State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.5.04.03	Remote Access	B	12/14/2018	1 of 4

1.0 PURPOSE

This standard provides for the basic security of devices and methods used to establish remote connections into the protected business network from untrusted networks.

2.0 SCOPE

This standard applies to all state agencies within 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

NRS 281.195 Use of Computers
State Information Security Program Policy 100, Section 5.4.2 Remote Access and Dial-In

6.0 STANDARD

6.1 Dedicated Access

Dedicated access will be allowed to state networks on a case-by-case basis. All requests to create or change current configurations to support access shall be submitted via the EITS Helpdesk at least 60 days in advance of the need.

6.2 Modem Use

Internet access via Dial-Up modem to or from State equipment is not permitted in any case. Dial-Up modem use between State of Nevada systems and any other system is subject to approval by the CISO.

6.3 Virtual Private Networks (VPN)

Virtual Private Networks generally fall into two categories, client-based and network-based. VPN technology is used to extend network services, virtually, across untrusted or semi-trusted networks. All VPNs shall meet the following standards:

A. Unauthorized users are not allowed access to internal networks.

B. All VPN connection services must be managed by State IT staff. Personal (non-business) VPN connections are not permitted.

C. Consult the Office of Information Security for the current list of acceptable encryption algorithms.

6.4 VPN Client-based Systems

A. VPN connections shall be disconnected after a reasonable amount of inactivity, determined by classification and risk.

B. Client VPN connections shall be terminated after 12 hours, regardless of activity.

C. All VPN users shall have personal firewalls installed and properly configured.

D. No VPN client connection that crosses network administration perimeters, inbound or outbound, shall be allowed local area network LAN access (client side – AKA split tunneling) while the tunnel is active.

E. Methods for authentication, authorization, and accounting must be used on any VPN client system.

F. Client systems must be centrally controlled by IT staff.

6.5 VPN Network-based Systems

A. VPN tunnels must encrypt the payload of each packet, providing confidentiality, data origin authentication, connectionless integrity, an anti-replay service, perfect forward secrecy, and limited traffic flow confidentiality.

B. IKE version 2 will be used if the equipment is capable. Purchases of equipment to support VPN terminations for IPSEC must support IKEv2.

C. Within State networks, equipment that terminates a VPN tunnel (peer) must be managed by the administrators of the network that the tunnel terminates within. Agencies creating binding agreements for VPN or network services may be exempt from this requirement, subject to approval by the CISO.

D. Agencies that create VPN tunnels to devices managed by another network provider shall isolate the equipment (nodes) that the remote entity connects to behind a firewall system. The remote entity nodes shall not be able to access other nodes within Silvernet through the tunnel. The segregated State nodes shall be strictly controlled by the firewall system, allowing only limited access to other Silvernet nodes (only as required).

6.6 Remote Control (remote session)

A. Unmonitored remote-control sessions are not permitted.

B. Remote control products may be restricted by managed security systems based on business need or possible malicious impact.

C. Remote control products used by an agency must be documented with the agency's ISO.

D. Use of permitted remote-control products must be approved by agency IT management. No personal remote-control products may be executed from Silvernet.

7.0 DEFINITIONS

Network Provider: The agency, group, or unit responsible for the allocation and management of network addresses on a day-to-day basis. This does not include LAN addressing (individual nodes).

Dedicated Access: Defined as access to the State of Nevada data communications network via any accepted method across dedicated communication circuits.

Dial-Up: Any connection made with a modem over plain old telephone system (POTS) public wiring.

Gateway: Any device, whether virtual or physical, that serves as an entrance to another network.

Remote Control (session): Includes but is not limited to the following kinds of connections:

1. A terminal emulator is a hardware device or program that makes a computer respond like a particular type of terminal. Typically, an emulator is provided when a popular hardware device becomes outdated and no longer marketed but legacy applications exist that still need to communicate with the older devices. The practice of using an emulator to make an older program work with a new end-use device is called terminal emulation. Windows HyperTerminal is an example of a VT100 terminal emulator.

2. A remote control program such as VNC, GoToMyPC, Dameware, Citrix, RDWeb, Skype, PCAnywhere, Netmeeting, Cisco WebEx, Google Chrome Remote Desktop or Teamviewer, allowing users to connect to a remote display system or share displays. It allows a user to view and access a computing 'desktop' environment not only on the machine where it is running but from anywhere on the Internet and from a wide variety of machine architectures as well as share displays and take control of remote displays ((for unauthorized or unauthenticated users)).

3. Remote system administration programs or plug-ins include programs such as Microsoft console, powershell, SecureCRT, telnet or putty (SSH).

Silvernet: The protected business network of the State of Nevada.

8.0 RESOURCES

N/A

9.0 EXCEPTIONS

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).

State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.5.04.03	Remote Access	B	12/14/2018	4 of 4

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	4/26/2018
State Chief Information Security Officer (CISO)	Signature on File	12/04/2018
State Chief Information Officer (CIO)	Signature on File	12/14/2018

Document History

Revision	Effective Date	Change
A	4/26/2018	Initial release
B	12/26/2018	Renumbering (140 to S.5.04.03) and compliance to ADA standards.