State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
128	A	Border Security	02/22/2018	**1** of **5**

1.0 PURPOSE

This standard is established to enhance the protection of agency internal networks.

2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State IT Security Policy, Section 2.0 Scope.

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

Information Security Program Policy 100 Rev C
Standard 144: Suspension of Services
EITS Standard 126: SilverNet Security Classifications
NRS 205, 603A

6.0 STANDARD

This enforces a 'defense in depth' approach that creates the need for multiple controls to protect internal systems.

6.0.1 FIREWALLS

A firewall is an organization's first line of segmentation against malicious activity that originates from outside the secure area of the business. A firewall system must be used at a site's dedicated connection to the Internet and between connections with other untrusted networks.

A. Firewall Systems

1) Agencies deploying firewall systems shall have a firewall administrative policy describing authorized and unauthorized use of their firewall system.

2) All firewall systems must fail in a closed state, not allowing any traffic to pass.

3) Firewall systems must be certified using common criteria by an independent reviewer.

4) The firewall system shall have the ability to support a "deny all services except those specifically permitted" design.

5) Firewalls will not allow an untrusted or semi-trusted node to initiate a connection directly to trusted nodes.

6) Firewalls shall have the ability to support complex access control for transit traffic in any direction.

7) Firewalls must support Network Address Translation (NAT) in IP v.4 environments.

8) IPv6 must be disabled on all firewall devices if the protocol is not in use.

B. Packet Capture

Firewalls must be capable of capturing relevant packet data for analysis and forensics.

C. System Management

1) The firewall administrator shall be formally trained in the secure configuration and management of their system.

2) If a firewall device uses any underlying Operating System (OS), this OS must be secured and regularly patched in accordance with agency and State security standards for server OS.

3) System administrators shall develop and adhere to procedures for the installation of patches and security fixes in a timely manner.

4) System administrators shall test their systems by performing periodic, non-destructive scans and other checks to detect security vulnerabilities, expected response and errors in configuration.

5) System administration features or privileged functions must be restricted to authorized administrators. Administrators must use secure protocols (cryptography) when not physically connected to the device.

6) All configuration changes will use the agency's documented change management process. If no process exists, a documented change management process must be created and used for configuration changes.

7) Separate test environments should exist to test configuration changes and code upgrades prior to deployment. When the upgrade is to repair a critical vulnerability or the test environment is not capable of representing the complexity of the production environment or adequately testing the conditions necessary, this at the discretion of the agency.

8) Configurations must be reviewed for unnecessary and incorrect data at least quarterly.

9) Firewalls must be deployed to protect state data between administrative network boundaries.

10) Firewalls shall use all AAA features for management of that system.

6.0.2 Server Security

Any device with the capability to receive initiated connections from the Internet must be placed behind a firewall that only allows the minimum necessary ports and protocols to accomplish the business needs, and must be actively monitored by the enterprise Intrusion Protection System (IPS).

6.0.3 Intrusion Prevention Systems (IPS)

1) IPS scans or response features shall not be directed at untrusted network nodes or directed at trusted nodes outside of their administrative domain without prior written approval.

2) Automated response to malicious events consisting of blocking traffic to State of Nevada resources, dropping traffic or manipulating content is permitted under the guidelines of Standard 144: Suspension of Network Services.

6.0.4 Email Security Systems

1) Email systems reachable via the Internet must be placed behind a network firewall system and IPS.

2) Email systems must specifically inspect email for malicious content and employ some form of blacklisting for senders or domains that are routinely responsible for the delivery of malware.

7.0 DEFINITIONS

AAA: Authentication, Authorization and Accounting**.**

ACLs (Access Control Lists): An access control list is a group of statements that defines a pattern

that would be found in an IP packet. Incoming packets are then scanned for a pattern that matches one defined in the list. A permit or deny rule associated with the pattern, determines whether the packet is allowed to continue to its destination or not.

Border Security: Security measures designed and implemented on systems, appliances and devices that face the Internet.

Common Criteria: The Common Criteria for Information Technology Security Evaluation, international standard (ISO/IEC 15408)

Complex access control: Able to manipulate traffic by source or destination address, protocol, or port or any combination of those identifiers in any direction.

Firewall system: A firewall system can be any device specifically engineered to shield a site, subnet or individual computer from protocols and services that can be abused from hosts outside the secure area of the business. Firewalls are usually located at a site's connection to the Internet, but may also be located to provide protection for a smaller collection of hosts, a single host, or subnet which has access to external networks.

Formally trained: Technicians and staff who have received advanced training in system, appliance or devices management from the vendors or certified third parties.

NAT (Network Address Translation): NAT translates between the internal address and the assigned registered internet address.

Trusted Nodes: A node that is within the boundaries of an administrative domain (AD) and is trusted in the sense that the admission control requests from such a node do not necessarily need a policy decision point (PDP) (RFC 2753).

8.0 EXCEPTIONS/OTHER ISSUES

Request for exception to the requirements of this IT Security Standard must be documented, provided to and approved by the State IT Security Committee and Chief Information Officer (CIO).

Approved By		
Title	**Signature**	**Date**
State IT Security Committee	Approved by Committee	02/22/2018
State Chief Information Security Officer	Signature on File	03/19/2018
State Chief Information Officer	Signature on File	04/05/2018

Document History		
Revision	**Date**	**Change**
(-)		Initial release.
A	2/22/2018	Major revision.