# CLOUD SYSTEM SECURITY PLAN (CSSP)

Department Logo Here

 ENTITY NAME

*The Cloud System Security Plan (CSSP) is a lightweight SSP that enables State entities to initiate their cloud journey(s) with confidence. The CSSP serves as the solution blueprint and allows CDT to perform a high-level assessment for quality assurance prior to launch. The CSSP is not intended to substitute existing IT Security compliance requirements.*

Contents

[CLOUD SYSTEM SECURITY PLAN (CSSP) 1](#_Toc149120245)

[**1.** **NIST Security Control Families** **3**](#_Toc149120246)

[**2. System Identification Information 3**](#_Toc149120247)

[**3. Information System Owner 4**](#_Toc149120248)

[**4. Information System Contacts 4**](#_Toc149120249)

[**5. System Operational Status 6**](#_Toc149120250)

[**6. Information System Type 6**](#_Toc149120251)

[**7. Operational Support Level 7**](#_Toc149120252)

[**8. System Description and Purpose 7**](#_Toc149120253)

[**9. System Environment 8**](#_Toc149120254)

[**10. System Physical Location 8**](#_Toc149120255)

[**11. System Information/Components 8**](#_Toc149120256)

[**12. Categorization of Information and Information System 9**](#_Toc149120257)

[**13. SYSTEM AND DATA CLASSIFICATION 11**](#_Toc149120259)

[13.1 Privacy Threshold Assessment 11](#_Toc149120260)

[13.2 Information Classification 12](#_Toc149120261)

[**14. Cloud Information Systems Architecture Standard (CISAS) 13**](#_Toc149120263)

[**15. Network Architecture and System Environment 16**](#_Toc149120264)

[15.1 System Confidential Data transfer inventory 16](#_Toc149120265)

[15.2 User Community Organizations and Access 17](#_Toc149120266)

[**16. System Interconnection/Information Sharing 17**](#_Toc149120267)

[16.1 System Inputs and Outputs 17](#_Toc149120268)

[16.2 System Interconnections 18](#_Toc149120269)

[16.3 Documentation of Untrusted Connections 19](#_Toc149120270)

[**17. Information System Security Plan Completion Date 20**](#_Toc149120271)

[**18. Information System Security Plan Approval Date 20**](#_Toc149120272)

[**19. Information System Recovery Plan Approval Date 20**](#_Toc149120273)

## **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:  | Click or tap here to enter text. |
| System Acronym: | Click or tap here to enter text. |

## **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: | Click or tap here to enter text. |
| Title: | Click or tap here to enter text. |
| Entity: | Click or tap here to enter text. |
| Address: | Click or tap here to enter text. |
| Contact information: | Click or tap here to enter text. |
| Other: | Click or tap here to enter text. |

## **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 [STATE ENTITY] 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: | Click or tap here to enter text. |
| Title: | Click or tap here to enter text. |
| Phone number: | Click or tap here to enter text. |
| Email: | Click or tap here to enter text. |

Authorizing Official – Technical Owner

List the Technical Owner or action committee for the system.

|  |  |
| --- | --- |
| Name: | Click or tap here to enter text. |
| Title: | Click or tap here to enter text. |
| Organization: | Click or tap here to enter text. |
| Email: | Click or tap here to enter text. |

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: | Click or tap here to enter text. |
| Title: | Click or tap here to enter text. |
| Phone number: | Click or tap here to enter text. |
| Email: | Click or tap here to enter text. |

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: | Click or tap here to enter text. |
| Title: | Click or tap here to enter text. |
| Phone number: | Click or tap here to enter text. |
| Email: | Click or tap here to enter text. |

## **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: | Click or tap here to enter text. |
| Operational: | Click or tap here to enter text. |
| Major modification: | Click or tap here to enter text. |
| Decommissioned: | Click or tap here to enter text. |
| Other: | Click or tap here to enter text. |

## **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: | Click or tap here to enter text. |
| General support system: | Click or tap here to enter text. |
| Major modification: | Click or tap here to enter text. |
| Decommissioned: | Click or tap here to enter text. |
| Other: | Click or tap here to enter text. |

## **Operational Support Level**

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

|  |  |
| --- | --- |
| Support Level Agreement Information*SLA can be a separate document* | Click or tap here to enter text. |

## **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

|  |  |
| --- | --- |
| Business function: | Click or tap here to enter text. |
| Who system serves: | Click or tap here to enter text. |
| Data type: | Click or tap here to enter text. |
| Third party: | Click or tap here to enter text. |
| Level of access needed: | Click or tap here to enter text. |
| # of users/internal or external | Click or tap here to enter text. |
| Data classification levels | Click or tap here to enter text. |
| Comments | Click or tap here to enter text. |

## **System Environment**

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

|  |  |
| --- | --- |
| System environment data: | Click or tap here to enter text. |

## **System Physical Location**

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

|  |  |
| --- | --- |
| Location name/address: | Click or tap here to enter text. |
| Description: | Click or tap here to enter text. |
| Cloud services: | [ ]  Yes [ ]  No |
| Type, characteristics, service model, region, service provider: | Click or tap here to enter text. |

## **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  |
| --- | --- | --- | --- |
| Operating System  | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Data Transmission Servers  | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Application Servers  | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Database Servers  | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Storage Area Network (SAN)  | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Access management  | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Other (specify)  | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

## **Categorization of Information and Information System**

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. |[ ]

#### 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 could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.  |[ ]
| **Moderate:** The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, 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.  |[ ]

#### 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. |[ ]

#### System Security Categorization

|  |  |
| --- | --- |
| FIPS 199 Categorization: Choose the highest CIA impact level.  | [ ]  High[ ]  Moderate[ ]  Low |

## **SYSTEM AND DATA CLASSIFICATION**

###  Privacy Threshold Assessment

Below is the Privacy Threshold Assessment used by [State Entity]. 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 | [ ]  | [ ]  |
| Date of Birth  | [ ]  | [ ]  |
| Social Security Number (SSN) | [ ]  | [ ]  |
| Truncated SSN | [ ]  | [ ]  |
| Driver’s License number or State Identification Card Number | [ ]  | [ ]  |
| Financial Data (e.g., account number or credit card numbers, etc.) | [ ]  | [ ]  |
| 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.) | [ ]  | [ ]  |
| Medical Information (e.g., medical history, mental and physical condition, or medical treatment or diagnosis, etc.) | [ ]  | [ ]  |
| User ID, email address, password or security question and answer | [ ]  | [ ]  |
| Physical Description (including height, weight, etc. please specify) | [ ]  | [ ]  |
| Biometric Data (e.g., fingerprints, iris scans, DNA, photographic facial images etc.) | [ ]  | [ ]  |
| Education History | [ ]  | [ ]  |
| Other personal information (e.g., home address, email address, mother’s maiden name, home phone #, cell phone #, place of birth, etc.). Specify: Click or tap here to enter text. | [ ]  | [ ]  |

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 [STATE ENTITY] Data Classification Standard(per SIMM 5305-A) | Yes  | No |
| --- | --- | --- |
| Public | [ ]  | [ ]  |
| Sensitive | [ ]  | [ ]  |
| 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  | [ ]  | [ ]  |
| 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: Click or tap here to enter text. | [ ]  | [ ]  |
| Employee PII  | [ ]  | [ ]  |
| Proprietary Information to [STATE ENTITY]  | [ ]  | [ ]  |
| 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.  | [ ]  | [ ]  |
| Federal Tax Information (FTI), or State Tax or Non-Tax (STNT) | [ ]  | [ ]  |
| Family Educational Rights and Privacy Act (FERPA) | [ ]  | [ ]  |
| Health Insurance Portability and Accountability Act (HIPAA) | [ ]  | [ ]  |
| Protected Health Information (PHI) | [ ]  | [ ]  |
| Criminal Justice Information Services (CJIS) | [ ]  | [ ]  |
| Personal Information for Research Purposes | [ ]  | [ ]  |

## **Cloud Information Systems Architecture Standard (CISAS)**

The Cloud Information Systems Architecture Standard (CISAS) 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. |
| Segments internal networks to limit damage, should a security incident occur. |
| Architecture deploys firewalls, routers, and other perimeter security tools which enforce network security architecture decisions. |
| With exception of HTTPS/API traffic, all management traffic does not traverse the public internet (example: no RDP/SSH traffic allowed over public internet). |
| Network traffic inspection inspected with IDS/IPS system with logs sent to SIEM. |
| Identity and Access Management  |
| Maintain an inventory of credentials with cloud including root email addresses, account IDs, and points of contacts. |
| Maintain a method of tracking configuration changes and viewing inventory and configuration history of cloud services.  |
| 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).  |
| 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.  |
| 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.  |
| Configure fine-grained user permissions according to least privilege. |
| Ensure attempts to perform actions not permitted prompt notification of insufficient privilege and log to SIEM.  |
| Maintain logical perimeters between production and non-production environments (e.g., development, test).   |
| Where feasible, programmatically generate temporary credentials instead of long-term credentials like passwords or access keys.  |
| Provide access to cloud services by federated authentication through a centralized identity management system. |
| 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. |
| Deploy Web Application Firewalls and/or Distributed Denial of Service protection services to protect public-facing applications. |
| Require authentication and authorization when accessing cloud-based resources even across dedicated network connections, except resources intended to be publicly accessible.  |
| Utilize tools to programmatically scan for weak configurations, including identification and vulnerability assessment of public facing resources.   |
| Infrastructure deployed in HA configuration with DR Optional. |
| Employ deployment practices which replace running instances with new instances created from an updated configuration, rather than updating running instances.  |
| 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. |
| Configure fine-grained data access policies. |
| 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.  |
| 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.  |
| 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).  |
| 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.  |
| Employ encryption methods to protect data in transit even within trusted network boundaries.  |
| Data location and compliance requirements align with state security policies. |
| Detection |
| Log cloud management events to centralized log storage for each cloud service provider, maintaining audit records in accordance with SAM Section 5335.2.  |
| Log and forward API calls to SIEM solution. |
| Publish cloud logs to the Security Information and Event Management (SIEM) system operated by the California Department of Technology (CDT) Security Operations Center (SOC).  |
| **Recovery** |
| Identification of requisite formats for transfer of data to state entity or subsequent service provider.  |
| A defined transition period to enable a successful transfer of data from service provider to state entity.  |
| Configures automated data backups and virtual machine snapshots across zones and/or regions, according to recovery time and recovery point objectives.  |

## **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: |
| *Please enter Network Diagram attachment name here* |

### 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: | Click or tap here to enter text. |
| Input or Output? | Click or tap here to enter text. |
| Method of transfer: | Click or tap here to enter text. |
| Origination (system or user): | Click or tap here to enter text. |
| Destination IP, host, or physical address: | Click or tap here to enter text. |
| Frequency: | Click or tap here to enter text. |
| Contact information: | Click or tap here to enter text. |

### User Community Organizations and Access

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

|  |  |
| --- | --- |
| User group: | Click or tap here to enter text. |
| Organization: | Click or tap here to enter text. |
| Internal/External: | Click or tap here to enter text. |
| Component: | Click or tap here to enter text. |
| Data access: | Click or tap here to enter text. |
| Facility access: | Click or tap here to enter text. |
| IT resource access: | Click or tap here to enter text. |

###

### Security Operations Center as a Service (SOCaaS)

Indicate if SOCaaS (provided by CDT) will be used in this environment. Click or tap here to enter text.

If not, please attach the exemption request required by **SAM 4983.1**

## **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

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

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.

|  |  |
| --- | --- |
| System: | Click or tap here to enter text. |
| Description of data exchange: | Click or tap here to enter text. |
| Data classification: | Click or tap here to enter text. |
| Method of transfer: | Click or tap here to enter text. |
| Input or output: | Click or tap here to enter text. |
| Destination IP, host, or physical address: | Click or tap here to enter text. |
| Frequency: | Click or tap here to enter text. |
| Contact information | Click or tap here to enter text. |

###  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 [STATE ENTITY] system, indicate that the connection is trusted.

| Connection (Sys ID # if [STATE ENTITY] system or description if external)  | G2G | G2B | G2C | Trusted Connection?  |
| --- | --- | --- | --- | --- |
| Click or tap here to enter text. |[ ] [ ] [ ]  Click or tap here to enter text. |

###  Documentation of Untrusted Connections

Any connection to a system not under [STATE ENTITY] 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 [STATE ENTITY] systems. Ensure that all agreements contain the following:

|  |  |
| --- | --- |
| Name of system: | Click or tap here to enter text. |
| Entity: | Click or tap here to enter text. |
| Type of interconnection: | Click or tap here to enter text. |
| Agreement (ISA/MOU/MOA): | Click or tap here to enter text. |
| Date: | Click or tap here to enter text. |
| FIPS 199 Category: | Click or tap here to enter text. |
| Authorizing Official: | Click or tap here to enter text. |
| Other: | Click or tap here to enter text. |

##

## **Information System Security Plan Completion Date**

* Enter the completion date (If applicable) of plan: Click or tap here to enter text.

## **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: Click or tap here to enter text.

## **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: Click or tap here to enter text.