State of Nevada VPN Service FAQs:

What is VPN and what can the service do for me? VPN is the acronym for Virtual Private Network. VPNs are created by encrypting the data between two points to create a “tunnel” between them. When these two devices or their subordinate devices share data, that data is encrypted between the pair of VPN servers, so that it cannot be intercepted and interpreted.

- A VPN system allows a user or group of users to interact with a private network through the public Internet as if they were part of the private network.
- You <u>must</u> have a connection to the Internet to run the VPN client. The VPN client runs over an existing Internet connection.

Where VPN is extremely powerful is when you use it to leverage your broadband connection speed to interact with sites within the statewide private network. If you have DSL, cable, wireless or T-1 connection to the Internet, you can use the VPN client to ‘join’ the private network and interact with the servers and services you require access to. A VPN client should not be considered a permanent connection. There is a 30-minute inactivity timeout on the system so that only those who are actively using it share the bandwidth. Additionally, there is a 12-hour session timeout; any VPN session will be disconnected after 12 hours.

If you are not IT savvy, you should seek assistance from your IT staff.

Who is eligible for the VPN service? This service is available to all State of Nevada Employees, contractors or official designees according to need and availability. <u>Users must be able to bill to a State of Nevada budget code</u>.

How much does it cost? Currently, the monthly rate per user ID is less than $10.00 a month. This rate may change after the conclusion of each legislative session.

What do I do if I believe the software is causing my machine to continually fault or fail? Contact your local network administrator or designated technical support for assistance with your PC. If EITS supplies your technical support at work, then please call the EITS helpdesk at (775) 684-4333.

What applications can I use? Virtually every IP-enabled application. The following applications have been tested and functioned normally (according to the speed of your connection) through the VPN:

✓Terminal Services (see caveats at bottom)
✓Hummingbird Host Explorer
✓Internet Browsers (Internet Explorer, Firefox, Chrome, Opera, etc.)
✓Outlook and Outlook Express
✓FTP Clients
✓Media Players
✓Remote Desktop (recommended for remote control) (see caveats at bottom)
✓Other Remote Control Products (PCAnywhere, VNC, etc.)

Is service guaranteed 24 X 7? Service is provided 24 hours a day, 7 days a week. Any planned disruptions in service will be announced via the Silvernet maintenance list server. In the unlikely event of a long service disruption (more than 5 days), accounts will be credited for the time the service was unavailable.

Can I use my personal firewall? Yes. Although you may require some additional configuration, we have tested most personal firewalls and they will work through the VPN (**see caveats**). Any additional configuration is the responsibility of the user. EITS requires use of a personal firewall for all VPN users as well as current virus protection software.

Can I use the client behind my corporate firewall? Yes, however, your firewall administrator may need to add certain permissions to permit key exchange and encapsulation protocols to pass from our VPN device to your client or you may need to use IPSEC over TCP/UDP transport mode; contact us first.

I use Internet connection sharing at home. Can I share my VPN connection? No. The client does not support Internet connection sharing.

Can I give the software to a fellow employee to use? No. The software or login information is not transferable to any other individual, party, or group.

Do I need a username and password? Yes. Username / password combinations will be assigned by EITS after the signed Software Instructions and Conditions form is received, unless you elect to use your EITS e-mail account for authentication.

Are there any special requirements for my device? The supported operating systems are:

- Windows
  1. 2000 & 2003
  2. XP
  3. Vista (both 64-bit and 32-bit)
  4. Windows 7 (both 64-bit and 32-bit)
- Linux
- Macintosh
- Apple iPhone and iPad
- Android phones and tablets

Can I login to my Microsoft Domain or Novell NDS from home and see my drives? Yes, network connectivity is established; however, client workstation and server options will need to be configured by your agency network administrators for rights and access. This type of access is not recommended, as shares and trees require more bandwidth than remote control products and if session connectivity is lost due to any problem on the Internet or your local PC or our system, you could lose work. You will need to request all necessary permissions for this on the VPN Host Access Request form.

Can I stay logged into the VPN all day? Yes, but there are session timeouts for inactivity. If your connection is inactive for more than 30 minutes (no data transferred) the system will log you out. Additionally, any session older than 12 hours, regardless of activity, will be logged out.

How do I log in? FIRST, you ENSURE your connection to the Internet is ACTIVE. The VPN works across your normal connection to the Internet whether via DSL, cable modem, wireless, or other. Then, you execute the VPN client, click connect, and enter your username/password combination.

Can I surf the Internet on my personal connection while the VPN is working? Only State employees have this access (contractors do not). **HOWEVER**, When connected to the VPN, **ALL** of your traffic will be directed through the State system. You must disconnect the VPN session if you wish to surf non-work related sites.

While logged on, can I use my local network printers while connected to the VPN? NO. When you connect to the VPN, you will lose your Local Area Network (LAN) connection, which means you won't be able to access your server or printers (unless you have a directly connected printer, via a printer cable). We do not permit split tunneling of your VPN connection.

What if I enter my password wrong? You have only three chances to enter your password. If you are using your EITS e-mail account for authentication to VPN, you can reset your password online at https://mail.state.nv.us/empowerid/mypassword. If you do not elect to use your EITS e-mail account for authentication or do not have one, you will need to call the EITS helpdesk to reset your password at (775) 684-4333.

What else should I know to use this service? You must read and understand the Nevada Revised Statutes that govern unlawful acts regarding computers and information services. These statutes (NRS 205.473 through 205.513) are available online at http://leg.state.nv.us/NRS/NRS-205.html#NRS205Sec473. You must also agree to and sign our user agreement.

OPEN CLIENT ISSUES

1. **Microsoft's Internet Connection Sharing (ICS) is not possible with the VPN client.**
2. **Networking clients change the environment of your PC. Most clients are designed for an uninterrupted physical connection. Please consult your network administrators prior to loading any networking clients on your home PC. The WAN group highly recommends Remote Desktop Connection or other remote control products for use through the VPN, to control your work PC from home.**
3. **One user's PC was rendered inoperable after client installation. It is possibly related to a pre-existing Microsoft VPN client. Please ensure that you remove any Microsoft VPN services or clients prior to loading the Cisco VPN client.**
4. **If you are using the Microsoft ISA Server as a proxy and a firewall, please consult Knowledge Base Article 812076 on Microsoft's support site. Additionally, you will need to contact us before your clients can connect through the ISA Server.**
5. **There is a confirmed problem with the McAfee Firewall on WinXP, when using the VPN client in IPSEC over TCP mode. Disabling the firewall causes the initialization of the client to halt the XP operating system. Setting the firewall to "Allow All" causes the same error. Only removing the firewall removes the problem. Additionally, the client will not connect via IPSEC over TCP with the Firewall enabled.**
6. **There are some home or office DSL and CABLE routers that do not permit more than ONE IPSEC connection at a time. If you are attempting to use more than ONE connection through these routers, the first person connected will be disconnected when the**

second person attempts to login. Please contact router vendors prior to purchasing a router, or request assistance from your vendor on how to circumvent this problem. We have only seen this with one router type so far and there is currently no workaround.

7. **Using the Internet while attached to the VPN may be slower at times than using the Internet while not connected. While connected, ALL of your traffic is directed through the State system.**
8. **You will have problems at home if you have bridging setup in Microsoft networking. That is, you have allowed a computer to use another computer as a gateway to the Internet. The VPN client will NOT work on a computer with bridging enabled.**
9. **For mobile devices, you cannot use the imbedded IPSEC VPN Clients; we have disabled their use. You must use the Cisco AnyConnect Secure Mobility client found in your app store or online market.**