State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S 5 04 04	Data Security Architecture	B	9/6/2018	1 of 2

1.0 PURPOSE

This establishes minimum security standards for the architectural protection of information technology (IT) applications, systems, and data.

2.0 SCOPE

This standard applies to any entity, regardless of physical location, that operates, manages, stores, or processes State information.

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 Program Policy – 100, Section 5.4

6.0 STANDARD

The core component of determining the appropriate security model to utilize is based on the data classification of the information being protected, requirements mandated by legal and regulatory governance, and the agency's willingness to accept risk.

6.1 Data Security Architecture

A. A risk analysis must be performed and approved by the agency's ISO before implementation of a new service, application, or system.

B. A separate, distinct, and complete security policy must be placed between data security layers with differing levels of trust. A single security policy filter may not be used for multiple data security layers.

C. Agency ISOs are responsible to ensure security policy filters are applied and functioning as required to protect State information.

7.0 DEFINITIONS/BACKGROUND

Data Security Layers: A security layer consists of a defined set of objects, components, or process, that requires the same level of trust.

Security Policy Filter: A hardware and/or software component that performs one or more of the following functions: (i) content verification to ensure the data type of the submitted content; (ii) content inspection, analyzing the submitted content to verify it complies with a defined policy (e.g., allowed vs. disallowed file constructs and content portions); (iii) malicious content checker

that evaluates the content for malicious code; (iv) suspicious activity checker that evaluates or executes the content in a safe manner, such as in a sandbox/detonation chamber and monitors for suspicious activity; or (v) content sanitization, cleansing, and transformation, which modifies the submitted content to comply with a defined policy. Some examples include:

1. Firewalls
2. Intrusion prevention services or systems
3. Access control configured to inspect for source host, destination host, and source and destination protocol and ports
4. Other security appliances specifically designed to inspect all communications between layers

8.0 RESOURCES

NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

NIST 800-53, AC-4 Supplemental Guidance on Security Policy Filters

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	Approval Date
State Information Security Committee	Approved by Committee	8/30/2018
State Chief Information Security Officer (CISO)	Signature on File	9/6/2018
State Chief Information Officer (CIO)	Signature on File	9/6/2018

Document History

Revision	Effective Date	Change
A	9/6/2018	Initial release
B	12/26/2018	Renumbering (115 to S 5 04 04) and compliance to ADA standards.