# State of Nevada

***Information Security Committee***

# Standard

| Document ID | Title | Revision | Effective Date | Page |
|---|---|---|---|---|
| S.5.06.01 | Cloud Services | H | 05/09/2025 | 1 of 4 |

## 1.0 PURPOSE

Cloud services refer to any IT services that are provisioned and accessed from a cloud computing provider. This is a broad term that incorporates all delivery and service models of cloud computing and related solutions. The purpose of this standard is to ensure that cloud services used by the State of Nevada include appropriate controls to protect the information and computing environment of the State.

This standard is not to be misinterpreted as requiring any state agency to utilize cloud services.

## 2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

## 3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

## 4.0 RESPONSIBILITIES

The agency head and appointed Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

## 5.0 RELATED DOCUMENTS

NRS 603A, Security and Privacy of Personal Information
State Information Security Program Policy, 100
Data Sensitivity, S.3.02.02
Information Security Risk Analysis, S.3.07.01

## 6.0 STANDARD

6.1 Cloud Service Providers (CSPs) offering Infrastructure as a Service (IaaS) shall demonstrate or show proof of comparable controls and processes needed to meet FedRAMP certified requirements or Center for Internet Security (CIS) controls identified as applicable to IaaS service models in the current CIS Controls Cloud Companion Guide, as well as comply with applicable State and Federal security requirements for the information being collected, processed, transmitted, stored, destroyed, or interconnected.

6.2 CSPs offering Platform as a Service (PaaS) shall demonstrate or show proof of comparable controls and processes needed to meet FedRAMP certified requirements or CIS controls identified as applicable to PaaS service models in the current CIS Controls Cloud Companion Guide, as well as comply with applicable State and Federal security requirements for the information being collected, processed, transmitted, stored, destroyed, or interconnected.

6.3 CSPs offering Software as a Service (SaaS) or any other cloud service model not explicitly named in this standard shall demonstrate or show proof of comparable controls and processes needed to meet the current version of CIS controls identified as applicable to SaaS service models in the current CIS Controls Cloud Companion Guide, as well as

applicable State and Federal security requirements for data classification of the information being collected, processed, transmitted, stored, destroyed, or interconnected.

6.4 CSPs offering Function as a Service (FaaS) shall demonstrate or show proof of comparable controls and processes needed to meet the current version of CIS controls identified as applicable to FaaS service models in the current CIS Controls Cloud Companion Guide, as well as applicable State and Federal security requirements for the data classification of information being collected, processed, transmitted, stored, destroyed, or interconnected.

6.5 To assure the confidentiality, integrity, and availability of state data, the following requirements are considered minimum baseline for all Cloud services:

A. CSP data centers processing, transmitting, storing, or interconnecting State data in a cloud environment must be located within the continental United States. Staff and contractors may be located outside of the continental U.S. only for support of the underlying infrastructure, patching, and maintenance of systems. Data is adequately protected to ensure that no direct access to data is allowed. A formally documented, industry standard best practice risk analysis must be performed. This risk analysis must include data classification, data sensitivity, and mitigating controls.

B. Shared data elements shall be identified, and classification assigned per S.3.02.01. These data elements and classifications shall be formally documented by the agency.

C. Multi-factor Authentication (MFA) will be required for State employees and contractors when connecting from outside SilverNet to a cloud service that collects, processes, transmits, stores, or interconnects with state data. Devices that connect via a state-hosted virtual private network (VPN) connection, including EITS hosted VPN, meet this requirement.

D. Cloud services must enforce least-privilege access to data, based on access roles established or agreed to by the agency.

E. State data must be encrypted both at rest and in transit. In these cases, the agency should control and manage the encryption keys where possible.

6.6 The State agency will be responsible for assuring that all Federal, State and other interagency security agreements and requirements applicable to the information being collected, processed, transmitted, stored, destroyed, or interconnected are communicated to and met by the CSP.

6.7 Prior to authorizing use of a Cloud service, the agency shall conduct a formal risk assessment of the proposed connections utilizing agency risk management processes. The agency ISO shall use a risk-based approach and evaluate each CSP solution based on the classification of data, and probability vs impact of an event. This will include the agency processes associated with the CSP. The agency ISO shall use risk based analysis tools provided by the State CISO office, or equivalent industry best practice tools and documentation. This risk based evaluation shall be formally documented.

6.8 The agency shall promptly report to the agency ISO any material changes to the use of a CSP that would affect the risk based evaluation.

6.9 The agency ISO shall reserve the right to deny the use of a CSP by the agency, impose additional security requirements and processes, or require additional documentation based on the formal risk assessment of the CSP and related agency processes. These decisions must be supported by formal documentation based on industry best practice. Appeals to these decisions made by the ISO must be submitted by the agency via formal exception to the State CISO.

## 7.0 DEFINITIONS

**Cloud computing**: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

**Cloud service models**: There are currently four distinct service models for the cloud environment:

- **Infrastructure as a Service (IaaS)** is a cloud environment with computing resource such as virtual servers, storage, and network. The consumer uses their own software, including operating systems, middleware and applications. The underlying physical infrastructure is managed by the Cloud Service Provider (CSP).
- **Platform as a Service (PaaS)** is a cloud environment for development and management of consumer applications. It includes the infrastructure layer – virtual servers, storage and network – while tying in middleware and development tools to allow the consumer to deploy their applications. It is designed to support the complete development lifecycle while leaving the management of the physical infrastructure to the CSP.
- **Software as a Service (SaaS)** is a cloud computing solution that provides the consumer with access to a complete software product. The application resides on a cloud platform and is accessed by the consumer through a web interface or application program interface (API). The physical and virtual infrastructure, operating system, middleware and application are all managed by the CSP.
- **Function as a Service (FaaS)** is a cloud service that allows the consumer to develop, manage and run their application functionalities without having to manage and maintain any infrastructure that is required. The consumer can execute code in response to events that happen within the CSP or application without having to build out or maintain a complex underlying infrastructure.

## 8.0 RESOURCES

To assist in implementing this standard, additional information and resources are available at the following links:

CIS Controls and Cloud Companion Guide
https://www.cisecurity.org/controls/

Current list of FedRAMP Certified cloud providers
https://marketplace.fedramp.gov/index.html#/products?status=Compliant&sort=productName

American Institute of Certified Public Accountants (AICPA) SOC for Service Organizations

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html

## 9.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

**Approved By**

| Title | Signature | Approval Date |
|---|---|---|
| State Information Security Committee | Approved by SISC | 03/27/2025 |
| State Chief Information Security Officer (CISO) | Signature on File | 05/01/2025 |
| State Chief Information Officer (CIO) | Signature on File | 05/09/2025 |

**Document History**

| Revision | Effective Date | Change |
|---|---|---|
| A | 11/17/2016 | Initial release |
| B | 4/10/2017 | Change to Section 6.0.1 (D) |
| C | 3/29/2018 | Major revision to address implementation concerns |
| D | 12/26/2018 | Renumbering (134 to S.5.06.01) and compliance to ADA standards |
| E | 1/30/2020 | Revision to include FaaS model, CIS control references |
| F | 12/31/2020 | Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1). Other changes for consistency with State Information Security Program policy and practices. |
| G | 11/01/2023 | Major revision to address implementation concerns |
| H | 03/XX/2025 | Update to 6.5.A. |