Responsible: Office of Information Technology

PURPOSE

This administrative procedure provides guidelines for Virtual Private Network (VPN) connections to the private network of the Washoe County School District ("District" or "WCSD").

PROCEDURE

1. General

    a. A Virtual Private Network (VPN) is a private communication network usually used to communicate over a public network.

    b. This administrative procedure applies to all District employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing Virtual Private Networks (VPN) to access the District's network; and to implementation of Virtual Private Networks (VPN) that are directed through an IPSec Concentrator, a device in which Virtual Private Network (VPN) connections are terminated.

    c. Approved District employees and authorized third parties (contractors, vendors, agents, etc.) may utilize the benefits of Virtual Private Networks (VPN), which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Procedure.

2. Responsibilities

    a. It is the responsibility of District employees and authorized third parties (contractors, vendors, agents, etc.) with Virtual Private Network (VPN) access privileges to the District's private network to ensure that the computer that they are connecting to the District's network has:

        i. Installed virus scanning software with current virus definition files;

        ii. Up to date operating system patches installed; and

        iii. Personal Firewall in place (hardware or software).

    b. It is the responsibility of employees with Virtual Private Network (VPN) privileges to ensure that unauthorized users are not allowed access to District internal networks.

c. Virtual Private Network (VPN) use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

d. When actively connected to the private network, Virtual Private Networks (VPN) will force all traffic to and from the individual's personal computer over the VPN tunnel: all other traffic will be dropped.

e. Dual (split) tunneling is NOT permitted; only one network connection is allowed. Dual Tunnel or a multiple-branch networking path is a tunnel that is split allowing some network traffic to be sent to the Virtual Private Network (VPN) server and other traffic is sent directly to the remote location without passing through the VPN server.

f. Virtual Private Network (VPN) gateways will be set up and managed by District network operational groups.

g. All computers connected to District internal networks via Virtual Private Network (VPN) or any other technology must use the most up-to-date anti-virus software.

h. Virtual Private Network (VPN) users will be automatically disconnected from the District's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

    i. A ping is a computer network tool used to test whether a particular host is reachable across an IP network by sending ICMP "echo request" packets to target host and listening for ICMP "echo response" replies.

i. The Virtual Private Network (VPN) concentrator is limited to an absolute connection time of 24 hours.

j. Users of computers that are not District-owned equipment must configure the equipment to comply with the District's Virtual Private Network (VPN) and Network policies and procedures.

k. Only Virtual Private Network (VPN) clients approved by the District's Office of Information Technology may be used.

l. By using Virtual Private Network (VPN) technology with personal equipment, users must understand their machines are a de facto extension of the District's network, and as such are subject to the same rules and regulations that apply to District-owned equipment (i.e., their machines must be configured to comply with Information Technology's

Security Policies.).

3. Enforcement

   a. Any employee found to have violated this procedure may be subject to disciplinary action as provided for in negotiated agreements. The employee may also be held financially liable for any cost incurred to District computer hardware or software. Unlawful activity may result in criminal prosecution.

   b. Any authorized third party found to have violated this procedure may have their Virtual Private Network (VPN) access terminated. The third party may also be held financially liable for any cost incurred to District computer hardware or software. Unlawful activity may result in criminal prosecution.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This Administrative Procedure reflects the goals of the District's Strategic Plan and complies/aligns with the governing documents of the District.

REVIEW AND REPORTING

1. This procedure and any accompanying documents will be reviewed bi-annually, in even numbered years.

REVISION HISTORY

Date	Revision	Modification
10/10/06	A	Adopted as CSI Procedure IT-P005
2/01/2007	B	Revised
2/22/2008	C	Revised, added definition of Ping
12/08/2016	1.0	Revised: converted to Administrative Procedure