



## **OIT Security Office**

### **Virtual Private Network Access Request v3.0**

#### **Service**

This document outlines a service for accessing the University of the Pacific's network, PacificNet, by means of a Virtual Private Network (VPN) connection, within the Remote Access Policy of the University. The Remote Access Policy states: Remote access to the University will be appropriately provisioned and/or controlled to ensure required security.

#### **Definitions**

**Virtual Private Network (VPN):** A VPN creates a secure connection, called a tunnel, between a client computer and a VPN server. This connection is usually made over the Internet and, in that case, has the effect of extending PacificNet to remote users. Once connected, a user may access files and/or applications stored on central servers just as if the user's machine was connected directly to PacificNet on any Pacific campus. If a VPN is used on campus, the effect is to create an encrypted connection across PacificNet.

**Third (3<sup>rd</sup>) Party:** Any person, group or organization who is not directly employed by Pacific or who is under contract to provide goods and services. Examples include but are not limited to: Staff hired through a temporary agency, temp-casual employees, contracted vendors, and contracted service organizations.

#### **Service Terms and Conditions**

Approved faculty, staff and other Pacific community members may connect to PacificNet via VPN. VPN service is not currently available to students. Approvals must be obtained from the appropriate management at the Director level and above. VPN capability for individuals who are not employees of Pacific must also be approved by the University Security Officer through the 3<sup>rd</sup> Party Network Access Request process. 3<sup>rd</sup> Party Network Access Request forms can be found on the OIT website. VPN service requestors must have a demonstrated academic or business need to connect securely and/or to appear as a part of PacificNet. Use of this service in the performance of activities unrelated to the mission of the University is strictly prohibited.

VPN is a user managed service, which means that off-campus users of this technology are responsible for selecting an Internet Service Provider (ISP), coordinating installation with their ISP of any required software, and paying associated fees.

Additionally,

1. It is the responsibility of those with VPN privileges to prevent unauthorized access to PacificNet from their VPN connected computer.
2. Users will be authenticated through their PacificNet ID and password.
3. Users with VPN privileges may only use VPN client software obtained from the Office of Information Technology (OIT) or their local TSP (as provided by OIT).
4. All computers connected to PacificNet **must**:
  - a. Use the most current anti-virus protection. Users may access OIT's website ([www.pacific.edu/oit](http://www.pacific.edu/oit)) to obtain anti-virus software.
  - b. Keep computers updated with the latest critical operating systems patches
  - c. Use compatible firewall protection. More information regarding Cisco compatible firewalls are also listed on this site.
  - d. Not bridge PacificNet to another network using this VPN connection.
5. When remotely connected to PacificNet via VPN, off-campus users agree that they are subject to the same University rules and regulations that apply to on-campus usage. In particular, users must adhere to Pacific's Information Technology Policies including its Acceptable Use Policies (AUP) see Appendix 1.
6. To use VPN client software, computers must meet University configuration standards for machine hardware and VPN minimum requirements. See OIT's website for hardware and software configuration requirements.
7. VPN users will be disconnected from PacificNet after 15 minutes of inactivity. Pings or other artificial means used to bypass this time limit are strictly prohibited.
8. VPN absolute connection times are limited to 8 hours.
9. When actively connected to Pacific Net, VPN access will be limited to Pacific Net only. Users will not have the ability to browse the Internet, or use Pacific Net as a pass-through to sites on the Internet.
10. All requestors must read and agree to these terms and condition before a connection is granted.
11. Data collected, stored, backed up, processed or accessed using this service must be protected according to University policies and procedures.
12. **The storing of confidential university data on privately owned systems is strongly discouraged.**
13. Proper data removal/destruction procedure must be followed for off-campus systems at the end of employment, any contractual arrangement, or cessation of the individuals VPN service.
14. IT Security Office may annually review VPN requests for validation and audit purposes.

#### **Enforcement**

All individuals granted access to this VPN service must adhere to the service terms and conditions. If these terms and conditions are violated, VPN access will be revoked. Violations will also be reported to the users' management, which may lead to other disciplinary action up to and including termination for employees or legal action for non-employees.



**OIT Security Office**  
**Virtual Private Network Access Request v3.0**

**VPN Network Access Request Form**

<b>Instructions</b>	<ul style="list-style-type: none"> <li>• Complete the Personal Data Section</li> <li>• Read the service terms and conditions</li> <li>• Have your supervisor complete the Management Authorization section</li> <li>• Sign and date the form</li> <li>• Deliver signed request form to the Customer Support Center (CSC)</li> <li>• VPN access will not be granted until approvals are obtained</li> </ul>
<b>Personal Data</b> (Requestor to Complete)	<p><b>Personal Data:</b> Please Print      VPN Start Date: _____      VPN Expiration Date: _____</p> <p>Last Name: _____      First Name: _____      ID# 988 _____</p> <p>TITLE: _____      EXT: _____      CAMPUS: _____      STK SFO SAC  <small>(Circle One)</small></p> <p>EMAIL: _____ @pacific.edu      DEPT/SCHOOL: _____</p> <p><b>I have read the service terms and conditions and agree to abide by the policies outlined therein.</b></p> <p>Employee Signature: _____      Date: _____</p>
<b>Management Authorization</b>	<p><b>Supervisor's Authorization:</b></p> <p><b>I approve the access requested by the above employee. If the employee leaves the university or transfers to a different department, I will notify OIT to terminate VPN access.</b></p> <p>Print Last Name: _____      Print First Name: _____</p> <p>Approval Signature: _____      Date: _____      EXT: _____</p>
<b>IT Security</b> (Official Use Only)	<p><b>HEAT #</b> _____      Reviewed By: _____      Date: _____</p> <p><input type="checkbox"/> Scheduled for Review      Date: _____</p>