State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
134	C	Cloud Hosting	03/29/2018	1 of 4

1.0 PURPOSE

Cloud computing is an enabler of business and information management in state government. However, an unmanaged cloud environment will create enormous risk to the State and its agencies. An enterprise governance standard is necessary to prevent a next generation of legacy systems and provide the best solution and/or business value to meet the ever changing demands of State of Nevada agencies as we move safely and securely into the next era of digital business systems/solutions.

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

This standard establishes a baseline security standard for the State of Nevada. Agencies with security requirements exceeding this standard are encouraged to adopt a separate standard containing those requirements. No agency may adopt a standard with lower requirements than this standard.

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 Information Security Consolidated Policy, Sections 4.4, 5.4.1, 5.4.3, 5.6
- Nevada Revised Statue (NRS) 603A

6.0 STANDARD

6.0.1 General Agency Management Requirements

A. Cloud Service Providers (CSPs) offering Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) shall demonstrate or show proof of comparable controls and processes needed to meet FedRAMP certified requirements as well as comply with applicable State

and Federal security requirements for the information being collected, processed, transmitted, stored, destroyed, or interconnected.

B. CSPs offering Software as a Service (SaaS) shall, at the minimum, demonstrate or show proof of comparable controls and processes needed to meet the current version of NIST SP 800-171 or SOC 2 Type 2, as well as applicable State and Federal security requirements for the information being collected, processed, transmitted, stored, destroyed, or interconnected.

C. The follow requirements are considered minimum baseline for all Cloud Hosted solutions:

1) CSP data centers, staff and contractors collecting, processing, transmitting, storing, or interconnecting State data in a cloud environment must be located within the continental United States.

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

3) Cloud Hosted solutions must enforce least-privilege access to data, based on access roles established by the agency.

4) Any sensitive information as defined in section 7.0 of this standard must be encrypted both at rest and in transit. In these cases, the agency must control and manage the encryption keys.

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

E. Prior to authorizing a Cloud Hosted solution, agency management and IT shall coordinate with EITS Network team to determine impact to SilverNet and Internet access, and network utilization. The agency and EITS Network must agree upon the final design prior to approval and implementation of the cloud solution.

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

G. For Cloud Hosting systems installed prior to the Standard current version 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 the applicable requirements in this Standard. The period prescribed is not greater than three years, with a preferential replacement cycle as soon as possible. An exception is required to be approved by the CISO and filed with OIS for any current Cloud Hosting system that does not meet the applicable requirements in this Standard.

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

Least Privilege: A security principle where the user is only granted the minimum permissions to systems or data to perform their assigned duties.

Multifactor Authentication: From NIST SP 800-53r4, "Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card."

S**ensitive information:** Any information or data containing Personal Information per NRS 603A.040, declared confidential per NRS 242.105, required by federal regulations or law, or otherwise classified by an agency as restricted to a limited number of personnel.

Silvernet: The computer networks owned, operated, or administered by the Department of Administration, Enterprise IT Services, Communication and Computing Unit (NRS 242.080). This includes all State government networks dependent upon Silvernet for Internet connectivity.

8.0 RESOURCES

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

NIST Special Publication 800-145 – Definition of Cloud Computing
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NIST Special Publication 800-171r1 - Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Revision 1
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.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

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/OTHER ISSUES

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	03/29/18
State Chief Information Security Officer (CISO)	Signature on File	03/29/18
State Chief Information Officer (CIO)	Signature on File	4/5/2018

Document History		
Revision	**Date**	**Change**
A	11/17/16	Initial Release
B	04/10/17	Change to Section 6.0.1 (D)
C	03/29/18	Major revision to address implementation concerns