State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.5.04.02	Data Communications and Remote Connections	F	12/31/2020	1 of 5

1.0 PURPOSE

This standard establishes the minimum security requirements for devices and methods used to establish data connections.

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

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.

5.0 RELATED DOCUMENTS

State Information Security Program Policy, 100
Information Security Officer (ISO) Roles and Responsibilities, S.3.03.01
Border Security, S.5.04.01
Wireless Networks, S.5.08.01
Software Patch Management, S.6.03.01
Secure Software Configuration, S.6.05.01
Malware Defenses, S.6.08.01
Boundary Defense, S.6.12.01
Wireless Access Control, S.6.15.01

6.0 STANDARD

6.1 Data Communications Equipment Documentation and Control

A. System/Network Administrators shall maintain a current inventory of all data communications equipment, e.g., modems, communications lines, workstations, and related devices.

B. System/Network Administrators shall maintain network diagrams that document both the physical and logical connections between data communications and other computer equipment.

C. System/Network Administrators shall document all workstations, port assignments, and data communications configurations.

6.2 Data Communications Local Area Network (LAN) Access Security

A. The LAN Administrator shall employ the appropriate access controls of workstations and servers within their area of responsibility to prohibit unauthorized access.

B. Administrative consoles must have access control protection inherent in the operating system running on the device and shall be secured when not in use.

6.3 Dedicated Access

Dedicated access will be allowed to state networks on a case-by-case basis. All requests to create or change current circuit configurations to support this access shall be submitted to the Enterprise IT Services (EITS) Help Desk.

6.4 Dial-up Access

A. Agencies providing dial-up access shall use either an Authentication, Authorization, and Accounting (AAA) model, incorporating the Challenge Handshake Authentication Protocol (CHAP), or the device granting access must use a callback mechanism.

B. If a AAA server model is used, the user account database server must reside on a server device that is physically separate from the data circuit-terminating equipment (modem, modem server, or access server).

C. All Dial-Up accounts shall be reviewed at least each quarter and discontinued if no longer justified.

6.5 Modem Use for Dial-out

Computers connected to a state network shall not use modems to connect to a non-state Internet service provider (ISP).

6.6 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 connections. All VPNs shall meet the following standards.

A. It is the responsibility of agencies permitting VPN connections to ensure that unauthorized users are not allowed access to internal networks.

B. Only EITS-approved VPN clients or methods shall be used.

C. VPN tunnels shall use IPSEC encryption only.

D. All electronic transmissions must be encrypted using Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules.

6.7 VPN Requirements Specific to Client-based Systems

A. VPN tunnels shall disconnect the client after a reasonable amount of inactivity, determined by classification and risk.

B. Client VPN tunnels that remain open (connected) shall be terminated after 12 hours, regardless of activity.

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

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

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

6.8 VPN Requirements Specific to Network-based Systems

A. Within State networks, the network provider for the network that the tunnel terminates on is responsible for managing the equipment that defines, creates, secures, and maintains the tunnel.

B. 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).

C. All agencies sponsoring VPN tunnels must have applicable policy and/or guidelines addressing use of this technology.

6.9 Virtual Terminals

A. Established levels of access authorization shall protect login to virtual terminals.

B. User authentication challenges must be presented to anyone attempting access via virtual terminals.

C. Virtual terminal access to computers housing data classified as sensitive shall be secured by an AAA solution.

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

Virtual Terminals: Include but are 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 VT100 terminal emulator.

2. A remote control program such as PCAnywhere, Netmeeting or Reachout, allows users to connect to a remote display system. 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.

3. Remote system administration programs or plug-ins include programs such as Microsoft console.

4. Novell’s Rconsole or Rconj is another form of remote access and control.

5. Telnet is the main Internet protocol for creating a connection with a remote machine.

Wired Network: At least two computers communicating via a physical medium.

Wireless Network: Radio frequency (RF) networks; any frequency within the electromagnetic spectrum associated with radio wave propagation. Many wireless technologies are based on RF field propagation. The term Wi-Fi is also used to denote wireless networks. Wi-Fi is short for wireless fidelity and is meant to be used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc.

8.0 RESOURCES

Center for Internet Security (CIS), CIS Controls v7.1 Guide

Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules

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.5.04.02	Data Communications and Remote Connections	F	12/31/2020	5 of 5

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	11/19/2020
State Chief Information Security Officer (CISO)	Signature on File	11/24/2020
State Chief Information Officer (CIO)	Signature on File	11/30/2020

Document History

Revision	Effective Date	Change
A	5/09/2002	Initial release
B	11/25/2002	Addition of wireless information
C	2/28/2005	VPN added
D	1/22/2015	OIS biennial review, replaces standard 4.62
E	12/28/2018	Renumbering (129 to S.5.04.02) and compliance to ADA standards
F	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)