**SYSTEM SECURITY PLAN (SSP)**



**CALIFORNIA DEPARTMENT OF TECHNOLOGY (CDT)**

*This System Security Plan (SSP) serves as the solution blueprint and allows CDT to perform a high-level assessment for quality assurance prior to launch. The SSP is not intended to substitute existing IT Security compliance requirements.*

**Table of Contents**

[1. NIST Security Control Families 3](#_Toc189493925)

[2. System Identification Information 4](#_Toc189493926)

[3. Information System Owner 4](#_Toc189493927)

[4. Information System Contacts 4](#_Toc189493928)

[5. System Operational Status 6](#_Toc189493929)

[6. Information System Type 6](#_Toc189493930)

[7. Operational Support Level 7](#_Toc189493931)

[8. System Description and Purpose 7](#_Toc189493932)

[9. System Environment 8](#_Toc189493933)

[10. System Physical Location 8](#_Toc189493934)

[11. System Information/Components 9](#_Toc189493935)

[12. Categorization of Information and Systems 10](#_Toc189493936)

[12.1. Security Objectives 10](#_Toc189493937)

[12.1.1. Confidentiality 10](#_Toc189493938)

[12.1.2. Integrity 10](#_Toc189493939)

[12.1.3. Availability 11](#_Toc189493940)

[12.1.4. System Security Categorization 11](#_Toc189493941)

[13. SYSTEM AND DATA CLASSIFICATION 12](#_Toc189493942)

[13.1. Privacy Threshold Assessment 12](#_Toc189493943)

[13.2. Information Classification 13](#_Toc189493944)

[14. Cloud Information Systems Architecture Standard (CISAS) 14](#_Toc189493945)

[15. Network Architecture and System Environment 17](#_Toc189493946)

[15.1. System Confidential Data transfer inventory 18](#_Toc189493947)

[15.2. User Community Organizations and Access 18](#_Toc189493948)

[16. System Interconnection/Information Sharing 20](#_Toc189493949)

[16.1. System Inputs and Outputs – Not Applicable 20](#_Toc189493950)

[16.2. System Interconnections 21](#_Toc189493951)

[16.3. Documentation of Untrusted Connections 22](#_Toc189493952)

[17. Information System Security Plan Completion Date 23](#_Toc189493953)

[18. Information System Security Plan Approval Date 23](#_Toc189493954)

[19. Information System Recovery Plan Approval Date 23](#_Toc189493955)

[20. Appendix 24](#_Toc189493956)

# NIST Security Control Families

There are three general classes of security controls (i.e., management, operational, and technical). Each family contains security controls related to the security function of the family. A standardized, two-character identifier is assigned to uniquely identify each control family.

| **CLASS** | **FAMILY** | **IDENTIFIER** |
| --- | --- | --- |
| Management | Risk Assessment | RA |
| Management | Planning | PL |
| Management | System and Services Acquisition | SA |
| Management | Certification, Accreditation, and Security Assessments | CA |
| Operational | Personnel Security | PS |
| Operational | Physical and Environmental Protection | PE |
| Operational | Contingency Planning | CP |
| Operational | Configuration Management | CM |
| Operational | Maintenance | MA |
| Operational | System and Information Integrity | SI |
| Operational | Media Protection | MP |
| Operational | Incident Response | IR |
| Operational | Awareness and Training | AT |
| Technical | Identification and Authentication | IA |
| Technical | Access Control | AC |
| Technical | Audit and Accountability | AU |
| Technical | System and Communications Protection | SC |

# System Identification Information

Information System Name/Title

|  |  |
| --- | --- |
| Official System Name:  | [[system\_name]] |
| System Acronym: |  [[system\_acronym]] |

# Information System Owner

Identify the designated system owner for this system. This person is the key point of contact (POC) for the system and is responsible for coordinating system development life cycle (SDLC) activities specific to the system.

|  |  |
| --- | --- |
| Name: | ​ ​[[owner\_name]] |
| Title: | [[owner\_title]] |
| Entity: | [[owner\_entity]] |
| Address: | [[owner\_address]] |
| Contact information: | [[owner\_contact]] |
| Other: |  [[owner\_other]] |

# Information System Contacts

Add the Authorizing Official as well as other key personnel for this information system. The Authorizing Official has two roles:

1. The business owner, who is responsible for defining the [CDT] business Confidentiality, Integrity, Availability (CIA) requirements for the information system.
2. A technical owner who is responsible for implementing the necessary controls to preserve the CIA of the information assets.

Authorizing Official – Business Data Owner

List the Business Data Owner or action committee responsible for this system.

|  |  |
| --- | --- |
| Name: |  [[bdo\_name]] |
| Title: | [[bdo\_title]] |
| Phone number: |  [[bdo\_phone]] |
| Email: | [[bdo\_email]] |

Authorizing Official – Technical Owner

List the Technical Owner or action committee for the system.

|  |  |
| --- | --- |
| Name: |  [[to\_name]] |
| Title: | [[to\_title]] |
| Organization: | [[to\_org]] |
| Email: | [[to\_email]] |

Information System Security Officer

This person/group is responsible for the actual implementation of the required security controls. Usually this is the system administrator.

|  |  |
| --- | --- |
| Name: | [[isso\_name]] |
| Title: | [[isso\_title]] |
| Phone number: | [[isso\_phone]] |
| Email: | [[isso\_email]] |

Other Key Contacts

List any other critical subject matter experts (SME) or functions in the operation of this system. Ex. business analysts, system administrators, developers, etc.

|  |  |
| --- | --- |
| Name: |  [[okc\_name]] |
| Title: | [[okc\_title]] |
| Phone number: | [[okc\_phone]] |
| Email: | [[okc\_email]]  |

# System Operational Status

Indicate dates for all applicable lifecycle phases. If the system is under development or undergoing a major modification, include a schedule for the system design, development, implementation, and operational phases.

|  |  |
| --- | --- |
| Under development: | **[[status\_under\_dev]]** |
| Operational: | [[status\_operational]] |
| Major modification: | [[status\_major\_mod]] |
| Decommissioned: | [[status\_decom]] |
| Other: | [[status\_other]] |

# Information System Type

Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 8. [System Description and Purpose](#_System_Description_and).

|  |  |
| --- | --- |
| Major application: | [[type\_major\_app]] |
| General support system: | [[type\_gss]] |
| Major modification: | [[type\_major\_mod]] |
| Decommissioned: | [[type\_decommissioned]] |
| Other: | [[type\_other]] |

# Operational Support Level

Indicate the service level agreement (SLA) of the system.

|  |  |
| --- | --- |
| Support Level Agreement Information*SLA can be a separate document* | [[sla]] |

# System Description and Purpose

Describe the following:

1. Business function/process for the system.
2. Who the system serves.
3. Type of data it utilizes.
4. Third party (vendor) involvement with the system.
5. Describe the user’s level of access to system-related data (read-only, alter etc.)
6. # of users. Indicate internal or external.
7. Data classifications of assets
* The Alerton EnVision for BACTalk is a specialized building automation control system designed to monitor and manage facility equipment.
* It functions as a critical operational tool for building management, providing real-time monitoring and control capabilities.
* The system manages various building systems including HVAC, lighting, and security.
* It leverages the BACnet protocol to communicate with diverse building automation devices.
* The platform creates a unified interface for facility management.
* Alerton's solution combines the Envision for BACtalk operator workstation with WEBtalk functionality.
* It translates complex building system data into accessible information through intuitive graphical interfaces.
* This solution enables facilities staff to maintain optimal building performance.
* It allows implementation of energy management strategies and efficient response to system alerts.
* The jump server configuration provides secure connectivity to various internal network devices.
* The system maintains appropriate access controls for security.

|  |  |
| --- | --- |
| Business function: | [[business\_function]] |
| Who system serves: | [[who\_serves]] |
| Data type: | ​ [[data\_type]] |
| Third party: | ​​ [[third\_party]] |
| Level of access needed: | ​ [[level\_access]] |
| # of users/internal or external | [[user\_counts]] |
| Data classification levels |  [[data\_classification\_levels]] |
| Comments |  [[purpose\_comments]] |

# System Environment

Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

|  |  |
| --- | --- |
| System environment data: | [[environment]] |

# System Physical Location

Provide system location and description. If Cloud services provide system identifiers

|  |  |
| --- | --- |
| Location name/address: | [[location\_name]] |
| Description: | [[location\_description]] |
| Cloud services: | [[cloud\_services]] |
| Type, characteristics, service model, region, service provider: | [[cloud\_details]] |

# System Information/Components

Indicate a high-level asset inventory for each component of the system. Include Servers, Application Code or Modules, Network Equipment and any other component that is covered in this security plan.

| Components  | Server Names  | Description  | Function  |
| --- | --- | --- | --- |
| [[#components]][[component]] | [[server\_names]] | [[description]] | [[function]][[/components]] |

# Categorization of Information and Systems

The security categories are based on the potential impact on an entity should certain events occur which jeopardize the information and information systems needed by the entity to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. For the FIPS 199 system categorization, select the highest of the three impact ratings. Ex. if confidentiality is moderate impact, but integrity and availability are low impacts, the FIPS 199 categorization level is medium.

## Security Objectives

### Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

| Sensitivity Level of System Information | Impact Rating: Select one level |
| --- | --- |
| **High:** The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.**Moderate:** The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.**Low:** The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | **[[cia\_confidentiality]]**  |

### Integrity

Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

| Sensitivity Level of System Information | Impact Rating: Select one level |
| --- | --- |
| **High:** The unauthorized modification or destruction of information couldbe expected to have a severe or catastrophic adverse effect onorganizational operations, organizational assets, or individuals.**Moderate:** The unauthorized modification or destruction of informationcould be expected to have a serious adverse effect on organizationaloperations, organizational assets, or individuals.**Low:** The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. |  [[cia\_integrity]]  |

### Availability

Ensuring timely and reliable access to and use of information.

| Sensitivity Level of System Information | Impact Rating: Select one level |
| --- | --- |
| **High:** The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.**Moderate:** The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.**Low:** The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | [[cia\_availability]] |

### System Security Categorization

|  |  |
| --- | --- |
| FIPS 199 Categorization: Choose the highest CIA impact level.  | **[[fips199]]** |

# SYSTEM AND DATA CLASSIFICATION

## Privacy Threshold Assessment

Below is the Privacy Threshold Assessment used by [CDT]. The assessment tool allows the user to identify Personal Identifiable Information (PII); based on responses the user would then need to move into a full Privacy Impact Assessment. (*Please reference SIMM 5310-C for further assistance*.)

| Will the system collect, use, maintain or share any of the following types of personally identifiable information as it relates to an individual?1  | Yes | No |
| --- | --- | --- |
| Name, Former Name, or Alias [[pta\_name\_alias]] | [[pta\_name\_alias\_yes]]  | [[pta\_name\_alias\_no]] |
| Date of Birth  | [[pta\_dob\_yes]] | [[pta\_dob\_no]] |
| Social Security Number (SSN) | [[pta\_ssn\_yes]]  | [[pta\_ssn\_no]] |
| Truncated SSN | [[pta\_trunc\_ssn\_yes]]  | [[pta\_trunc\_ssn\_no]] |
| Driver’s License number or State Identification Card Number | [[pta\_dl\_stateid\_yes]] | [[pta\_dl\_stateid\_no]] |
| Financial Data (e.g., account number or credit card numbers, etc.) | [[pta\_financial\_yes]]  | [[pta\_financial\_no]] |
| Health Insurance Information (e.g., including policy number, subscriber identifier, medical ID, or any information in an individual’s application or claims history, including appeals records, etc.) | [[pta\_hii\_yes]]  | [[pta\_hii\_no]] |
| Medical Information (e.g., medical history, mental and physical condition, or medical treatment or diagnosis, etc.) | [[pta\_medical\_yes]]  | [[pta\_medical\_no]] |
| User ID, email address, password or security question and answer | [[pta\_auth\_yes]]  | [[pta\_auth\_no]] |
| Physical Description (including height, weight, etc. please specify) | [[pta\_physical\_yes]]  | [[pta\_physical\_no]] |
| Biometric Data (e.g., fingerprints, iris scans, DNA, photographic facial images etc.) | [[pta\_biometric\_yes]]  | [[pta\_biometric\_no]] |
| Education History | [[pta\_education\_yes]]  | **[[pta\_education\_no]]** |
| Other personal information (e.g., home address, email address, mother’s maiden name, home phone #, cell phone #, place of birth, etc.). Specify:  | [[pta\_other\_yes]]  | **[[pta\_other\_no]]** |

System owners must assign a classification to the information system. The overall system classification is determined by the data contained or processed by that system. Using the definitions in Appendix I, select the appropriate information classification and system security category.

## Information Classification

Specify the classification of data that will be contained within or processed by this system.

| Data Types defined in [CDT] Data Classification Standard(per SIMM 5305-A) | Yes  | No |
| --- | --- | --- |
| Public | [[ic\_public\_yes]]  | [[ic\_public\_no]] |
| Sensitive | [[ic\_sensitive\_yes]]  | [[ic\_sensitive\_no]] |
| Personal Identifiable Information (PII): information which can be used to distinguish or trace an individual’s identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual  | [[ic\_pii\_yes]]  | [[ic\_pii\_no]] |
| Other personal information (e.g., home address, email address, mother’s maiden name, home phone number, personal cell phone number, place of birth, etc.). Specify:  | [[ic\_other\_pi\_yes]]  | **[[ic\_other\_pi\_no]]** |
| Employee PII  | [[ic\_employee\_pii\_yes]]  | [[ic\_employee\_pii\_no]]  |
| Proprietary Information to [CDT]  | [[ic\_proprietary\_yes]]  | [[ic\_proprietary\_no]]  |
| System information (e.g., network routing tables, password files, and cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed, stored, or transmitted by the information system to ensure confidentiality, integrity, and availability.  | [[ic\_system\_info\_yes]] | [[ic\_system\_info\_no]] |
| Federal Tax Information (FTI), or State Tax or Non-Tax (STNT) | [[ic\_fti\_stnt\_yes]]  | [[ic\_fti\_stnt\_no]]  |
| Family Educational Rights and Privacy Act (FERPA) | [[ic\_ferpa\_yes]]  | [[ic\_ferpa\_no]]  |
| Health Insurance Portability and Accountability Act (HIPAA) | [[ic\_hipaa\_yes]]  | [[ic\_hipaa\_no]]  |
| Protected Health Information (PHI) | [[ic\_phi\_yes]]  | [[ic\_phi\_no]]  |
| Criminal Justice Information Services (CJIS) | [[ic\_cjis\_yes]]  | [[ic\_cjis\_no]]  |
| Personal Information for Research Purposes | [[ic\_research\_pi\_yes]]  | [[ic\_research\_pi\_no]]  |

# Cloud Information Systems Architecture Standard (CISAS)

The Cloud Information Systems Architecture Standard (ISAS) is intended to provide guidance consistent with policy and best practices in the areas of Cloud Networking, Identity and Access Management, Infrastructure Protection, Data Protection, Detection and Recovery. Each IaaS and PaaS implementation is required to comply with the below mentioned CISAS standard.

| Cloud Network |
| --- |

|  |
| --- |
| Architecture includes distinct zones to separate internal, external, and DMZ traffic.* **[[c14n\_zones\_dmz\_yes]] [[c14n\_zones\_dmz\_no]] [[c14n\_zones\_dmz\_na]] -[[c14n\_zones\_dmz\_notes]]**
 |
| Segments internal networks to limit damage, should a security incident occur.* **[[c14n\_perimeter\_yes]] [[c14n\_perimeter\_no]] [[c14n\_perimeter\_na]] -[[c14n\_perimeter\_notes]]**
 |
| Architecture deploys firewalls, routers, and other perimeter security tools which enforce network security architecture decisions.* **[[c14n\_mgmt\_not\_public\_yes]] [[c14n\_mgmt\_not\_public\_no]] [[c14n\_mgmt\_not\_public\_na]] -[[c14n\_mgmt\_not\_public\_notes]]**
 |
| With exception of HTTPS/API traffic, all management traffic does not traverse the public internet (example: no RDP/SSH traffic allowed over public internet).* **[[c14n\_ids\_ips\_siem\_yes]] [[c14n\_ids\_ips\_siem\_no]] [[c14n\_ids\_ips\_siem\_na]] - [[c14n\_ids\_ips\_siem\_notes]]**
 |
| Network traffic inspection inspected with IDS/IPS system with logs sent to SIEM.* **[[c14n\_zones\_dmz\_yes]] [[c14n\_zones\_dmz\_no]] [[c14n\_zones\_dmz\_na]] -[[c14n\_zones\_dmz\_notes]]**
 |
| Identity and Access Management  |
| Maintain an inventory of credentials with cloud including root email addresses, account IDs, and points of contacts.* **[[c14i\_cred\_inventory\_yes]] [[c14i\_cred\_inventory\_no]] [[c14i\_cred\_inventory\_na]] -[[c14i\_cred\_inventory\_notes]]**
 |
| Maintain a method of tracking configuration changes and viewing inventory and configuration history of cloud services. * **[[c14i\_config\_history\_yes]] [[c14i\_config\_history\_no]] [[c14i\_config\_history\_na]] -[[c14i\_config\_history\_notes]]**
 |
| Maintain a tiered IAM structure and apply restrictions on subordinate permissions (e.g., denying the removal of logging and security features, denying access to services that do not comply with regulatory requirements). * **[[c14i\_tiered\_iam\_yes]] [[c14i\_tiered\_iam\_no]] [[c14i\_tiered\_iam\_na]] -[[c14i\_tiered\_iam\_notes]]**
 |
| Restrict usage of superuser access (i.e., root users) to the creation of less-privileged users for role-based access and administrative actions that can only be performed with superuser access. * **[[c14i\_restrict\_root\_yes]] [[c14i\_restrict\_root\_no]] [[c14i\_restrict\_root\_na]] -[[c14i\_restrict\_root\_notes]]**
 |
| Require multi-factor authentication for all (1) privileged access, (2) user access to sensitive or confidential data, and (3) accounts representing official communications from state departments. * **[[c14i\_mfa\_all\_yes]] [[c14i\_mfa\_all\_no]] [[c14i\_mfa\_all\_na]] - [[c14i\_mfa\_all\_notes]]**
 |
| Configure fine-grained user permissions according to least privilege.* **[[c14i\_least\_priv\_yes]] [[c14i\_least\_priv\_no]] [[c14i\_least\_priv\_na]]**

 **-[[c14i\_least\_priv\_notes]]** |
| Ensure attempts to perform actions not permitted prompt notification of insufficient privilege and log to SIEM. * **[[c14i\_insufficient\_perm\_alert\_yes]] [[c14i\_insufficient\_perm\_alert\_no]] [[c14i\_insufficient\_perm\_alert\_na]] -[[c14i\_insufficient\_perm\_alert\_notes]]**
 |
| Maintain logical perimeters between production and non-production environments (e.g., development, test).  * **[[c14i\_env\_perimeters\_yes]] [[c14i\_env\_perimeters\_no]] [[c14i\_env\_perimeters\_na]] -[[c14i\_env\_perimeters\_notes]]**
 |
| Where feasible, programmatically generate temporary credentials instead of long-term credentials like passwords or access keys. * **[[c14i\_temp\_creds\_yes]] [[c14i\_temp\_creds\_no]] [[c14i\_temp\_creds\_na]]**

**- [[c14i\_temp\_creds\_notes]]** |
| Provide access to cloud services by federated authentication through a centralized identity management system.* **[[c14i\_federated\_auth\_yes]] [[c14i\_federated\_auth\_no]] [[c14i\_federated\_auth\_na]] -[[c14i\_federated\_auth\_notes]]**
 |
| Infrastructure Protection  |
| Limit resource exposure to the public internet to only those resources intended to be publicly accessible and protected accordingly, including deployment of endpoint defense capabilities in accordance with SAM Section 5355.* **[[c14f\_limit\_public\_yes]] [[c14f\_limit\_public\_no]] [[c14f\_limit\_public\_na]]**

**-[[c14f\_limit\_public\_notes]]** |
| Deploy Web Application Firewalls and/or Distributed Denial of Service protection services to protect public-facing applications.**• [[c14f\_waf\_ddos\_yes]] [[c14f\_waf\_ddos\_no]] [[c14f\_waf\_ddos\_na]]** **-[[c14f\_waf\_ddos\_notes]]** |
| Require authentication and authorization when accessing cloud-based resources even across dedicated network connections, except resources intended to be publicly accessible. * **[[c14f\_auth\_dedicated\_yes]] [[c14f\_auth\_dedicated\_no]] [[c14f\_auth\_dedicated\_na]] - [[c14f\_auth\_dedicated\_notes]]**
 |
| Utilize tools to programmatically scan for weak configurations, including identification and vulnerability assessment of public facing resources.  * **[[c14f\_scan\_configs\_yes]] [[c14f\_scan\_configs\_no]] [[c14f\_scan\_configs\_na]]**

 **- [[c14f\_scan\_configs\_notes]]** |
| Infrastructure deployed in HA configuration with DR Optional.* **[[c14f\_ha\_dr\_yes]] [[c14f\_ha\_dr\_no]] [[c14f\_ha\_dr\_na]] -[[c14f\_ha\_dr\_notes]]**
 |
| Employ deployment practices which replace running instances with new instances created from an updated configuration, rather than updating running instances. * **[[c14f\_immutable\_deploy\_yes]] [[c14f\_immutable\_deploy\_no]] [[c14f\_immutable\_deploy\_na]] -[[c14f\_immutable\_deploy\_notes]]**
 |
| Data Protection |
| Select and configure storage services according to data availability (i.e., resilience to system downtime) and durability (i.e., resilience to data loss) requirements, which may include replication across cloud service provider zones and/or regions.* **[[c14d\_storage\_avail\_dur\_yes]] [[c14d\_storage\_avail\_dur\_no]] [[c14d\_storage\_avail\_dur\_na]] - [[c14d\_storage\_avail\_dur\_notes]]**
 |
| Configure fine-grained data access policies.* **[[c14d\_data\_access\_policies\_yes]] [[c14d\_data\_access\_policies\_no]] [[c14d\_data\_access\_policies\_na]] - [[c14d\_data\_access\_policies\_notes]]**
 |
| Protect data at rest by employing SAM Section 5350.1 compliant encryption and/or tokenization methods to transform confidential, sensitive, or personal data into a form that is unreadable to unauthorized users. * **[[c14d\_encrypt\_at\_rest\_yes]] [[c14d\_encrypt\_at\_rest\_no]] [[c14d\_encrypt\_at\_rest\_na]] - [[c14d\_encrypt\_at\_rest\_notes]]**
 |
| Protect data in transit by employing SAM Section 5350.1 compliant encryption and/or tokenization methods to transform confidential, sensitive, or personal data into a form that is unreadable to unauthorized users. * **[[c14d\_encrypt\_in\_transit\_yes]] [[c14d\_encrypt\_in\_transit\_no]] [[c14d\_encrypt\_in\_transit\_na]] - [[c14d\_encrypt\_in\_transit\_notes]]**
 |
| Protect data encryption keys from unauthorized use by defining restrictive policies for key use that enforce the principles of least privilege and separation of duties (e.g., separate users with key administration permissions from users with key use permissions, separate applications that require permission to encrypt data from applications that require permission to decrypt data, require decryption requests to come from a trusted network path). * **[[c14d\_key\_mgmt\_sod\_yes]] [[c14d\_key\_mgmt\_sod\_no]] [[c14d\_key\_mgmt\_sod\_na]]- [[c14d\_key\_mgmt\_sod\_notes]]**
 |
| Employ SAM Section 5350.1 compliant encryption methods to protect data in transit outside trusted network boundaries, even across dedicated network connections to cloud service providers. * **[[c14d\_encrypt\_outside\_trusted\_yes]] [[c14d\_encrypt\_outside\_trusted\_no]] [[c14d\_encrypt\_outside\_trusted\_na]] - [[c14d\_encrypt\_outside\_trusted\_notes]]**
 |
| Employ encryption methods to protect data in transit even within trusted network boundaries. * **[[c14d\_encrypt\_inside\_trusted\_yes]] [[c14d\_encrypt\_inside\_trusted\_no]] [[c14d\_encrypt\_inside\_trusted\_na]] - [[c14d\_encrypt\_inside\_trusted\_notes]]**
 |
| Data location and compliance requirements align with state security policies.* **[[c14d\_data\_location\_policy\_yes]] [[c14d\_data\_location\_policy\_no]] [[c14d\_data\_location\_policy\_na]] -[[c14d\_data\_location\_policy\_notes]]**
 |
| Detection |
| Log cloud management events to centralized log storage for each cloud service provider, maintaining audit records in accordance with SAM Section 5335.2. * **[[c14t\_central\_logs\_yes]] [[c14t\_central\_logs\_no]] [[c14t\_central\_logs\_na]] - [[c14t\_central\_logs\_notes]]**
 |
| Log and forward API calls to SIEM solution.* **[[c14t\_api\_logs\_siem\_yes]] [[c14t\_api\_logs\_siem\_no]] [[c14t\_api\_logs\_siem\_na]] -[[c14t\_api\_logs\_siem\_notes]]**
 |
| Publish cloud logs to the Security Information and Event Management (SIEM) system operated by the California Department of Technology (CDT) Security Operations Center (SOC). * **[[c14t\_publish\_to\_soc\_yes]] [[c14t\_publish\_to\_soc\_no]] [[c14t\_publish\_to\_soc\_na]] - [[c14t\_publish\_to\_soc\_notes]]**
 |
| **Recovery** |
| Identification of requisite formats for transfer of data to state entity or subsequent service provider. * **[[c14r\_transfer\_formats\_yes]] [[c14r\_transfer\_formats\_no]] [[c14r\_transfer\_formats\_na]] - [[c14r\_transfer\_formats\_notes]]**
 |
| A defined transition period to enable a successful transfer of data from service provider to state entity. * **[[c14r\_transition\_period\_yes]] [[c14r\_transition\_period\_no]] [[c14r\_transition\_period\_na]] -[[c14r\_transition\_period\_notes]]**
 |
| Configures automated data backups and virtual machine snapshots across zones and/or regions, according to recovery time and recovery point objectives. * **[[c14r\_backups\_snapshots\_yes]] [[c14r\_backups\_snapshots\_no]] [[c14r\_backups\_snapshots\_na]] -[[c14r\_backups\_snapshots\_notes]]**
 |

# Network Architecture and System Environment

Include a detailed topology narrative and network connectivity diagram (network topology diagram) that clearly depicts the system boundaries, system interconnections, and key devices within it. (Note: this does not require depicting every workstation or desktop, but you must include an instance for each operating system in use, an instance for portable components (if applicable), all servers (file, print, web, database, application, etc.), as well as any networked workstations, firewalls, load balancers, routers, switches, multi-function devices, printers, etc.) If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote system boundaries by referencing the system security plan of other system(s) in the diagram. Provide a narrative consistent with a graphic that clearly lists and describes each system component.

|  |
| --- |
| Network Diagram attachment name: |
| [[%netdiag\_img]] |

## System Confidential Data transfer inventory

List all sources of confidential data within the system. Include both inputs and outputs, including web-based systems that accept user input.

|  |  |
| --- | --- |
| Name of transfer: | [[#transfers]][[name]] |
| Input or Output? | [[io]]  |
| Method of transfer: |  [[method]]  |
| Origination (system or user): |  [[origin]] |
| Destination IP, host, or physical address: |  [[dest]] |
| Frequency: |  [[frequency]] |
| Contact information: |  [[contact]][[/transfers]] |

## User Community Organizations and Access

Describe the level of access for any privileged system users. Include all system, service, and administrative accounts.

|  |  |
| --- | --- |
| User group: | ​​[[#users]][[group]]  |
| Organization: | [[org]]  |
| Internal/External: | [[internal]] |
| Component: |  [[component]] |
| Data access: | [[data\_access]]  |
| Facility access: | [[facility\_access]]  |
| IT resource access: | [[it\_access]][[/users]] |
|  |  |

# System Interconnection/Information Sharing

Note: NIST SP 800-47 defines a system interconnection as a “direct connection of two or more IT systems for the purpose of sharing information resources.”

## System Inputs and Outputs – Not Applicable

In the table below, please provide system inputs and outputs to include the following:

* System
* Data Exchanged
* Data Classification
* Method of Transfer
* Input or Output – Input into or output from the system
* Destination IP, host, or physical address
* Frequency
* Contact Information

**No data is being transferred**

Include all connections to other systems not governed by this security plan, including untrusted connections or connections to the internet that require protective devices as a barrier to unauthorized system intrusion.

**Not Applicable**

|  |  |
| --- | --- |
| System: |  [[#io]][[system]] |
| Description of data exchange: |  [[data]] |
| Data classification: |  [[classification]] |
| Method of transfer: |  [[method]] |
| Input or output: |  [[direction]] |
| Destination IP, host, or physical address: |  [[destination]] |
| Frequency: |  [[frequency]]  |
| Contact information |  [[contact]][[/io]] |

## System Interconnections

In the table below, list system connections and check the appropriate box as to whether each connection is/are government-to government (G2G), government-to-business (G2B), or government-to-citizen (G2C). Describe the controls to allow and restrict public access. If the connection is to another [CDT] system, indicate that the connection is trusted.

| **Connection (Sys ID # if [STATE ENTITY] system or description if external)**  | **G2G** | **G2B** | **G2C** | **Trusted Connection?**  |
| --- | --- | --- | --- | --- |
| [[#connections]][[desc]] | [[g2g]] | [[g2b]] | [[g2c]] | [[trusted]][[/connections]] |

##  Documentation of Untrusted Connections

**There are no untrusted connections**

**Not applicable**

Any connection to a system not under [CDT] control is considered an untrusted connection. All untrusted connections require documentation. Reference here and attach copies of all Interconnection Security Agreements (ISA) and Memoranda of Understanding (MOU)/Memoranda of Agreement (MOA) for provision of IT security for this connectivity. Other relevant State of California security plans may also be referenced. State if no agreement or contracts are required because the only interconnection is with other [CDT] systems. Ensure that all agreements contain the following:

|  |  |
| --- | --- |
| Name of system: |  [[#untrusted]][[name]] |
| Entity: |  [[entity]] |
| Type of interconnection: |  [[intertype]] |
| Agreement (ISA/MOU/MOA): |  [[agreement]]  |
| Date: |  [[date]] |
| FIPS 199 Category: |  [[fips]] |
| Authorizing Official: |  [[ao]] |
| Other: |  [[other]][[/untrusted]] |

# Information System Security Plan Completion Date

* Enter the completion date (If applicable) of plan**: [[completion\_date]]**

# Information System Security Plan Approval Date

* Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file: **[[approval\_date]]**

# Information System Recovery Plan Approval Date

* Enter the date the Information System Recovery Plan was approved and indicate if the approval documentation is attached or on file: **[[recovery\_approval\_date]]**

# Appendix