Virtual Private Network (VPN) Remote Access  UDOT 07A-04
Effective:  June 27, 2016               Revised: New

Purpose
To define the policy and procedures that help secure data protections and system access by proper authorization, set-up, and use of a Virtual Private Network (VPN) connection within the Utah Department of Transportation (Department).

Policy
Using the VPN is a privilege and is granted only with an approved VPN Certification Agreement. Department employees, contractors, consultants and third parties may request the use of a VPN connection. The VPN user will be required to sign a certification agreement. VPN users will be reviewed and verified at least annually for security, activity, and validity of use. Unused, misused, or invalid VPN connections will be deleted.

Only Department issued devices will be used for the VPN connection to the State Network by State employees. Contractors, consultants, or any third party users are obligated to meet security protocols and must agree to secure any device being used to the same security standards as are used for Department owned devices.

Individuals using the VPN are responsible to verify no unauthorized devices are used or unauthorized users access the State network through their device. Data copied, transferred, or removed from the State network must be protected and not distributed without authorization from the Department. Employees who violate this policy may be subject to discipline, up to and including termination. Contractors, consultants, or other third party users who violate this policy may be subject to contract termination and legal responsibility.

The Department Point of Contact (POC) conducts at a minimum, a yearly review of the Department’s VPN access users. A list of invalid, inactive, or high risk VPN accounts that need to be deleted, resulting from the review, is sent to the Department of Technology Services (DTS) to administer the deletion of such VPN access or account.

Notification is sent to the Department POC who notifies the VPN user if access is revoked to the VPN by DTS administration for any reason.
Background
VPN provides a way for an authorized employee, contractor, consultant, or third party to log into the State computer network and gain access to data and applications securely as if physically at work. VPN accomplishes this by encrypting network traffic to prevent unauthorized interception of data. It requires authorization and authentication via a username and password.

Definitions
Approved Authorizer
Employee: Their region director or group leader.
Contractor, consultant or third party: Their Department contract administrator’s director.

Authentication
This is a process that verifies who you are, typically through requiring entry of a valid user name and password.

Authorization
This is a process that verifies and controls what you are authorized to do and what information and applications you can access.

POC
This is the Department Point of Contact who approves VPN access and validates the requests by the Approved Authorizer. This role is assigned to the Director of Program Development.
Procedures
General Information
The processes and procedures for gaining access to the different aspects of VPN Remote Access Management are specified.

Requesting VPN Access
The VPN request and approval process begins with a user identifying a need for remote access to the State data systems or programs. The user must read the VPN Certification Agreement, sign it, and submit the agreement to their Approved Authorizer for approval and signature.

Upon signature from Approved Authorizer the user requests VPN access as follows:
1. Go to dts.utah.gov
2. Select "Get a Product/Service"
3. Click on "Remote Access VPN"
4. Click on "Order Now"
5. Follow the instruction to complete the VPN Request form
6. Click on the "Order Now" button located in the upper right hand corner
7. Answer the questions shown on the screen.

Authorizing VPN Access:
The DTS system manager sends an approve/deny request to the Department POC.

The POC authorizes VPN access by doing the following:
1. POC reviews the VPN request regarding the types of access desired.
2. POC contacts the Approved Authorizer and requests a copy of the signed VPN Certification Agreement.
3. The POC approves or denies the VPN request using the DTS request system.
4. An email is sent to the requestor by DTS notifying them that the VPN access has been authorized or denied.

Installing the VPN Client
DTS, if approved will send instructions to the new VPN user of how to install the VPN client on their Department issued device or other equally secure device.

There are two steps for the User:
1. Install the VPN client by following the instructions sent with the approval email.
2. Map network drives to the new VPN user’s PC. This step is accomplished by contacting the Department Help Desk for their assistance in completing the drive mapping.
Utah Department of Transportation
VPN CERTIFICATION AGREEMENT
(Virtual Private Network)

Utah Department of Transportation and Department of Technology Services approved devices or clients, as described in the VPN Request and Approval application process, can be used to connect to the State Network. All other devices are obligated to meet the same security standards as are used for State owned devices before connecting to the State Network.

I certify that I understand, agree with and will follow the following stipulations for the use of a VPN connection to the State IT network:

**Department Employees**
I certify that I will only use a Department issued PC device remotely to connect to the Department’s secure network.

**All Others**
I certify that as a contractor, consultant, or third party, using a personal or company device that the PC device I use is configured with an up-to-date firewall, anti-virus protection, and malware protection. Furthermore, if private or restricted data is being accessed or stored, then I certify I will utilize disk encryption software on my device. I understand that I am obligated to secure any PC device being used to the same standards as are used for State owned devices.

I agree that data I remove from the State network must be protected, and not released or distributed to outside parties without authorization from Department. I further understand I am responsible to guarantee no unauthorized users access the State network through my device.

Should private or restricted data be taken by unauthorized entities, I understand that I could be held liable, subject to legal action, or discipline including possible termination of contacts and/or employment.

VPN Applicant (Signature):____________________________ (Date):_____________

Approved Authorizer (Senior Leader):____________________ (Date):_____________