# Old Dominion University
# Technology Policies, Standards, Procedures and Guidelines

## Compliance Procedure

**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 standards.
     - **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 a "Virtual Private Network" account request through the MIDAS web site.
   - Step by step procedure is available at www.odu.edu/information-technology-services/midas/account-request

3. **Enroll in the "VPN Security Awareness Training" course.**
   - Log into Canvas with your MIDAS ID and password (canvas.odu.edu)
   - After logging in, go to canvas.odu.edu/enroll/7T6PNG
   - Click on the Enroll button. (Note: You may see a message that says the course does not allow self-enrollment. You can ignore this message.)
   - An email will be sent to the course leaders requesting your enrollment. Once a course leader approves your enrollment, you will receive an email telling you that you have been successfully enrolled.

4. **Take and pass the "VPN Security Awareness Training" course in Canvas**
   - Log into Canvas with your MIDAS ID and password (canvas.odu.edu)
   - In your Dashboard, Click on the "**VPN Security Awareness Training**".
   - Click on "Start Here," 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 "VPN Security Awareness Training" course in Canvas, 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:
     - www.odu.edu/information-technology-services/vpn/vpnclient
     - Read and follow the installation/setup guide for your operating system.

   - Questions should be directed to the IT Help Desk.
     - Phone: 757-683-3192
     - Email: itshelp@odu.edu

   - Client Restrictions:
     - Devices must be running a supported operating system. (See Palo Alto's Compatibility Matrix.)
     - Devices must have operating system updates enabled and must not be missing any critical patches.
     - Devices must have anti-virus software installed and enabled (applicable only to desktop operating systems).
     - Devices must have a firewall installed and enabled (applicable only to desktop operating systems).

   - Support for third-party VPN clients:
     - Third-party VPN clients such as the PPTP and LT2P tunneling protocols built-in to most current operating systems are not supported.

| **Policy References**<br><br>**ODU faculty, staff and students are bound by all applicable laws, policies, standards and procedures and guidelines. For reference, some frequently referenced documents are noted. This is a non-inclusive list and not intended to limit applicability of any other law or policy.** | |
|---|---|
| Policy Foundation: | Federal and State Law<br>Policy 3501 - Information Technology Access Control Policy<br>Policy 3505 - Security Policy |
| Related Standards: | 02.6.0 - Remote Access and Virtual Private Network Standard<br>04.2.0 - Account Management Standard |
| Related Procedures, Forms: | Universal Account Request Form |
| Related Guidelines: | None |
| Maintenance: | Information Technology Services |
| Effective Date: | March 4, 2019<br>Reviewed on an annual basis |
| Approved by: | ITS Policy Office<br>Approved March 7, 2019 |