State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
134	B	Cloud Hosting	05/12/2017	1 of 3

1.0 PURPOSE

Cloud computing is an enabler of business and information management in state government. However, an unmanaged cloud environment will create just the opposite situation. An enterprise governance standard is necessary in preventing a next generation of legacy systems. The following requirements will assist preventing a legacy environment in the future.

This standard is not to be misinterpreted as requiring any state agency to utilize Cloud Hosting.

2.0 SCOPE

This standard applies to all state agencies using Cloud Hosting within or for the Executive Branch of Nevada State Government.

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. The agency ISO and unit managers are responsible for disseminating this standard and implementation within their units.

5.0 RELATED DOCUMENTS

State Administrative Manual (SAM)
State Security Policies, Standards & Procedures
Agency / Department Policies, Standards & Procedures
http://admin.nv.gov/Documents/Policies/Procedures/

6.0 STANDARD

6.0.1 General Agency Management Requirements

A. A Cloud Service Provider (CSP) shall demonstrate or show proof of comparable controls and processes needed to meet FedRAMP certified requirements as well as comply with State Security Requirements.

B. Prior to authorizing a Cloud Hosted solution, agency management shall conduct a formal risk assessment of the proposed connections utilizing agency Risk Management

processes and completing the Cloud Hosting Assessment Worksheet available on the State information security standards webpage.

C. State agencies shall document this risk analysis and retain it for six years.

D. For Cloud Hosting systems installed prior to the standard effective date, the agency is required to "sunset" its system within a reasonable period of time if it does not comply or cannot be brought into compliance with Section 6.0.1 (A). The period prescribed is not greater than three years, with a preferential replacement cycle as soon as possible. An exception is required and filed via CBTAP for any current Cloud Hosting system that does not meet Standard 6.0.1 (A).

6.0.2 Terms of Use

A. Agencies are responsible to make sure the terms of use are in affect along with the appropriate agency computer use policies.

7.0 DEFINITION

Cloud computing is 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

8.0 RESOURCES

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

NIST Special Publication 800-145
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NASCIO Special Publication on Cloud Services
http://www.nascio.org/Content/Publications-View/PID/652/evl/0/CategoryID/40/CategoryName/Cloud-Services

Federal Information Security Modernization Act (FISMA)
https://www.dhs.gov/fisma

9.0 EXCEPTIONS/OTHER ISSUES

State of Nevada

Information Security Committee

Standard

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**	**Date**
State Information Security Committee	Approved by Committee	4/27/17
State Chief Information Security Officer (CISO)	Signature on File	5/11/17
State Chief Information Officer (CIO)	Signature on File	5/12/17

Document History		
Revision	**Date**	**Change**
A	11/17/16	Initial Release
B	04/10/17	Change to Section 6.0.1 (D)