

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 Campus VPN access. The intent is to provide remote access to sensitive data securely that is used to conduct university business.

ODU VPN Access requires Supervisor approval for Faculty and Staff. Vendors and other non-ODU customers require approval from an ODU sponsor to obtain ODU Campus VPN access. A sponsor can be a departmental director, assistant director, manager, dean and etc.

Procedures & Related Information

The following procedures should be followed to acquire VPN access:

- 1. Review Policy, Standards and get approval.**
 - Discuss the viability of remote access with your immediate supervisor or sponsor.
 - Review the VPN Policy and Standard.
Policy: <http://occs.odu.edu/policies/index.php>
[3500 - Policy on the Use of Computing Resources.pdf](#)
 - Standard:** <http://occs.odu.edu/policies/index.php>
[05.4.4 - Virtual Private Network Standard 2006.pdf](#)
- 2. Submit a Universal Account Request form.**
 - Obtain account request form from OCCS Customer Service Center desk or online at <http://occs.odu.edu/>. Click on **Computing**, then **Forms Online** and then click on " [Universal Account Request Form](#)".
 - Fill out the "Applicant Information" section of the form (Name, etc.)
 - Check "**Other**" for Accounts Needed and type in "**Campus VPN**"
 - Read, sign and date the "Acceptable Usage Statement"
 - Have the form signed by your Budget unit Director
 - Submit the form to the OCCS Accounts Manger as indicated on the form
- 3. Enroll in the "OCCS Remote User Security Training" course.**
 - Log into Blackboard with your MIDAS ID and password (www.blackboard.odu.edu)
 - Click on the "**My Professional Learning**" tab.
 - Type "**Remote User**" in the "Organization Search" window and click in the "**GO!**" button.
 - Click on the "**Enroll**" button to the right of the "Remote User Security Training" course.
 - Follow the on screen directions.
 - 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)
 - Click on the "My Professional Learning" tab.
 - Click on the "OCCS Remote User Security Training" course in the "My Organizations" window.
 - Review all of the lessons and pass all quizzes in the course
 - Record the VPN "Group ID" and "Group Password" presented in the VPN lesson of the course. You will need it to configure the VPN software on your workstation.
- 5. Account Setup.**

After your approved Universal Account Request form has been received by OCCS and you have completed the "OCCS Remote user Security Training" course in Blackboard, then your "Campus VPN" account will be set up and synchronized with MIDAS. You will see the Campus VPN account on your MIDAS "My Services" page.

Old Dominion University Technology Policies, Standards, Procedures and Guidelines

- 6. Download, install and configure the CISCO VPN Client software on your workstation.**
- The VPN client (software) and installation/setup instructions can be accessed at Student/Faculty/Staff Downloads:
 - <http://occs.odu.edu/hardwaresoftware/downloads/facstaff/facstaff.shtml>
 - **DOWNLOADS FOR STUDENTS, FACULTY/STAFF**
 - Download the client and installation/setup guide.
Note: The VPN client (software) and installation/setup guide for Vendors and non-ODU customers can be obtained from the sponsor.
 - Read and follow the installation/setup guide for your operating system
Note: You will need the "Group ID" and "Group Password" provided to you in the VPN lesson of the Remote User Security Training course.

 - Questions should be directed to the OCCS Customer Service Center.
 - Phone: 757-683-3192
 - E-Mail: OCCSHELP@odu.edu

 - Client Restrictions:
 - incompatible with most VPN clients from other vendors
 - incompatible with many personal firewalls. Firewalls may need to be specially configured, or turned off, when running the Cisco VPN client
 - incompatible with Windows Internet Connection Sharing (ICS incompatible with AOL 7.0 and AOL 8.0)

 - Non-Cisco VPN clients:

Windows VPN clients are not supported when the VPN concentrator is behind a natted device such as a hardware firewall. ODU's VPN concentrator is located behind a natted device.

Policy References

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 Policy 3505 Security Policy COV ITRM standard SEC501-01
Ⓜ Related Standards:	05.4.4 – Virtual Private network Standard
☐ Related Procedures, Forms:	Universal Account Request Form
① Related Guidelines:	None
✂ Maintenance:	Office of Computing and Communications Services
✓ Effective Date: April 21, 2008	Reviewed on an annual basis
☐ Approved by: Approved April 18, 2008	Rusty Waterfield Acting Assistant Vice President, Office of Computing and Communications Services