

BACK TO CONTENTS

IR-6 Incident Reporting

RISK STATEMENT

Security events and weaknesses are not detected and corrected due to lack of users reporting the events or weaknesses.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and
b. Reports security incident information to [Assignment: organization-defined authorities].

IMPLEMENTATION

STATE

a. Security incidents shall be promptly reported to immediate supervisors and the state organization Information Security Officer. Security incidents that require timely reporting to the department include those events that are assessed to:
   1. Propagate to other state systems;
   2. Result in criminal violations that shall be reported to law enforcement; or
   3. Involve the unauthorized disclosure or modification of confidential information, e.g., sensitive personal information as defined in §521.002(a)(2), Business and Commerce Code, and other applicable laws that may require public notification.
b. If the security incident is assessed to involve suspected criminal activity (e.g., violations of Chapters 33, Penal Code (Computer Crimes) or Chapter 33A, Penal Code (Telecommunications Crimes)), the security incident shall be investigated, reported, and documented in a manner that restores operation promptly while meeting the legal requirements for handling of evidence.
c. Depending on the criticality of the incident, it will not always be feasible to gather all the information prior to reporting. In such cases, incident response teams should continue to report information to the department as it is collected. The department shall instruct state organizations as to the manner in which they shall report such information to the department. Supporting vendors or other third parties that report security incident information to a state organization shall submit such reports to the state organization in the form and manner specified by the department, unless otherwise directed by the state organization.
d. Summary reports of security-related events shall be sent to the department on a monthly basis no later than nine (9) calendar days after the end of the month. Organizations shall submit summary security incident reports in the form and manner specified by the department. Supporting vendors or other third parties that report security incident information to a state organization shall submit such reports to the state organization in the form and manner specified by the department, unless otherwise directed by the state organization.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a defined hierarchy for reporting security incidents.

BACK TO CONTENTS

IR-7 Incident Response Assistance

RISK STATEMENT

Lack of a Security Incident Response Program may result in improper identification and handling of security events.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

IMPLEMENTATION

STATE

The state organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has defined a resource and a back-up resource to provide guidance for the incident management response process.

BACK TO CONTENTS

IR-8 Incident Response Plan

RISK STATEMENT

The organization is unable to manage the initial phase of an incident since the plan is not well designed and documented.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops an incident response plan that:
   1. provides the organization with a roadmap for implementing its incident response capability;
   2. describes the structure and organization of the incident response capability;
   3. provides a high-level approach for how the incident response capability fits into the overall organization;
   4. meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. defines reportable incidents;
   6. provides metrics for measuring the incident response capability within the organization;
   7. defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8. is reviewed and approved by [Assignment: organization-defined personnel or roles];
b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];
c. Reviews the incident response plan [Assignment: organization-defined frequency];
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and
f. Protects the incident response plan from unauthorized disclosure and modification.

IMPLEMENTATION

STATE

The state organization has an incident management policy that describes the requirements for dealing with computer security incidents including prevention, detection, response, remediation, and reporting

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a written, document incident response plan in place.

BACK TO CONTENTS

IR-9 Information Spillage Response

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;
b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;
c. Isolating the contaminated information system or system component;
d. Eradicating the information from the contaminated information system or component;
e. Identifying other information systems or system components that may have been subsequently contaminated; and
f. Performing other [Assignment: organization-defined actions].

IMPLEMENTATION

STATE

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

IR-10 Integrated Information Security Analysis Team

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

IMPLEMENTATION

STATE

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

MA–Maintenance

MA-1 System Maintenance Policy and Procedures

RISK STATEMENT

Commercial software is not supported by a vendor and introduces errors into the information system processing environment.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
b. Reviews and updates the current:
   1. System maintenance policy [Assignment: organization-defined frequency]; and
   2. System maintenance procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization has a policy that addresses system maintenance controls.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has written, documented system maintenance policies and procedures in place.

BACK TO CONTENTS

MA-2 Controlled Maintenance

RISK STATEMENT

Unforeseen hardware failures occur due to lack of up to date maintenance records.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

IMPLEMENTATION

STATE

The state organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization maintains, updates and accepts maintenance records according to vendor specifications.

BACK TO CONTENTS

MA-3 Maintenance Tools

RISK STATEMENT

Equipment is not available due to improper maintenance.

PRIORITY/BASELINE

P3 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization approves, controls, and monitors information system maintenance tools.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Diagnostic equipment is available and designated for application information system software/hardware.

BACK TO CONTENTS

MA-4 Nonlocal Maintenance

RISK STATEMENT

Unauthorized access is gained through diagnostic and configuration network ports.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Approves and monitors nonlocal maintenance and diagnostic activities;
b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintains records for nonlocal maintenance and diagnostic activities; and
e. Terminates session and network connections when nonlocal maintenance is completed.

IMPLEMENTATION

STATE

The state organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization disables or controls network ports.

BACK TO CONTENTS

MA-5 Maintenance Personnel

RISK STATEMENT

Unauthorized visitors gain physical access to facilities due to insufficient physical entry controls.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

IMPLEMENTATION

STATE

The state organization allows only authorized personnel to perform maintenance on the information system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization escorts visitors through sensitive physical security areas.

BACK TO CONTENTS

MA-6 Timely Maintenance

RISK STATEMENT

The lack of processes for system maintenance may result in compromise of system security due to latest updates not being made to systems in a timely manner.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Maintenance resources are made readily available to personnel.

BACK TO CONTENTS

MP–Media Protection

MP-1 Media Protection Policy and Procedures

RISK STATEMENT

Media (e.g., documents, computer media (e.g. tapes, disks), input/output data, and system documentation) is compromised by unauthorized parties due to ineffective handling procedures.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
b. Reviews and updates the current:
   1. Media protection policy [Assignment: organization-defined frequency]; and
   2. Media protection procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization has a policy that addresses media protection controls.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has written, documented media protection policies and procedures in place.

BACK TO CONTENTS

MP-2 Media Access

RISK STATEMENT

Data stored on removable computer media is damaged or disclosed due to ineffective handling procedures.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

IMPLEMENTATION

STATE

The state organization restricts access to information system media to authorized individuals.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users are limited access to media based on roles and/or responsibilities.

BACK TO CONTENTS

MP-3 Media Marking

RISK STATEMENT

Information is disclosed due to mislabeled, unlabeled or mishandled physical or electronic media.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Media is labeled for handling with detail as appropriate.

BACK TO CONTENTS

MP-4 Media Storage

RISK STATEMENT

The lack of formal procedures for handling, processing, storing and communicating information consistent with its classification scheme, may result in potential mishandling or misuse of information by unauthorized parties.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Media is secured in locked storage bins or containers.

BACK TO CONTENTS

MP-5 Media Transport

RISK STATEMENT

Information stored in physical media may be disclosed to or altered by unauthorized parties while being physically transported.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards];
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The agency employee protection mechanisms during the transportation of media, such locks, secured bins, etc.

BACK TO CONTENTS

MP-6 Media Sanitization

RISK STATEMENT

Data stored on disposed-of media is inappropriately disclosed to unauthorized parties due to ineffective data disposal procedures.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

IMPLEMENTATION

STATE

Prior to the sale or transfer of data processing equipment, to other than another Texas state agency or agent of the state, state agencies shall assess whether to remove data from any associated storage device.

Electronic state records shall be destroyed in accordance with §441.185, Government Code. If the record retention period applicable for an electronic state record has not expired at the time the record is removed from data process equipment, the state agency shall retain a hard copy or other electronic copy of the record for the required retention period.

If it is possible that restricted personal information, confidential information, mission critical information, intellectual property, or licensed software is contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. Additional information on sanitization tools and methods of destruction (that comply with the Department of Defense 5220.22-M standard) are provided in the “Sale or Transfer of Computers and Software” guidelines available at http://www.dir.texas.gov.

State agencies shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information:

- date;
- description of the item(s) and serial number(s);
- inventory number(s);
- the process and sanitization tools used to remove the data or method of destruction; and
- the name and address of the organization the equipment was transferred to.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has implemented procedures to dispose of media containing departmental data in a manner that adequately protects the confidentiality of the data and renders it unrecoverable (e.g., as overwriting or modifying the electronic media to make it unreadable or indecipherable or otherwise physically destroying the electronic media), and in accordance with organizational records retention schedules.

BACK TO CONTENTS

MP-7 Media Use

RISK STATEMENT

Inadequate procedures for handling media (disclosure, modification, removal, and destruction) may result in potential compromise of information by unauthorized parties.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].

IMPLEMENTATION

STATE

The state organization restricts the use of mobile devices with information storage capability, based on documented risk management decisions

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Policy or procedures prohibit use of certain types of media.

BACK TO CONTENTS

MP-8 Media Downgrading

RISK STATEMENT

Confidential information could be exposed by media which is incorrectly downgraded.

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Establishes [Assignment: organization-defined information system media downgrading process] that includes employing downgrading mechanisms with [Assignment: organization-defined strength and integrity];
b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
c. Identifies [Assignment: organization-defined information system media requiring downgrading]; and
d. Downgrades the identified information system media using the established process.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Removal of information from media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed.

PE–Physical and Environmental Protection

PE-1 Physical and Environmental Protection Policies and Procedures

RISK STATEMENT

Unauthorized parties have access to facilities due to security flaws in physical layout.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

b. Reviews and updates the current:
   1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and
   2. Physical and environmental protection procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization head or his or her designated representative(s) shall document and manage physical access to mission critical information resources facilities to ensure the protection of information resources from unlawful or unauthorized access, use, modification or destruction.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has documented policies and supporting procedures to protect organizational facilities based on their criticality, and has implemented physical access safeguards to appropriate granting, controlling, and monitoring of physical access to organizational facilities.

BACK TO CONTENTS

PE-2 Physical Access Authorizations

RISK STATEMENT

Unauthorized parties gain physical access to facilities due to insufficient physical entry controls.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and
d. Removes individuals from the facility access list when access is no longer required.

IMPLEMENTATION

STATE

The state organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Only accepted personnel may enter secured areas.

BACK TO CONTENTS

PE-3 Physical Access Control

RISK STATEMENT

Unauthorized parties gain physical access to facilities due to insufficient physical perimeter controls.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards];
b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];
c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];
e. Secures keys, combinations, and other physical access devices;
f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and
g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

IMPLEMENTATION

STATE

The state organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Individuals may access individually secured areas by accepted, distributed electronic badge access.

BACK TO CONTENTS

PE-4 Access Control for Transmission Medium

RISK STATEMENT

Physical equipment is compromised due to the lack of protection from environmental threats and hazards.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Access to the datacenter is limited to accepted, appropriate personnel.

BACK TO CONTENTS

PE-5 Access Control for Output Devices

RISK STATEMENT

Appropriate physical safeguards have not been established to protect sensitive documents and/or output devices.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Information system processing areas are secured and limited to personnel based on roles/responsibilities.

BACK TO CONTENTS

PE-6 Monitoring Physical Access

RISK STATEMENT

To prevent unauthorized parties from having inappropriate physical access to specific rooms and offices of a facility.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

IMPLEMENTATION

STATE

The state organization monitors physical access to the information system to detect and respond to physical security incidents.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has documented standards and procedures to monitor physical access to offices, rooms, data centers, areas containing information systems, and other facilities based on risk. Monitoring includes review of logs and alerts from physical security systems, and cameras.

BACK TO CONTENTS

PE-7 Withdrawn

BACK TO CONTENTS

PE-8 Visitor Access Records

RISK STATEMENT

Failure to protect facilities through sufficient physical entry controls may result in unauthorized parties accessing the organization's facilities.

PRIORITY/BASELINE

P3 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and
b. Reviews visitor access records [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible)

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Visitors are escorted at specific times and a log of entry/exit is maintained.

BACK TO CONTENTS

PE-9 Power Equipment and Cabling

RISK STATEMENT

Unauthorized access to information resources is obtained through tapping into inappropriately exposed cabling infrastructure.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization protects power equipment and power cabling for the information system from damage and destruction.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Cabling infrastructure is not readily accessible to employees, and/or protected by physical access mechanisms.

BACK TO CONTENTS

PE-10 Emergency Shutoff

RISK STATEMENT

Utility outages disrupt business systems.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Emergency shut-off switches are available for usage in critical processing areas.

BACK TO CONTENTS

PE-11 Emergency Power

RISK STATEMENT

The lack of acceptable plans and operational controls to enable power contingency mechanisms may lead to potential disruptions of equipment supporting critical business operations.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An uninterruptible power supply is available to the information system infrastructure.

BACK TO CONTENTS

PE-12 Emergency Lighting

RISK STATEMENT

The lack of automatic emergency lighting during power outage or disruption may potentially disrupt continuity of business functions.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

IMPLEMENTATION

STATE

The state organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has lighting in critical processing areas supported through a separate power grid or source in the event of an emergency.

BACK TO CONTENTS

PE-13 Fire Protection

RISK STATEMENT

External and/or environmental threats (e.g., fire, flood, earthquake, civil unrest) disrupt operations due to inadequate physical security controls.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

IMPLEMENTATION

STATE

Information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

a. The organization deploys appropriate fire suppression equipment to protect organizational data centers, server rooms, and other areas containing information systems in the event of a fire.
b. The staff receives training in appropriate response in case of emergencies and use of fire suppression equipment.

BACK TO CONTENTS

PE-14 Temperature and Humidity Controls

RISK STATEMENT

External and/or environmental threats (e.g., fire, flood, earthquake, civil unrest) disrupt operations due to inadequate physical security controls.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and
b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The data center and other critical processing areas has humidity monitors.

BACK TO CONTENTS

PE-15 Water Damage Protection

RISK STATEMENT

Information systems are compromised due to the lack of protection from environmental threats and hazards.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

IMPLEMENTATION

STATE

The state organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The data center or other critical processing area has a water shut-off valve.

BACK TO CONTENTS

PE-16 Delivery and Removal

RISK STATEMENT

Unauthorized parties gain physical access to critical or sensitive information processing facilities due to inadequate physical security policies and standards.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.

IMPLEMENTATION

STATE

The state organization authorizes, monitors, and controls system components entering and exiting data processing facilities and maintains records of those items

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has assessed whether physical security to sensitive areas (e.g., data center, server room, student or patient records room, etc.) can be circumvented.

BACK TO CONTENTS

PE-17 Alternate Work Site

RISK STATEMENT

Unauthorized parties gain physical access to critical or sensitive information processing facilities due to inadequate physical security policies and standards.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Employs [Assignment: organization-defined security controls] at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An alternative, offsite work site is available in the event of a natural disaster in the primary processing location.

BACK TO CONTENTS

PE-18 Location of Information System Components

RISK STATEMENT

Unauthorized parties gain physical access to critical or sensitive information resources due to resources being located in proximity to public areas.

PRIORITY/BASELINE

P3 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

PE-19 Information Leakage

RISK STATEMENT

PRIORITY / BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization protects the information system from information leakage due to electromagnetic signals emanations.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

PE-20 Asset Monitoring and Tracking

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Employs [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas]; and
b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

PL–Planning

PL-1 Security Planning Policy and Procedures

RISK STATEMENT

Information security is not defined in a framework within the organizational environment.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
b. Reviews and updates the current:
   1. Security planning policy [Assignment: organization-defined frequency]; and
   2. Security planning procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

As required by TAC 202.71(d)(4), the state organization delivers, at least annually, to the organization head a report on state organization information security program

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has written, documented security policies and procedure in place.

BACK TO CONTENTS

PL-2 System Security Plan

RISK STATEMENT

Management does not have a documented security plan.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops a security plan for the information system that:
   1. is consistent with the organization's enterprise architecture;
   2. explicitly defines the authorization boundary for the system;
   3. describes the operational context of the information system in terms of missions and business processes;
   4. provides the security categorization of the information system including supporting rationale;
   5. describes the operational environment for the information system and relationships with or connections to other information systems;
   6. provides an overview of the security requirements for the system;
   7. identifies any relevant overlays, if applicable;
   8. describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
   9. is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];
c. Reviews the security plan for the information system [Assignment: organization-defined frequency];
d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
e. Protects the security plan from unauthorized disclosure and modification.

IMPLEMENTATION

STATE

The state organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a broad system security plan in place and reviews it annually for appropriateness.

BACK TO CONTENTS

PL-3 Withdrawn

BACK TO CONTENTS

PL-4 Rules of Behavior

RISK STATEMENT

Improper use of information or assets occurs inside an information processing facility.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and
d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

IMPLEMENTATION

STATE

The state organization defines scope, behavior, and practices; compliance monitoring pertaining to users of information resources.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Personnel sign an acceptable usage policy and procedure.

BACK TO CONTENTS

PL-5 Withdrawn

BACK TO CONTENTS

PL-6 Withdrawn

BACK TO CONTENTS

PL-7 Security Concept of Operations

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and
b. Reviews and updates the CONOPS [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

PL-8 Information Security Architecture

RISK STATEMENT

The lack of establishing an enterprise information model may result in application development and decision-supporting activities that are inconsistent with IT plans.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Develops an information security architecture for the information system that:
   1. describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. describes any information security assumptions about, and dependencies on, external services;
b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and
c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Information security architecture is designed with consideration to the overall information security strategy of the organization.

BACK TO CONTENTS

PL-9 Central Management

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization centrally manages [Assignment: organization-defined security controls and related processes].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

PM–Program Management

PM-1 Information Security Program Plan

RISK STATEMENT

Lack of a comprising security program may result in the compromise of sensitive information due to loss of integrity or confidentiality.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Develops and disseminates an organization-wide information security program plan that:
   1. provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
   2. includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
   3. reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
   4. is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation;
b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency];
c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
d. Protects the information security program plan from unauthorized disclosure and modification.

IMPLEMENTATION

STATE

All state organizations are required to have an information resources security program consistent with these standards, and the state organization's head is responsible for the protection of information resources.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

a. The organization maintains an information security program accepted by the state organization head that includes appropriate protections, based on risk, for certain information resources owned, leased, or under the custodianship, including outsourced resources, department, operating unit, or employee of the organization.
b. The organization reviews and updates the information security program plan at least annually taking into account changes in business, technology, threats, incidents, organizational missions etc.

BACK TO CONTENTS

PM-2 Senior Information Security Officer

RISK STATEMENT

Responsibility for the security program has not been defined.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

IMPLEMENTATION

STATE

Each state organization head or his or her designated representative(s) shall designate an information security officer to administer the state organization information security program.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a designated security official who:

a. is responsible for the development and implementation of the organizational information security program;
b. is responsible for the development of information security policies and procedures;
c. is responsible for and has authority for monitoring of compliance to the organization's information security policy and procedures; and
d. has appropriate level of accessibility and visibility from executive leadership of the organization to be effective.

BACK TO CONTENTS

PM-3 Information Security Resources

RISK STATEMENT

Management does not provide guidance for security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
c. Ensures that information security resources are available for expenditure as planned.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has long-term and short-term budgeting and capital planning initiatives in place.

BACK TO CONTENTS

PM-4 Plan of Action and Milestones Process

RISK STATEMENT

Performance monitoring, assessment and reporting are not performed appropriately whereby remedial actions are not identified or initiated.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
   1. are developed and maintained;
   2. document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the nation; and
   3. are reported in accordance with OMB FISMA reporting requirements.
b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

IMPLEMENTATION

STATE

The state organization develops and updates, a plan of action and milestone process for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization reports, documents and updates a risk analysis and plans for corrective actions.

BACK TO CONTENTS

PM-5 Information System Inventory

RISK STATEMENT

Important assets have not been clearly identified and inventoried.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization develops and maintains an inventory of its information systems.

IMPLEMENTATION

STATE

The state organization develops and maintains an inventory of its information systems.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization conducts an automated or manual inventory of information systems bi-annually.

BACK TO CONTENTS

PM-6 Information Security Measures of Performance

RISK STATEMENT

Management has not aligned the technology architecture with corporate strategy or external threats.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization develops, monitors, and reports on the results of information security measures of performance.

IMPLEMENTATION

STATE

The state organization develops, monitors, and reports on the results of information security measures of performance.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has Periodic reporting and performance measurement mechanisms in place.

BACK TO CONTENTS

PM-7 Enterprise Architecture

RISK STATEMENT

Management does not review new or modifications of existing technology infrastructure to determine that implementations are in line with strategic goals.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization develops enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has documented and established an enterprise architecture model with consideration to information security.

BACK TO CONTENTS

PM-8 Critical Infrastructure Plan

RISK STATEMENT

Management does not have a documented critical infrastructure plan.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

CONTROL DESCRIPTION

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has documented and established an enterprise infrastructure model with consideration to information security.

BACK TO CONTENTS

PM-9 Risk Management Strategy

RISK STATEMENT

Basic risk management activities have not been incorporated into IT-related activities (e.g., setting risk appetite, identification of risks, risk assessment, reporting criteria, etc.) and may lead to unanticipated losses or the inability to respond appropriately to risks.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

CONTROL DESCRIPTION

The organization:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the nation associated with the operation and use of information systems;
b. Implements the risk management strategy consistently across the organization; and
c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a written, documented risk management strategy.

BACK TO CONTENTS

PM-10 Security Authorization Process

RISK STATEMENT

The lack of security authorization process for information systems may result in new information systems causing security and compatibility issues.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

CONTROL DESCRIPTION

The organization:

a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
c. Fully integrates the security authorization processes into an organization-wide risk management program.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has defined designated information security roles and responsibilities.

BACK TO CONTENTS

PM-11 Mission/Business Process Definition

RISK STATEMENT

The IT strategy is not aligned with the business strategy or fully understood by the board and executives, limiting the achievement of value objectives for the organization.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

CONTROL DESCRIPTION

The organization:

a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation; and
b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has a written security mission that is accepted by executive management.

BACK TO CONTENTS

PM-12 Insider Threat Program

RISK STATEMENT

Lack of consistent process to manage insider threats may result in an inability to respond to (detect and prevent) malicious insider activity

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

CONTROL DESCRIPTION

The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has an active insider threat program.

BACK TO CONTENTS

PM-13 Information Security Workforce

RISK STATEMENT

Lack of establishing focused security workforce development and improvement programs, may result in unclear expectations on safeguarding organizational operations and assets.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

CONTROL DESCRIPTION

The organization establishes an information security workforce development and improvement program.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization makes information security training opportunities available to personnel on a continuous basis.

BACK TO CONTENTS

PM-14 Testing, Training, and Monitoring

RISK STATEMENT

Inadequate mechanisms to test, monitor and remediate information security capabilities may result in suspicious or anomalous activities going undetected.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

CONTROL DESCRIPTION

The organization:

a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
   1. are developed and maintained; and
   2. continue to be executed in a timely manner;
b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has an information security training program specific to organizational systems.

BACK TO CONTENTS

PM-15 Contacts with Security Groups and Associations

RISK STATEMENT

Inadequate contacts and communication protocols with relevant authorities and special interest groups may result in the lack of knowledge of latest security threats and industry trends, information security incidents going unreported or unsupported by legal authorities.

PRIORITY/BASELINE

P3
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

CONTROL DESCRIPTION

The organization establishes and institutionalizes contact with selected groups and associations within the security community:

a. To facilitate ongoing security education and training for organizational personnel;
b. To maintain currency with recommended security practices, techniques, and technologies; and
c. To share current security-related information including threats, vulnerabilities, and incidents.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Employee personnel are members of external information security organizations.

BACK TO CONTENTS

PM-16 Threat Awareness Program

RISK STATEMENT

Failure to conduct suitable and relevant threat awareness program and to publish notifications to enhance awareness of organizational policies and procedures may result in potential security breach of the operational environment.

PRIORITY/BASELINE

P1
Deployed organization-wide.
Supporting information security program.
Not associated with security control baselines.
Independent of any system impact level.

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

IMPLEMENTATION

STATE

State implementation of this standard is incorporated into TAC 202

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A threat awareness program, such as email notification to alert of existing threats is in place.

BACK TO CONTENTS

PS–Personnel Security

PS-1 Personnel Security Policy and Procedures

RISK STATEMENT

Employees, contractors and third party users do not maintain their security responsibilities.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
b. Reviews and updates the current:
   1. personnel security policy [Assignment: organization-defined frequency]; and
   2. personnel security procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization has a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has written, documented personnel security policies and procedures in place.

BACK TO CONTENTS

PS-2 Position Risk Designation

RISK STATEMENT

Security roles and responsibilities are not defined and clearly communicated to job candidates during the pre-employment process.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and updates position risk designations [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

All authorized users (including, but not limited to, state organization personnel, temporary employees, and employees of independent contractors) of the state organization's information resources, shall formally acknowledge that they will comply with the security policies and procedures of the state organization or they shall not be granted access to information resources. The state organization head or his or her designated representative will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to state organization information resources.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization identifies and classifies personnel positions based on risk category. In other words - the context for classifying positions by risk level is to identify and enforce background checks and other controls due to the higher risk position, e.g., a security administrator with "keys to the kingdom" has a higher risk profile and may require higher analysis than a groundskeeper for instance.

BACK TO CONTENTS

PS-3 Personnel Screening

RISK STATEMENT

Employees, contractors and third party users breach security due to lack of management.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

IMPLEMENTATION

STATE

The state organization screens individuals requiring access to organizational information and information systems before authorizing access.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization uses background checks prior to hiring new employees.

BACK TO CONTENTS

PS-4 Personnel Termination

RISK STATEMENT

Security breaches occur during employment terminations or changes due to lack of defined management responsibilities for these situations.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization, upon termination of individual employment:

a. Disables information system access within [Assignment: organization-defined time period];
b. Terminates/revokes any authenticators/credentials associated with the individual;
c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
d. Retrieves all security-related organizational information system-related property;
e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

IMPLEMENTATION

STATE

The state organization, upon termination of individual employment, terminates information system access, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Employee access is revoked upon termination of employment.

BACK TO CONTENTS

PS-5 Personnel Transfer

RISK STATEMENT

Employee, contractor or third party user terminations or change of responsibilities could result in a security breach due to lack of a defined management process for terminations or changes in responsibilities.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

IMPLEMENTATION

STATE

The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Information system owners periodically review access privileges.

BACK TO CONTENTS

PS-6 Access Agreements

RISK STATEMENT

Employees or contractors do not agree or sign terms or conditions of employment.

PRIORITY/BASELINE

P3 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Develops and documents access agreements for organizational information systems;
b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and
c. Ensures that individuals requiring access to organizational information and information systems:
    1. Sign appropriate access agreements prior to being granted access; and
    2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Employees sign access agreements.

BACK TO CONTENTS

PS-7 Third-Party Personnel Security

RISK STATEMENT

Security is breached by employees, contractors or third party users that leverage access given after termination or change of their employment, contract or agreement.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and
e. Monitors provider compliance.

IMPLEMENTATION

STATE

The state organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Service level agreements (SLA's) are be used to define the role of third parties specific to applicable information security policies and procedures.

BACK TO CONTENTS

PS-8 Personnel Sanctions

RISK STATEMENT

Security breaches occur by employees due to lack of formal disciplinary process.

PRIORITY/BASELINE

P3 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

IMPLEMENTATION

STATE

The state organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Designated officials maintain a formal sanction program.

BACK TO CONTENTS

RA–Risk Assessment

RA-1 Risk Assessment Policy and Procedures

RISK STATEMENT

Management is unable to identify potential events with negative impact and events representing opportunities to be pursued which may lead to unmanageable IT risks.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
b. Reviews and updates the current:
   1. Risk assessment policy [Assignment: organization-defined frequency]; and
   2. Risk assessment procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization has a risk assessment policy which includes process of identifying, evaluating, and documenting the level of impact that may result from the operation of an information system on an organization's mission, functions, image, reputation, assets, or individuals.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Written, documented risk assessment policies and procedures are in place.

BACK TO CONTENTS

RA-2 Security Categorization

RISK STATEMENT

Information is disclosed due to lack of protection based on the need, priorities and expected degree of protection.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

IMPLEMENTATION

STATE

State organizations are responsible for defining all information classification categories except the Confidential Information category, which is defined in Subchapter A of this chapter, and establishing the appropriate controls for each.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

a. The organization has a documented data classification policy or standard that guides data owners on data categorization, and associated security requirements of information systems where such information is maintained.
b. Information systems have security plans that aligned with the classification of the information system.

BACK TO CONTENTS

RA-3 Risk Assessment

RISK STATEMENT

Information around risks and related control options are not presented to management before management decisions are made.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
c. Reviews risk assessment results [Assignment: organization-defined frequency];
d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

IMPLEMENTATION

STATE

A risk assessment of information resources shall be performed and documented. The risk assessment shall be updated based on the inherent risk. The inherent risk and frequency of the risk assessment will be ranked, at a minimum, as either "High," "Moderate," or "Low."

Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the state organization head or his or her designated representative(s). The state organization head or his or her designated representative(s) shall make the final risk management decisions to either accept exposures or protect the data according to its value/sensitivity. The state organization head or his or her designated representative(s) shall approve the security risk management plan. This information may be exempt from disclosure under §2054.077(c), Government Code.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

a. The organization has policies and supporting processes that define triggers for when information security related risk assessments should be conducted, as well as the criteria for risk assessment (e.g., likelihood and impact.
b. Information security risk assessments are conducted at least annually.

BACK TO CONTENTS

RA-4 Withdrawn

BACK TO CONTENTS

RA-5 Vulnerability Scanning

RISK STATEMENT

Technical vulnerabilities are exploited to gain inappropriate or unauthorized access to information systems due to lack of controls for those vulnerabilities.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

IMPLEMENTATION

STATE

The state organization scans for vulnerabilities in the information system at least annually or when significant new vulnerabilities potentially affecting the system are identified and reported.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has periodic vulnerability scanning processes in place and operational.

BACK TO CONTENTS

RA-6 Technical Surveillance Countermeasures Survey

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators occur]].

IMPLEMENTATION

STATE

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE(S)

SA–System and Service Acquisition

SA-1 System and Services Acquisition Policy and Procedures

RISK STATEMENT

Acquiring resources for IT is done inconsistently with unreasonable cost.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
b. Reviews and updates the current:
   1. System and services acquisition policy [Assignment: organization-defined frequency]; and
   2. System and services acquisition procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has documented acquisition policies and procedures in place.

BACK TO CONTENTS

SA-2 Allocation of Resources

RISK STATEMENT

Management has not aligned the information technology architecture with corporate strategy.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Determines information security requirements for the information system or information system service in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

IMPLEMENTATION

STATE

The state organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Resource allocation is a part of the general budgeting strategy for the organization.

BACK TO CONTENTS

SA-3 System Development Life Cycle

RISK STATEMENT

Developed and implemented systems do not consider the design phase of the systems development lifecycle.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
b. Defines and documents information security roles and responsibilities throughout the system development life cycle;
c. Identifies individuals having information security roles and responsibilities; and
d. Integrates the organizational information security risk management process into system development life cycle activities.

IMPLEMENTATION

STATE

Information security, security testing, and audit controls shall be included in all phases of the system development lifecycle or acquisition process

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

a. The existing system development lifecycle includes consideration for information security.
b. Test environments are kept either physically or logically separate from production environments.
c. Copies of production data are not used for testing unless the data has been authorized for public release or unless all custodians involved in testing are otherwise authorized access to the data.

BACK TO CONTENTS

SA-4 Acquisition Process

RISK STATEMENT

The organization's interests are not protected in IT acquisition contractual agreements.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

IMPLEMENTATION

STATE

The state organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws and standards.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization includes security requirements in contracts for acquisition of information systems.

BACK TO CONTENTS

SA-5 Information System Documentation

RISK STATEMENT

Sensitive system configuration information is accessed by unauthorized parties due to inadequate security of system documentation.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization:

a. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to [Assignment: organization-defined personnel or roles].

IMPLEMENTATION

STATE

The state organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization effectively secures system security documentation and configuration settings.

BACK TO CONTENTS

SA-6 Withdrawn

BACK TO CONTENTS

SA-7 Withdrawn

BACK TO CONTENTS

SA-8 Security Engineering Principles

RISK STATEMENT

Programming errors or misconfiguration leads to vulnerabilities that can be exploited.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Code updates are reviewed for security gaps/concerns.

BACK TO CONTENTS

SA-9 External Information System Services

RISK STATEMENT

Services, reports and records provided by a third party are not consistently monitored and reviewed by management.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

IMPLEMENTATION

STATE

The state organization requires that providers of external information system services employ adequate security controls in accordance with these standards and monitors security control compliance.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization explicitly defines usage of external systems.

BACK TO CONTENTS

SA-10 Developer Configuration Management

RISK STATEMENT

Changes are made to production systems without a formal change process.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation];
b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

IMPLEMENTATION

STATE

All security-related information resources changes shall be approved by the information owner through a change control process. Approval shall occur prior to implementation by the state organization or independent contractors.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization should have documented change control procedures that:

a. requires approval for making changes;
b. takes into account impact on information security and related configurations;
c. performs appropriate level of testing of changes, including information security, as applicable;
d. tracks defects and security flaws; and
e. requires approval from appropriate level of management for authorizing changes into production.

BACK TO CONTENTS

SA-11 Developer Security Testing and Evaluation

RISK STATEMENT

Systems are implemented which are not developed according to internal security standards.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization requires the developer of the information system, system component, or information system service to:

a. Create and implement a security assessment plan;
b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];
c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d. Implement a verifiable flaw remediation process; and
e. Correct flaws identified during security testing/evaluation.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Security assessment planning and analysis are a part of the routine code development process.

BACK TO CONTENTS

SA-12 Supply Chain Protection

RISK STATEMENT

PRIORITY/BASELINE

P1 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-13 Trustworthiness

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Describes the trustworthiness required in the [Assignment: organization-defined information system, information system component, or information system service] supporting its critical missions/business functions; and
b. Implements [Assignment: organization-defined assurance overlay] to achieve such trustworthiness.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-14 Criticality Analysis

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization-defined decision points in the system development life cycle].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-15 Development Process, Standards, and Tools

RISK STATEMENT

PRIORITY/BASELINE

P2 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
   1. Explicitly addresses security requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
b. Reviews the development process, standards, tools, and tool options/configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [Assignment: organization-defined security requirements].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-16 Developer-provided Training

RISK STATEMENT

PRIORITY/BASELINE

P2 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-17 Developer Security Architecture and Design

RISK STATEMENT

PRIORITY/BASELINE

P1 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;
b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-18 Tamper Resistance and Detection

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization implements a tamper protection program for the information system, system component, or information system service.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-19 Component Authenticity

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and
b. Reports counterfeit information system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-20 Customized Development of Critical Components

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization re-implements or custom develops [Assignment: organization-defined critical information system components].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-21 Developer Screening

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization requires that the developer of [Assignment: organization-defined information system, system component, or information system service]:

a. Have appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and
b. Satisfy [Assignment: organization-defined additional personnel screening criteria].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SA-22 Unsupported System Components

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC–System and Communication Protection

SC-1 System and Communications Protection Policy and Procedures

RISK STATEMENT

IT security procedures are not documented and communicated.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

b. Reviews and updates the current:
   1. System and communications protection policy [Assignment: organization-defined frequency]; and
   2. System and communications protection procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The state organization develops, disseminates, and periodically reviews/updates:

- a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has documented policies and supporting processes for defining and enforcing requirements to protect data transmissions and system-to-system communications, including analyzing the identity of communicators (for example, over the Internet, within the organization, private networks, etc.).

BACK TO CONTENTS

SC-2 Application Partitioning

RISK STATEMENT

The integrity of a business process is compromised due to the lack of segregation of duties (e.g., maker & checker).

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system separates user functionality (including user interface services) from information system management functionality.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

BACK TO CONTENTS

SC-3 Security Function Isolation

RISK STATEMENT

PRIORITY/BASELINE

P1 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system isolates security functions from nonsecurity functions.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-4 Information in Shared Resources

RISK STATEMENT

Sensitive systems co-located with less sensitive systems are accessed by unauthorized parties.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system prevents unauthorized and unintended information transfer via shared system resources.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Consideration of shared system resources are evaluated once a risk assessment and data classification are completed.

BACK TO CONTENTS

SC-5 Denial of Service Protection

RISK STATEMENT

Inadequately managed and controlled networks and supporting infrastructure expose systems and applications.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].

IMPLEMENTATION

STATE

Each state organization head or his/her designated representative and information security officer shall establish a security strategy that includes perimeter protection.

The department will provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize State information resources as specified in Chapters 2054 and 2059, Government Code. Perimeter security controls may include some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has controls in place to decrease risk of denial of service attacks (internal and external) on critical information systems. Examples could include use of tools and configuration settings at the network layer to combat such attempts, and/or proactively monitoring for denial of service attempts so timely steps can be taken to address the risk.

BACK TO CONTENTS

SC-6 Resource Availability

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-7 Boundary Protection

RISK STATEMENT

Computer connections and information flows breach access control policy as a result of inconsistencies with network routing configurations.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

IMPLEMENTATION

STATE

The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The system boundary is explicitly defined and protection by a combination of hardware mechanisms (i.e., defense in depth).

BACK TO CONTENTS

SC-8 Transmission Confidentiality and Integrity

RISK STATEMENT

Files may be disclosed or modified by unauthorized parties as they are transferred.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.

IMPLEMENTATION

STATE

Confidential information that is transmitted over a public network (e.g.: the Internet) must be encrypted with, at minimum a 128-bit encryption algorithm. An organization may also choose to implement encryption for other data classifications.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization utilizes cryptographic mechanisms to protect the integrity of transmissions.

BACK TO CONTENTS

SC-9 Withdrawn

BACK TO CONTENTS

SC-10 Network Disconnect

RISK STATEMENT

Lack of network connection controls over communications sessions may result in unauthorized access to information systems

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Network connections are automatically disabled after a set time of inactivity.

BACK TO CONTENTS

SC-11 Trusted Path

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-12 Cryptographic Key Establishment and Management

RISK STATEMENT

Cryptographic keys are modified, lost, destroyed or disclosed to unauthorized parties.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

IMPLEMENTATION

STATE

When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization appropriately secures public and private keys.

BACK TO CONTENTS

SC-13 Cryptographic Protection

RISK STATEMENT

Encryption and other cryptographic controls are inconsistently used to protect information assets and deviate with policy.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

IMPLEMENTATION

STATE

Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management shall be based on documented state organization risk management decisions.

Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted.

Confidential information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted.)

Storing confidential information on portable devices is discouraged. Confidential information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-state organization owned computing device.

The minimum algorithm strength for protecting confidential information is a 128-bit encryption algorithm, subject to state organization risk management decisions justified and documented in accordance with TAC 202.21(c)(1)(H) and (d)(5).

A state organization may also choose to implement additional protections, which may include encryption, for other data classifications.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization uses public and private keys, along with other cryptographic mechanisms according to applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

BACK TO CONTENTS

SC-14 Withdrawn

BACK TO CONTENTS

SC-15 Collaborative Computing Devices

RISK STATEMENT

Unauthorized parties gain access to sensitive, secure areas due to the lack of implemented physical security controls.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system:

a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and
b. Provides an explicit indication of use to users physically present at the devices.

IMPLEMENTATION

STATE

The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

a. Automated mechanisms prevent access to collaborative computing devices, unless explicitly defined.
b. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated

BACK TO CONTENTS

SC-16 Transmission of Security Attributes

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system associates [Assignment: organization-defined security attributes] with information exchanged between information systems and between system components.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-17 Public Key Infrastructure Certificates

RISK STATEMENT

Cryptographic keys are modified, lost, destroyed or disclosed to unauthorized parties.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Usage of public key certificates is explicitly defined.

BACK TO CONTENTS

SC-18 Mobile Code

RISK STATEMENT

Unauthorized mobile code disrupts the production environment due to lack of built-in security controls.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The usage of mobile code mechanisms is limited and/or explicitly defined.

BACK TO CONTENTS

SC-19 Voice over Internet Protocol

RISK STATEMENT

Users have access to networks that they are not authorized to use.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Where in use, access to Voice over Internet Protocol (VoIP) technologies is limited to appropriate personnel.

BACK TO CONTENTS

SC-20 Secure Name/Address Resolution Service (Authoritative Source)

RISK STATEMENT

Networks and supporting infrastructure are exposed to unauthorized parties due to lack of defined network security and administration policies, procedures and standards.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system:

a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

IMPLEMENTATION

STATE

The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The network has established parent and client zones to maintain the appropriate level of isolation.

BACK TO CONTENTS

SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

RISK STATEMENT

Lack of procedures to analyze the authenticity and data integrity of the name/address resolution responses might result in potential breaks to the chain of trust in the DNS infrastructure.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016/

CONTROL DESCRIPTION

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

IMPLEMENTATION

STATE

The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An automated mechanism considers the authenticity and data integrity of the DNS trust levels.

BACK TO CONTENTS

SC-22 Architecture and Provisioning for Name/Address Resolution Service

RISK STATEMENT

Information systems fail due to improper fault tolerant or redundant architectures.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

IMPLEMENTATION

STATE

The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A fault-tolerant network infrastructure is in place.

BACK TO CONTENTS

SC-23 Session Authenticity

RISK STATEMENT

Unauthorized users access operating systems by physically or logically accessing valid inactive and/or unattended sessions.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system protects the authenticity of communications sessions.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Users should use an individual ID to access information systems.

BACK TO CONTENTS

SC-24 Fail in Known State

RISK STATEMENT

PRIORITY/BASELINE

P1 > LOW–No MOD–no HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-25 Thin Nodes

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs [Assignment: organization-defined information system components] with minimal functionality and information storage.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-26 Honeypots

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-27 Platform-independent Applications

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system includes: [Assignment: organization-defined platform-independent applications].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-28 Protection of Information at Rest

RISK STATEMENT

Sensitive data is exposed to unauthorized disclosure or modification while in storage.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Information is protected while at rest, through encryption or other security mechanism.

BACK TO CONTENTS

SC-29 Platform-independent Applications Heterogeneity

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs a diverse set of information technologies for [Assignment: organization-defined information system components] in the implementation of the information system.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-30 Concealment and Misdirection

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs [Assignment: organization-defined concealment and misdirection techniques] for [Assignment: organization-defined information systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-31 Covert Channel Analysis

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and
b. Estimates the maximum bandwidth of those channels.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-32 Information System Partitioning

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization partitions the information system into [Assignment: organization-defined information system components] residing in separate physical domains or environments based on [Assignment: organization-defined circumstances for physical separation of components].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-33 Withdrawn

BACK TO CONTENTS

SC-34 Non-modifiable Executable Programs

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system at [Assignment: organization-defined information system components]:

a. Loads and executes the operating environment from hardware-enforced, read-only media; and
b. Loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-35 Honeyclients

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-36 Distributed Processing and Storage

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-37 Out-of-band Channels

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs [Assignment: organization-defined out-of-band channels] for the physical delivery or electronic transmission of [Assignment: organization-defined information, information system components, or devices] to [Assignment: organization-defined individuals or information systems].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-38 Operations Security

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-39 Process Isolation

RISK STATEMENT

Insufficient segregation of communications and interfaces between the system processes, may expose sensitive information resources to unauthorized access.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The information system maintains a separate execution domain for each executing process.

IMPLEMENTATION

STATE

The organization uses operating systems that support process isolation.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The information system automatically enables a separate execution domain.

BACK TO CONTENTS

SC-40 Wireless Link Protection

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system protects external and internal [Assignment: organization-defined wireless links] from [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-41 Port and I/O Device Access

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization physically disables or removes [Assignment: organization-defined connection ports or input/output devices] on [Assignment: organization-defined information systems or information system components].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-42 Sensor Capability and Data

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system:

a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and
b. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-43 Operations Security

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Establishes usage restrictions and implementation guidance for [Assignment: organization-defined information system components] based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of such components within the information system.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SC-44 Detonation Chambers

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs a detonation chamber capability within [Assignment: organization-defined information system, system component, or location].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SE–Security

SE-1 Inventory of Personally Identifiable Information

RISK STATEMENT

PII have not been clearly identified and inventoried.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and
b. Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The results of a data classification and risk assessment allow for the inventory of PII in information systems.

BACK TO CONTENTS

SE-2 Privacy Incident Response

RISK STATEMENT

Lack of a Privacy Incident Response program may result in improper identification and handling of privacy events.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Develops and implements a Privacy Incident Response Plan; and
b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A written, documented privacy incident response plan is in place.

BACK TO CONTENTS

SI–System and Information Integrity

SI-1 System and Information Integrity Policy and Procedures

RISK STATEMENT

Applications fail to process correctly and correctly due to a failure to design control during application development.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates the current:
   1. System and information integrity policy [Assignment: organization-defined frequency]; and
   2. System and information integrity procedures [Assignment: organization-defined frequency].

IMPLEMENTATION

STATE

The integrity of data, its source, its destination, and processes applied to it shall be assured. Changes to data shall be made only in an authorized manner.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has documented information integrity policies and procedures in place.

BACK TO CONTENTS

SI-2 Flaw Remediation

RISK STATEMENT

Security vulnerabilities may not be identified timely.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

IMPLEMENTATION

STATE

The state organization identifies, reports, and corrects information system flaws.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

System flaws are tracked in a central repository for anticipated corrective actions.

BACK TO CONTENTS

SI-3 Malicious Code Protection

RISK STATEMENT

Unauthorized, malicious code is executed on systems without authorization.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
    1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
    2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

IMPLEMENTATION

STATE

The information system implements malicious code protection.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Malicious code mechanism conduct periodic system scans for vulnerabilities.

BACK TO CONTENTS

SI-4 Information System Monitoring

RISK STATEMENT

Suspicious or anomalous activities are not are not detected due to lack of intrusion detection systems.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2015

CONTROL DESCRIPTION

The organization:

a. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and
   2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

IMPLEMENTATION

STATE

Each state organization head or his/her designated representative and information security officer shall establish a security strategy that includes perimeter protection.

The department will provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize State information resources as specified in Chapters 2054 and 2059, Government Code. Perimeter security controls may include some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization has effective tools and processes in place to proactively detect and respond to security threats/events, through:

a. effectively placed and configured intrusion-detection system(s) and/or intrusion-prevention system(s) to guard against or monitor for malicious network traffic at the perimeter;
b. effective placement and use of monitoring tools with configured applicable use cases to detect potential events relevant to the information system (e.g., DLP, SIEM, Netflow, etc.) ;
c. effective monitoring processes (e.g., alerts from IDS/IPS alert) for taking timely actions;
d. defined processes (e.g., use cases) that guide the responders to take appropriate level of action

BACK TO CONTENTS

SI-5 Security Alerts, Advisories, and Directives

RISK STATEMENT

Contacts with special interest groups or other specialists' security forums and professional associations is not coordinated or performed as a result of ill-defined processes.

PRIORITY/BASELINE

P1 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2016

CONTROL DESCRIPTION

The organization:

a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

IMPLEMENTATION

STATE

The state organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization periodically submits security directives to personnel for dissemination as appropriate.

BACK TO CONTENTS

SI-6 Security Function Verification

RISK STATEMENT

PRIORITY/BASELINE

P1 > LOW–No MOD–No HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system:

a. Verifies the correct operation of [Assignment: organization-defined security functions];
b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];
c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and
d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SI-7 Software, Firmware, and Information Integrity

RISK STATEMENT

Unauthorized tampering of system and/or configuration files is undetected due to the absence of file integrity mechanisms.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Software firmware allows for the scanning of information integrity.

BACK TO CONTENTS

SI-8 Spam Protection

RISK STATEMENT

Unauthorized information processing activities occur undetected due to lack of consistent logging and monitoring activities.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A spam filter is active on the organization email system.

BACK TO CONTENTS

SI-9 Withdrawn

BACK TO CONTENTS

SI-10 Information Input Validation

RISK STATEMENT

Data is input into applications that cause unexpected or incorrect results, possibly crashing or placing the application in an unknown and unplanned for state.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system checks the validity of [Assignment: organization-defined information inputs].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

An automated mechanism may allow for information system checks on the validity of information.

BACK TO CONTENTS

SI-11 Error Handling

RISK STATEMENT

System failure is not detected in a timely fashion due to inadequate fault logging and monitoring capabilities.

PRIORITY/BASELINE

P2 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system:

a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
b. Reveals error messages only to [Assignment: organization-defined personnel or roles].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

System failure notifications are provided to employee personnel as needed, automatically.

BACK TO CONTENTS

SI-12 Information Output Handling and Retention

RISK STATEMENT

Inaccurate data output from applications triggers unexpected results.

PRIORITY/BASELINE

P2 > LOW–Yes MOD–Yes HIGH–Yes

REQUIRED BY

February 2017

CONTROL DESCRIPTION

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

IMPLEMENTATION

STATE

The state organization handles and retains output from the information system in accordance with applicable laws, standards, and operational requirements.

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The organization handles information according to the standards set forth in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

BACK TO CONTENTS

SI-13 Predictable Failure Prevention

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Determines mean time to failure (MTTF) for [Assignment: organization-defined information system components] in specific environments of operation; and
b. Provides substitute information system components and a means to exchange active and standby components at [Assignment: organization-defined MTTF substitution criteria].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SI-14 Non-persistence

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization implements non-persistent [Assignment: organization-defined information system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SI-15 Information Output Filtering

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system validates information output from [Assignment: organization-defined software programs and/or applications] to ensure that the information is consistent with the expected content.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

SI-16 Memory Protection

RISK STATEMENT

Lack of operational controls to protect information system memory may result in malicious code exploiting the memory space to take control of critical systems and endpoints.

PRIORITY/BASELINE

P1 > LOW–No MOD–Yes HIGH–Yes

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

Execution of code is limited to appropriate personnel.

BACK TO CONTENTS

SI-17 Fail-safe Procedures

RISK STATEMENT

PRIORITY/BASELINE

P0 > LOW–No MOD–No HIGH–No

REQUIRED BY

No required date

CONTROL DESCRIPTION

The information system implements [Assignment: organization-defined fail-safe procedures] when [Assignment: organization-defined failure conditions occur].

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

BACK TO CONTENTS

TR–Transparency

TR-1 Privacy Notice

RISK STATEMENT

Laws and regulations are violated due to an organization failing to provide notices on usage of customer data.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;
b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and
c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

(1) PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE

The organization provides real-time and/or layered notice when it collects PII.

Supplemental Guidance: Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed/specific information.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

System banners (internal) and/or website notification (public) are in place to address the notification and usage of PII, where applicable.

BACK TO CONTENTS

TR-2 System of Records Notices and Privacy Act Statements

RISK STATEMENT

Laws and regulations are violated due to an organization failing to provide notices and privacy statements on usage of customer data.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);
b. Keeps SORNs current; and
c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

(1) SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS | PUBLIC WEBSITE PUBLICATION
The organization publishes SORNs on its public website.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

For applicable federal system, compliance with System of Records Notices criteria is followed.

BACK TO CONTENTS

TR-3 Dissemination of Privacy Program Information

RISK STATEMENT

Absence of privacy communication and reporting processes leading to policy violations and security breaches.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and
b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

A privacy impact officer is identified for the organization (as applicable).

BACK TO CONTENTS

UL–Use Limitation

UL-1 Internal Use

RISK STATEMENT

Customer information is improperly disclosed

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The usage of PII is limited to accepted personnel and tasks only.

BACK TO CONTENTS

UL-2 Information Sharing With Third Parties

RISK STATEMENT

Customer information is improperly disclosed when transmitted to a third party.

PRIORITY/BASELINE

REQUIRED BY

No required date

CONTROL DESCRIPTION

The organization:

a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;
b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;
c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and
d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

IMPLEMENTATION

STATE

No statewide control

STATE ORGANIZATION

[To be determined]

COMPARTMENT

[To be determined]

EXAMPLE

The usage of PII is limited to accepted personnel and tasks only.

BACK TO CONTENTS

APPENDIX A

NIST Control Families

Below is the inventoried list of NIST controls families that are included in this Control Catalog.

Access Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
AC-1	Access Control Policy and Procedures	P1	x	x	x	202.25(7)(B)	Feb-2015
AC-2	Account Management	P1	x	x	x	202.25 (2)	Feb-2015
AC-3	Access Enforcement	P1	x	x	x	202.20 (1)	Feb-2015
AC-4	Information Flow Enforcement	P1		x	x		
AC-5	Separation of Duties	P1		x	x	202.20(8)	Feb-2015
AC-6	Least Privilege	P1		x	x		
AC-7	Unsuccessful Logon Attempts	P2	x	x	x		Feb-2017
AC-8	System Use Notification	P1	x	x	x	202.25(9)	Feb-2015
AC-9	Previous Logon (Access) Notification	P0					
AC-10	Concurrent Session Control	P3			x		
AC-11	Session Lock	P3		x	x		
AC-12	Session Termination	P2		x	x		
AC-13	Supervision and Review — Access Control	---	withdrawn				
AC-14	Permitted Actions without Identification or Authentication	P3	x	x	x		Feb-2017
AC-15	Automated Marking	---	withdrawn				
AC-16	Security Attributes	P0					
AC-17	Remote Access	P1	x	x	x		Feb-2016
AC-18	Wireless Access	P1	x	x	x	202.25(7)(Z)	Feb-2015
AC-19	Access Control for Mobile Devices	P1	x	x	x		Feb-2016
AC-20	Use of External Information Systems	P1	x	x	x		Feb-2016
AC-21	Information Sharing	P2		x	x		
AC-22	Publicly Accessible Content	P3	x	x	x		Feb-2017
AC-23	Data Mining Protection	P0					
AC-24	Access Control Decisions	P0					
AC-25	Reference Monitor	P0					

Awareness and Training Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
AT-1	Security Awareness and Training Policy and Procedures	P1	x	x	x	202.25(7)(T)	Feb-2015
AT-2	Security Awareness Training	P1	x	x	x	202.27(d)	Feb-2015
AT-3	Role-Based Security Training	P1	x	x	x		Feb-2016
AT-4	Security Training Records	P3	x	x	x		Feb-2017
AT-5	Contacts with Security Groups and Associations	---	withdrawn				

Audit and Accountability Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
AU-1	Audit and Accountability Policy and Procedures	P1	x	x	x		Feb-2016
AU-2	Audit Events	P1	x	x	x	202.25(5)	Feb-2015
AU-3	Content of Audit Records	P1	x	x	x		Feb-2016
AU-4	Audit Storage Capacity	P1	x	x	x		Feb-2016
AU-5	Response to Audit Processing Failures	P1	x	x	x		Feb-2016
AU-6	Audit Review, Analysis, and Reporting	P1	x	x	x		Feb-2016
AU-7	Audit Reduction and Report Generation	P2		x	x		
AU-8	Time Stamps	P1	x	x	x		Feb-2016
AU-9	Protection of Audit Information	P1	x	x	x		Feb-2016
AU-10	Non-repudiation	P2			x		
AU-11	Audit Record Retention	P3	x	x	x		Feb-2017
AU-12	Audit Generation	P1	x	x	x		Feb-2016
AU-13	Monitoring for Information Disclosure	P0					
AU-14	Session Audit	P0					
AU-15	Alternate Audit Capability	P0					
AU-16	Cross-Organizational Auditing	P0					

Security Assessment and Authorization Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
CA-1	Security Assessment and Authorization Policies and Procedures	P1	x	x	x		Feb-2016
CA-2	Security Assessments	P2	x	x	x	202.21 (e)	Feb-2015
CA-3	System Interconnections	P1	x	x	x		Feb-2016
CA-4	Security Certification	---	withdrawn				
CA-5	Plan of Action and Milestones	P3	x	x	x		Feb-2017
CA-6	Security Authorization	P2	x	x	x		Feb-2017
CA-7	Continuous Monitoring	P2	x	x	x		Feb-2017
CA-8	Penetration Testing	P2			x		
CA-9	Internal System Connections	P2	x	x	x		Feb-2017

Configuration Management Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
CM-1	Configuration Management Policy and Procedures	P1	x	x	x	202.25 (7)(F)	Feb-2015
CM-2	Baseline Configuration	P1	x	x	x		Feb-2016
CM-3	Configuration Change Control	P1		x	x		
CM-4	Security Impact Analysis	P2	x	x	x	202.25 (6)(C)	Feb-2015
CM-5	Access Restrictions for Change	P1		x	x		
CM-6	Configuration Settings	P1	x	x	x		Feb-2016
CM-7	Least Functionality	P1	x	x	x		Feb-2016
CM-8	Information System Component Inventory	P1	x	x	x		Feb-2016
CM-9	Configuration Management Plan	P1		x	x		
CM-10	Software Usage Restrictions	P2	x	x	x		Feb-2017
CM-11	User-Installed Software	P1	x	x	x	202.25 (7)(V)	Feb-2015

Contingency Planning Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
CP-1	Contingency Planning Policy and Procedures	P1	x	x	x		Feb-2016
CP-2	Contingency Plan	P1	x	x	x	202.24 (a)	Feb-2015
CP-3	Contingency Training	P2	x	x	x		Feb-2017
CP-4	Contingency Plan Testing	P2	x	x	x	202.20(6)	Feb-2015
CP-5	Contingency Plan Update		withdrawn				
CP-6	Alternate Storage Site	P1		x	x	202.24 (b)	Feb-2015
CP-7	Alternate Processing Site	P1		x	x		
CP-8	Telecommunications Services	P1		x	x		
CP-9	Information System Backup	P1	x	x	x		Feb-2016
CP-10	Information System Recovery and Reconstitution	P1	x	x	x		Feb-2016
CP-11	Alternate Communications Protocols	P0					
CP-12	Safe Mode	P0					
CP-13	Alternative Security Mechanisms	P0					

Identification and Authentication Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
IA-1	Identification and Authentication Policy and Procedures	P1	x	x	x	202.25 (7)(K)	Feb-2015
IA-2	Identification and Authentication (Organizational Users)	P1	x	x	x	202.25 (3)(A)	Feb-2015
IA-3	Device Identification and Authentication	P1		x	x		
IA-4	Identifier Management	P1	x	x	x	202.25 (3)(B)	Feb-2015
IA-5	Authenticator Management	P1	x	x	x		Feb-2016
IA-6	Authenticator Feedback	P2	x	x	x		Feb-2016
IA-7	Cryptographic Module Authentication	P1	x	x	x		Feb-2016
IA-8	Identification and Authentication (Non-Organizational Users)	P1	x	x	x		Feb-2016
IA-9	Service Identification and Authentication	P0					
IA-10	Adaptive Identification and Authentication	P0					
IA-11	Re-authentication	P0					

Incident Response Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
IR-1	Incident Response Policy and Procedures	P1	x	x	x	202.26	Feb-2015
IR-2	Incident Response Training	P2	x	x	x		Feb-2017
IR-3	Incident Response Testing	P2		x	x		
IR-4	Incident Handling	P1	x	x	x		Feb-2016
IR-5	Incident Monitoring	P1	x	x	x		Feb-2016
IR-6	Incident Reporting	P1	x	x	x	202.26	Feb-2015
IR-7	Incident Response Assistance	P2	x	x	x		Feb-2017
IR-8	Incident Response Plan	P1	x	x	x		Feb-2016
IR-9	Information Spillage Response	P0					
IR-10	Integrated Information Security Analysis Team	P0					

Maintenance Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
MA-1	System Maintenance Policy and Procedures	P1	x	x	x		Feb-2016
MA-2	Controlled Maintenance	P2	x	x	x		Feb-2017
MA-3	Maintenance Tools	P3		x	x		
MA-4	Nonlocal Maintenance	P2	x	x	x		Feb-2017
MA-5	Maintenance Personnel	P2	x	x	x		Feb-2017
MA-6	Timely Maintenance	P2		x	x		

Media Protection Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
MP-1	Media Protection Policy and Procedures	P1	x	x	x		Feb-2016
MP-2	Media Access	P1	x	x	x		Feb-2016
MP-3	Media Marking	P2		x	x		
MP-4	Media Storage	P1		x	x		
MP-5	Media Transport	P1		x	x		
MP-6	Media Sanitization	P1	x	x	x	§202.28	Feb-2015
MP-7	Media Use	P1	x	x	x		Feb-2016
MP-8	Media Downgrading	P0					

Physical and Environmental Protection Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
PE-1	Physical and Environmental Protection Policy and Procedures	P1	x	x	x	202.23 (a)	Feb-2015
PE-2	Physical Access Authorizations	P1	x	x	x		Feb-2016
PE-3	Physical Access Control	P1	x	x	x		Feb-2016
PE-4	Access Control for Transmission Medium	P1		x	x		
PE-5	Access Control for Output Devices	P2		x	x		
PE-6	Monitoring Physical Access	P1	x	x	x		Feb-2016
PE-7	Visitor Control	---	withdrawn				
PE-8	Visitor Access Records	P3	x	x	x		Feb-2017
PE-9	Power Equipment and Cabling	P1		x	x		
PE-10	Emergency Shutoff	P1		x	x		
PE-11	Emergency Power	P1		x	x		
PE-12	Emergency Lighting	P1	x	x	x		Feb-2016
PE-13	Fire Protection	P1	x	x	x	202.23 (c)	Feb-2015
PE-14	Temperature and Humidity Controls	P1	x	x	x		Feb-2016
PE-15	Water Damage Protection	P1	x	x	x		Feb-2016
PE-16	Delivery and Removal	P2	x	x	x		Feb-2017
PE-17	Alternate Work Site	P2		x	x		
PE-18	Location of Information System Components	P3			x		
PE-19	Information Leakage	P0					
PE-20	Asset Monitoring and Tracking	P0					

Planning Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
PL-1	Security Planning Policy and Procedures	P1	x	x	x		Feb-2016
PL-2	System Security Plan	P1	x	x	x	202.71 (d)(2–3)	Feb-2015
PL-3	System Security Plan Update	---	withdrawn				
PL-4	Rules of Behavior	P2	x	x	x		Feb-2017
PL-5	Privacy Impact Assessment	---	withdrawn				
PL-6	Security-Related Activity Planning	---	withdrawn				
PL-7	Security Concept of Operations	P0					
PL-8	Information Security Architecture	P1		x	x		
PL-9	Central Management	P0					

Personnel Security Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
PS-1	Personnel Security Policy and Procedures	P1	x	x	x		Feb-2016
PS-2	Position Risk Designation	P1	x	x	x	202.27 (a)	Feb-2015
PS-3	Personnel Screening	P1	x	x	x		Feb-2016
PS-4	Personnel Termination	P1	x	x	x		Feb-2016
PS-5	Personnel Transfer	P2	x	x	x		Feb-2017
PS-6	Access Agreements	P3	x	x	x		Feb-2017
PS-7	Third-Party Personnel Security	P1	x	x	x		Feb-2016
PS-8	Personnel Sanctions	P3	x	x	x		Feb-2017

Risk Assessment Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
RA-1	Risk Assessment Policy and Procedures	P1	x	x	x		Feb-2016
RA-2	Security Categorization	P1	x	x	x	202.21 (b)	Feb-2015
RA-3	Risk Assessment	P1	x	x	x	202.22	Feb-2015
RA-4	Risk Assessment Update	---	withdrawn				
RA-5	Vulnerability Scanning	P1	x	x	x		Feb-2016
RA-6	Technical Surveillance Countermeasures Survey	P0					

System and Services Acquisition Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
SA-1	System and Services Acquisition Policy and Procedures	P1	x	x	x		Feb-2016
SA-2	Allocation of Resources	P1	x	x	x		Feb-2016
SA-3	System Development Life Cycle	P1	x	x	x	202.25(6)(B) & 202.25(7)(W)	Feb-2015
SA-4	Acquisition Process	P1	x	x	x	202.25 (7)(W)	Feb-2015
SA-5	Information System Documentation	P2	x	x	x		Feb-2017
SA-6	Software Usage Restrictions	---	withdrawn				
SA-7	User-Installed Software	---	withdrawn				
SA-8	Security Engineering Principles	P1		x	x		
SA-9	External Information System Services	P1	x	x	x		Feb-2016
SA-10	Developer Configuration Management	P1		x	x	202.25 (6)(c)	Feb-2015
SA-11	Developer Security Testing and Evaluation	P1		x	x		
SA-12	Supply Chain Protection	P1			x		
SA-13	Trustworthiness	P0					
SA-14	Criticality Analysis	P0					
SA-15	Development Process, Standards, and Tools	P2			x		
SA-16	Developer-Provided Training	P2			x		
SA-17	Developer Security Architecture and Design	P1			x		
SA-18	Tamper Resistance and Detection	P0					
SA-19	Component Authenticity	P0					
SA-20	Customized Development of Critical Components	P0					
SA-21	Developer Screening	P0					
SA-22	Unsupported System Components	P0					

System and Communications Protection Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
SC-1	System and Communications Protection Policy and Procedures	P1	x	x	x		Feb-2016
SC-2	Application Partitioning	P1		x	x		
SC-3	Security Function Isolation	P1			x		
SC-4	Information in Shared Resources	P1		x	x		
SC-5	Denial of Service Protection	P1	x	x	x	202.25 (8)	Feb-2015
SC-6	Resource Availability	P0					
SC-7	Boundary Protection	P1	x	x	x		Feb-2016
SC-8	Transmission Confidentiality and Integrity	P1		x	x	202.25 (4)	Feb-2015
SC-9	Transmission Confidentiality	---	withdrawn				
SC-10	Network Disconnect	P2		x	x		
SC-11	Trusted Path	P0					
SC-12	Cryptographic Key Establishment and Management	P1	x	x	x		Feb-2016
SC-13	Cryptographic Protection	P1	x	x	x	202.25(4) & 202.25(7)(H)	Feb-2015
SC-14	Public Access Protections	---	withdrawn				
SC-15	Collaborative Computing Devices	P1	x	x	x		Feb-2016
SC-16	Transmission of Security Attributes	P0					
SC-17	Public Key Infrastructure Certificates	P1		x	x		
SC-18	Mobile Code	P2		x	x		
SC-19	Voice Over Internet Protocol	P1		x	x		
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	x	x	x		Feb-2016
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	x	x	x		Feb-2016
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	x	x	x		Feb-2016
SC-23	Session Authenticity	P1		x	x		
SC-24	Fail in Known State	P1			x		
SC-25	Thin Nodes	P0					
SC-26	Honeypots	P0					
SC-27	Platform-Independent Applications	P0					

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
SC-28	Protection of Information at Rest	P1		x	x		
SC-29	Heterogeneity	P0					
SC-30	Concealment and Misdirection	P0					
SC-31	Covert Channel Analysis	P0					
SC-32	Information System Partitioning	P0					
SC-33	Transmission Preparation Integrity	---	withdrawn				
SC-34	Non-Modifiable Executable Programs	P0					
SC-35	Honeyclients	P0					
SC-36	Distributed Processing and Storage	P0					
SC-37	Out-of-Band Channels	P0					
SC-38	Operations Security	P0					
SC-39	Process Isolation	P1	x	x	x		Feb-2016
SC-40	Wireless Link Protection	P0					
SC-41	Port and I/O Device Access	P0					
SC-42	Sensor Capability and Data	P0					
SC-43	Usage Restrictions	P0					
SC-44	Detonation Chambers	P0					

System and Information Integrity Controls

CONTROL NUMBER	CONTROL NAME	PRIORITY	CONTROL BASELINE LOW	CONTROL BASELINE MODERATE	CONTROL BASELINE HIGH	LEGACY TAC 202	REQUIRED BY
SI-1	System and Information Integrity Policy and Procedures	P1	x	x	x		Feb-2016
SI-2	Flaw Remediation	P1	x	x	x		Feb-2016
SI-3	Malicious Code Protection	P1	x	x	x	202.75 (7)(Y)	Feb-2015
SI-4	Information System Monitoring	P1	x	x	x	202.25 (8)	Feb-2015
SI-5	Security Alerts, Advisories, and Directives	P1	x	x	x		Feb-2016
SI-6	Security Function Verification	P1			x		
SI-7	Software, Firmware, and Information Integrity	P1		x	x		
SI-8	Spam Protection	P2		x	x		
SI-9	Information Input Restrictions	---	withdrawn				
SI-10	Information Input Validation	P1		x	x		
SI-11	Error Handling	P2		x	x		
SI-12	Information Handling and Retention	P2	x	x	x		Feb-2017
SI-13	Predictable Failure Prevention	P0					
SI-14	Non-Persistence	P0					
SI-15	Information Output Filtering	P0					
SI-16	Memory Protection	P1		x	x		
SI-17	Fail-Safe Procedures	P0					

APPENDIX B

Acronyms and Abbreviations

AC | Access Control

AP | Authority and Purpose

AR | Accountability, Audit and Risk Management

AT | Awareness and Training

AU | Audit and Accountability

CA | Certification, Accreditation and Security Assessments

CIA | Confidentiality, Integrity, and Availability

CIO | Chief Information Officer

CISO | Chief Information Security Officer

CM | Configuration Management

CP | Contingency Planning

DI | Data Quality and Integrity

DIR | Department of Information Resources

DM | Data Minimization and Retention

DNS | Domain Name System

FISMA | Federal Information Security Management Act

HIPAA | Health Insurance Portability and Accountability Act

HITECH | Health Information Technology for Economic and Clinical Health Act

IA | Identification and Authentication

ID | Identifier

IP | Individual Participation and Redress

IR | Incident Response

IRS | Internal Revenue Service

IT | Information Technology

MA | Maintenance

MOD | Moderate

MP | Media Protection

NIST | National Institute of Standards and Technology

OCISO | Office of the Chief Information Security Officer

PE | Physical and Environmental Protection

PIA | Privacy Impact Assessment

PII | Personal Identifying Information

PL | Planning

PM | Program Management

POA&M | Plan of Action and Milestones

PS | Personnel Security

RA | Risk Assessment

SA | System and Services Acquisition

SC | System and Communications Protection

SDLC | System Development Life Cycle

SE | Security

SI | System and Information Integrity

SP | Special Publication

TAC | Texas Administrative Code

TR | Transparency

UL | Use Limitation

VoIP | Voice over Internet Protocol

VPN | Virtual Private Network

APPENDIX C

Glossary of Terms

The source for each term is shown in brackets.

Alternate Work Site | A working area that is attached to the Wide Area Network (WAN) either through a Public Switched Data Network (PSDN) or through the Internet. [IRS]

Attribute | A claim of a named quality or characteristic inherent in or ascribed to someone or something. [NIST]

Attribute-Based Access Control | Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. [IRS]

Authentication | Analyzing the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [NIST]

Banner | Display of an information system outlining the parameters for system or information use. [IRS]

Certification Authority (CA) | A trusted entity that issues and revokes public key certificates. [NIST]

Classified Information | National security information classified pursuant to Executive Order 12958. [IRS]

Confidentiality | Preserving authorized restrictions on information access and disclosure. [NIST]

Configuration Management | A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle. [IRS]

Cryptography | The process of rendering plain text information unreadable and restoring such unreadable information to a readable form. [IRS]

Data Integrity | The property that data has not been altered by an unauthorized entity. [NIST]

Data | A representation of facts, concepts, information or instruction suitable for communication, processing or interpretation by people or information systems. [IRS]

Decryption | The process of converting encrypted information into a readable form. Also called deciphering. [IRS]

Digital Signature | An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to inspect the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation. [NIST]

External Network | A network residing outside the security perimeter established by the telecommunications system. [IRS]

Extranet | A private data network using the public telephone network to establish a secure communications medium among authorized users (e.g., organization, vendors, business partners). An Extranet extends a private network (often referred to as an Intranet) to external parties in cases where both parties may be benefit from exchanging information efficiently and privately. [IRS]

Firewall | Telecommunication device used to regulate logical access authorities between network systems. [IRS]

Firmware | Microcode programming instructions permanently embedded into the Read Only Memory (ROM) control block of a computer system. Firmware is a machine component of computer system, similar to a computer circuit component. [IRS]

Identity | A set of attributes that uniquely describe a person within a given context. [NIST]

Information System | A collection of computer hardware, software, firmware, applications, information, communications, and personnel organized to accomplish a specific function or set of functions under direct management control. [IRS]

Integrity | Protection of information systems and information from unauthorized modification; determining quality, accuracy, completeness, non-repudiation, and authenticity of information. [IRS]

Internet | Two or more networks connected by a router; the world's largest network using TCP/IP to connect government, university, and commercial organizations. [IRS]

Intranet | A private network using TCP/IP, the Internet and world-wide-web technologies to share information efficiently and privately between authorized user communities, including organizations, vendors, and business partners. [IRS]

Key | Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information. [IRS]

Least Privilege | A security principle stating users or processes are assigned the specific restrictive set of privileges required to perform routine job responsibilities. [IRS]

Malicious Code | Rogue computer programs designed to inflict a magnitude of harm by diminishing the confidentiality, integrity and availability of information systems and information. [IRS]

Management Controls | Security controls focused on managing organizational risk and information system security, and devising sufficient countermeasures or safeguards for mitigating risk to acceptable levels. Management control families include risk assessment, security planning, system and services acquisition, and security assessment. [IRS]

Network | An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at a point between the parties (e.g., Claimant, Verifier, CSP or RP). [NIST]

Node | A device or object connected to a network. [IRS]

Password | A secret that a Claimant memorizes and uses to establish his or her identity. Passwords are typically character strings. [NIST]

Penetration Testing | A testing method where security evaluators attempt to circumvent the technical security features of the information system in efforts to identify security vulnerabilities. [IRS]

Personal Identifying Information (PII) | PII means information that alone or in conjunction with other information identifies an individual, including an individual's:

- name, social security number, date of birth, or government-issued identification number;
- mother's maiden name;
- unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
- unique electronic identification number, address, or routing code; and
- telecommunication access device as defined by Section 32.51, Texas Penal Code.

[Section 521.002, Texas Business and Commerce Code]

Plan of Action and Milestones (POA&M) | A management tool used to assist organizations in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in programs and systems. The POA&M arises from state organization conducted internal inspections and highlights corrections arising from the state organization conducted internal inspection. (Defined in OMB Memorandum 02-01). [IRS]

Private Key | The secret part of an asymmetric key pair that is used to digitally sign or decrypt data. [NIST]

Privileged User | A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. [NIST]

Protected Health Information (PHI) | HIPAA defines Individually Identifiable Health Information (IIHI) as information, including demographic data collected from an individual, that:

1) is created and received by a health care provider, health plan, employer or clearing house, and relates to
   - The individuals past, present, or future physical or mental health or condition
   - The provision of healthcare to that individual, or
   - The past, present, or future payment for the provision of healthcare to the individual; and
2) identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual

Protected Health Information (PHI) refers to any IIHI that is maintained or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, paper, or oral. There are certain exceptions such as for employment records held by a covered entity in its role as employer.

Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above. For example, a medical record, laboratory report, or hospital bill would be PHI because each document would contain a patient's name and/or other identifying information associated with the health data content. Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. If such information is listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI. [HIPAA]

Public Key | The public part of an asymmetric key pair that is used to verify signatures or encrypt data. [NIST]

Public Key Certificate | A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key. See also [RFC 3280]. [NIST]

Public Key Infrastructure (PKI) | A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. [NIST]

Risk Assessment | The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that could mitigate this impact. Part of Risk Management and synonymous with Risk Analysis. [NIST]

Risk Management | The routine process of identifying, analyzing, isolating, controlling, and minimizing security risk to achieve and maintain an acceptable risk level. A risk assessment is an instrumental component of the risk management life cycle. [IRS]

Risk | The potential adverse impact to the operation of information systems affected by threat occurrences on organizational operations, assets and people. [IRS]

Role-Based Access Control | Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. [NIST]

Security Policy | The set of laws, rules, directives and practices governing how organizations protect information systems and information. [IRS]

Security Requirement | The description of a specification required to enforce the security policy. See *Baseline Security Requirements*. [IRS]

Symmetric Key | A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to analyze the code. [NIST]

Token | Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to accredit the Claimant's identity. [NIST]

Virus | A self-replicating, malicious program that attaches itself to executable programs. [IRS]

Vulnerability Assessment | Systematic scrutiny of an information system to determine its' security posture, identify control deficiencies, propose countermeasures, and inspect the operating effectiveness of such security countermeasures after implementation. [IRS]

Vulnerability | A known deficiency in an information system that threat agents can exploit to gain unauthorized access to sensitive or classified information. [IRS]