ADMINISTRATIVE POLICY

Network Security

POLICY STATEMENT

Nevada State University's (NS) electronic resources and infrastructure must be protected from unauthorized access that could result in loss of connectivity or information. This policy is designed to minimize potential exposure of the Nevada State University network and attached devices to unauthorized access.

REASON FOR POLICY

This policy defines the requirements for establishing the network security controls related to the Nevada State University computer and communication systems infrastructure.

PROCEDURES

Network Devices

Intranet Connection Security Criteria - computer systems shall meet security criteria including, but not limited to, having an acceptable firewall, user-authentication system, and user privilege control system before it can be connected to the Nevada State University intranet.

Internet Access - All Internet access using computers at Nevada State University must be routed through a firewall.

Public Internet Servers - Public Internet servers must be placed on segmented subnets to which public traffic is restricted by routers or firewalls.

Internal Network Device Passwords - Network devices including, but not limited to, switches, routers, and firewalls, must employ passwords or other access control mechanisms.

Network Configuration

Network Protocol Restriction - All inbound traffic must be protected by a firewall that permits only the necessary ports/protocols required by Nevada State University hosted servers or applications.

Log On Banners - For Nevada State University managed network equipment, logon screens shall display a notice indicating that the system may be accessed only by authorized users and unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution.

Network Diagram - A network diagram that illustrates campus network connectivity must be developed and maintained.

Communication Line Changes - Installation, moves, or removal of voice or data lines require prior approval from Information & Technology Services.

Wireless Vendor Defaults - All vendor default settings on wireless equipment must be changed.

Wireless Encryption - All secure wireless networks must be configured to encrypt network communications.

Firewalls

Approvals and Review - Firewall change requests must be approved by the Information Security Officer prior to being implemented unless the change is considered an emergency or necessary for the immediate resolution of a system/network outage.

Configuration Changes - All firewall changes must be tracked and/or documented and contain the following information: source IP/network or hostname; destination IP/network or hostname; service name or port(s) required; and purpose.

Configuration Backup - Firewall rule sets and configurations must be backed up as changes are made to alternate storage (not the same device).

External Connections - All in-bound Internet connections to Nevada State University internal networks must pass through a firewall.

Secured Subnets - Portions of the Nevada State University internal network that contain sensitive or valuable information must employ a secured subnet. Access to this and other subnets must be restricted with firewalls or other access control measures.

Default to Denial - Every connectivity path and service not specifically permitted is blocked by default by Nevada State University firewalls. The lists of currently approved paths, services and applications are to be documented and maintained.

Administrative Access - Administrator accounts should be carefully protected and changed when an individual with knowledge of credentials terminates employment with the institution.

CONTACTS

SUBJECT	CONTACT	PHONE	EMAIL
Primary Contact(s)	Brian Chongtai	702-992-2410	brian.chongtai@nevadastate.edu

DEFINITIONS

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

RELATED INFORMATION

HISTORY

Revised 8/5/24