STATE OF NEVADA VPN SERVICE FAQ

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 dependent devices share data, that data is encrypted from your remote network to the state network so that it cannot be intercepted and deciphered.

- 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 *must* have a connection to the internet to run the VPN client. The VPN client runs over an existing internet connection.

- If you have a work PC, the Enterprise IT Services Division (EITS) recommends using a remote desktop application while using VPN (e.g., Microsoft Remote Desktop) to connect remotely to your work PC.

VPN can be used to leverage your broadband connection speed to interact with sites within the statewide private network. If you have a DSL, cable, or wireless connection to the internet, you can use the VPN client to connect to SilverNet and interact with the servers and services that you access to perform your job. A VPN client should not be considered a permanent connection. There is a thirty-minute inactivity timeout on the system so that only those who are actively using it share the bandwidth. Additionally, there is a twelve-hour session timeout; any VPN session will be disconnected after twelve hours regardless of activity.

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

WHO IS ELIGIBLE FOR THE VPN SERVICE?

This service is available to all State of Nevada Employees and contractors according to need and availability.

HOW MUCH DOES IT COST?

There is currently no cost associated with the VPN service.

WHAT DO I DO IF I BELIEVE THE SOFTWARE IS CAUSING MY MACHINE TO CONTINUALLY FAULT OR FAIL?

Contact your agency IT for assistance with your PC.

WHAT APPLICATIONS CAN I USE?

Virtually every IP-enabled application.

IS SERVICE GUARANTEED TWENTY-FOUR SEVEN?

VPN service is available twenty-four hours a day, seven days a week. Any planned disruptions in service will be announced via the SilverNet maintenance listserv.

CAN I USE THE CLIENT BEHIND MY CORPORATE FIREWALL?

Yes, however, your firewall administrator may need to add permits. Our service is based on TLS, using TCP and UDP port 443.

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-issued state email account for authentication. Additionally, you must use a multi-factor authentication token software, applied to a separate mobile device (a cellphone) or a hardware fob. After logging in with your username and password, you will be required to accept the login via the second factor request to your phone or type in the six-digit code from the fob before the login will be complete and the session is created.

ARE THERE ANY SPECIAL REQUIREMENTS FOR MY DEVICE?

The supported operating systems are:

- ➢ Windows
- ➢ Linux
- ➢ Macintosh
- ➢ Apple mobile devices
- ➢ Android mobile devices
- ➢ Chromebook

CAN I LOGIN TO MY MICROSOFT DOMAIN 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. **This connectivity will require configuration on the user's or agency's side.**

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?

The EITS Service Desk will send you information on how to log into your VPN account once your account has been created. A working internet connection is required.

WHY CAN'T I REACH THE INTERNET WHILE THE VPN IS CONNECTED?

Only state employees may be permitted this this access by default (contractors are not). Please refer to the acceptable use policy for internet usage while connected to VPN.

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).

WHAT IF I ENTER MY PASSWORD WRONG?

After three attempts, you will be locked out. Your account will unlock automatically after fifteen minutes. If you are using your EITS-issued state email account for authentication to VPN, you can reset your password online at https://pwportal.nv.gov.

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 https://www.leg.state.nv.us/NRS/NRS-205.html#NRS205Sec473. You must also agree to and sign our user agreement.

CISCO ANYCONNECT CLIENT EXPORT RESTRICTIONS

Under US export and re-export controls, Cisco's unrestricted and Mass Market encryption solutions may be exported or re-exported to most government end users located in all territories except the embargoed destinations and countries designated as supporting terrorist activities. Countries listed in Part 746 of the US Export Administration Act (EAR) as embargoed

destinations requiring a license are Cuba, Iran, North Korea, Sudan, Syria and the Crimea Region.

WHAT CLIENT SHOULD I USE FOR MY MOBILE DEVICES?

For mobile devices, the only authorized client is the Cisco AnyConnect Secure Mobility client found in your app store or online market.

Revised 6/9/22