Title: ODU CAMPUS VPN ACCESS  
Reference Number: 05.4.4

Purpose
The purpose of this procedure is to define the process to obtain ODU Virtual Private Network (VPN) access. The intent is to provide secure remote access to sensitive data that is used to conduct university business.

The account request process for the VPN service follows standard University account management practices. Vendors and other users not directly associated with the University may request access through the guest account process.

Procedures & Related Information

The following procedures should be followed to acquire VPN access:

1. **Review Policy, Standards and get approval.**
   - Discuss the business need for remote access with your immediate supervisor or sponsor.
   - Review related VPN policy and standard.
     - Policies  
       • 3500 - Policy on the Use of Computing Resources
     - Standards  
       • 02.6.0 - Remote Access and Virtual Private Network Standard
       • 04.2.0 - Account Management Standard

2. **Complete the Online Account Request process.**
   - Submit an account request through the MIDAS web site.
   - Step by step procedure is available at [https://www.odu.edu/ts/access/monarchkey/online-account](https://www.odu.edu/ts/access/monarchkey/online-account)

3. **Enroll in the “Remote User Security Training” course.**
   - Log into Blackboard with your MIDAS ID and password ([www.blackboard.odu.edu](http://www.blackboard.odu.edu))
   - After logging in, go to [https://www.blackboard.odu.edu/webapps/blackboard/execute/courseMain?course_id=_131894_1](https://www.blackboard.odu.edu/webapps/blackboard/execute/courseMain?course_id=_131894_1)
   - Click on the Enroll button on the left side of the page. (Note: You may see a message that says the course does not allow self-enrollment. You can ignore this message.)
   - An e-mail will be sent to the course leaders requesting your enrollment. Once a course leader approves your enrollment, you will receive an e-mail telling you that you have been successfully enrolled.

4. **Take and Pass the “OCCS Remote User Security Training” course in Blackboard**
   - Log into Blackboard with your MIDAS ID and password ([www.blackboard.odu.edu](http://www.blackboard.odu.edu))
   - Click on the “Organizations” in the left-hand menu.
   - Click on the “Remote User Security Training” course.
   - Click on “Information” in the left-hand menu and read the information about taking the course.
   - Review all of the lessons and pass all quizzes in the course.

5. **Account Setup.**
   After your approved Online Account Request form has been received by ITS and you have completed the “OCCS Remote user Security Training” course in Blackboard, then your VPN account will be set up and synchronized with MIDAS. You will see the “Virtual Private Network” service under your account within the MIDAS “My Services” page.
6. Download, install and configure the GlobalProtect VPN client software on your workstation or mobile device.
   • Instructions for downloading and installing the VPN client (software) can be accessed online at:
     o [https://www.odu.edu/ts/software-services/vpnclient](https://www.odu.edu/ts/software-services/vpnclient)
     o Read and follow the installation/setup guide for your operating system.
   • Questions should be directed to the ITS Help Desk.
     o Phone: 757-683-3192
     o E-Mail: itshelp@odu.edu
   • Client Restrictions:
     o Devices must be running a supported operating system.
       • Windows 8.1 or newer
       • MacOS 10.12 or newer
       • Red Hat Enterprise Linux 7, CentOS 7, or Ubuntu 18.04 or newer
       • iOS 10.3 or newer
       • Android OS 6.0 or newer
     o Devices must have operating system updates enabled and must not be missing any critical patches.
     o Devices must have anti-virus software installed and enabled. (applicable only to desktop operating systems)
     o Devices must have a firewall installed and enabled. (applicable only to desktop operating systems)
   • Support for third-party VPN clients:
     o Third-party VPN clients such as the PPTP and LT2P tunneling protocols built-in to most current operating systems are not supported.