OIT Security Office

Third (3rd) Party Network Access & VPN Request Form – V1.0

Instructions: Read these policies and terms carefully. Sign and completed the section on page 3 indicating your agreement. Please note that both the end-user and the sponsoring Pacific unit/department must agree to these terms and conditions

Third Party and Virtual Private Network (VPN) Access Request

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 (3rd) 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 3rd Party Network Access Request process. 3rd 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) 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.

Data Access Agreement

Version 1.02

1) I understand and accept that being granted access to the University of the Pacific's (from now on referred to as Pacific) network and information systems involves my assuming considerable responsibility for maintaining the integrity and security of Pacific's data. I am responsible for the privacy and confidentiality of any Pacific data to which I have access. Such data may include but is not limited to the student, financial, medical, and personnel records.

2) I will comply with all related University of the Pacific policies, including its Acceptable Use Policy. I will comply with all the applicable federal and state laws, including but not limited to FERPA, HIPAA, ECPA, USA Patriot Act, TEACH Act, GLBA and SEVIS.

3) I will not share any Pacific data with any third party without the express authorization from the Data Steward/Information Owner AND Pacific's IT Security Office or the Chief Information Officer. I understand that providing unauthorized access to Pacific data or information is in violation of applicable state and federal laws, as well as Pacific's Information Technology Policies.

4) I agree to keep all Pacific data that I collect, store, back-up, process or otherwise access secure by following accepted practice for secure use. For example, proper utilization of screen blanking, idle system timeouts, password standards, data encryption, anti-virus software, secure document storage and the shredding printed outputs, etc.

5) I agree to return or destroy all Pacific data in my possession upon the cessation of access to Pacific systems. I agree to immediately notify Pacific if my stewardship of Pacific data or my system access has been, or might have been, compromised. In case of reasonable suspicion or actual threat, I will immediately contact the University of the Pacific Helpdesk at 209-946-7400.

6) For remote access, I agree to sign and be bound by the terms and conditions of Pacific's Virtual Private Network Service. (To be attached to this agreement)

7) I understand the term of access granted will be limited to the dates indicated in the access request form and is not to exceed six (6) months. Long term access, beyond a six (6) month term, may be requested by Pacific's sponsoring division/unit but must be fully documented, justified and submitted to the IT Security Office for review.

I understand that violating these terms and conditions may result in my access being revoked without notice and could include additional legal action.

3rd Party Network Access & VPN Request Form

Instructions

- Read the service terms and conditions
- Complete the 3rd Party Data Section
- Have your sponsoring department/unit complete the Pacific Sponsor Authorization section
- Sign and date the form
- Deliver signed request form to the Pacific Human Resources Department
- Network access will not be granted until approvals are obtained

3rd Party Data
(Requestor to Complete)

3rd Party Data: Please Print

Required Access Start Date: ____________________ ***Required*** Access Expiration Date: ____________________

COMPANY: ____________________ ADDRESS: ____________________

LAST NAME: ____________________ FIRST NAME: ____________________ PHONE: ____________________

TITLE: ____________________ ____________________ CAMPUS: (Circle all that apply) STK SFO SAC

EMAIL: ____________________ VPN ACCESS REQUIRED? (Circle one) YES / NO

I have read the service terms and conditions and agree to abide by the policies outlined therein.

SIGNATURE: DATE:

Pacific Sponsor Authorization

Sponsoring Department/Unit Authorization: Please Print

LAST NAME: ____________________ FIRST NAME: ____________________

DEPARTMENT / UNIT: ____________________ CAMPUS: (Circle all that apply) STK SFO SAC

I approve the access requested for the above 3rd Party. When the 3rd Party leaves the university, I will notify OIT to terminate network access.

APPROVAL SIGNATURE: DATE: EXT:

IT Security
(Official Use Only)

HEAT # ____________________ REVIEWED BY: ____________________ DATE: ____________________

□ SCHEDUELED FOR REVIEW DATE: ____________________

Appendix 1

Acceptable Use Policy

Revision approved by Academic Council, February 8, 2007, Administration, March 19, 2007

POLICY: The University's Computing and Communications Resources shall be used securely, respectfully, cooperatively in support of the University's Mission.

Definition: *Computing and Communications Resources* include all electronic technology used to store, copy, transmit, or disseminate visual, auditory, and electronic information as well as the information contained therein. This includes, but is not limited to, computers, networks, phones, fax machines, copiers, PDAs, cell phones and the information contained in them.

Support of the University's Mission

The University provides Computing and Communications Resources to faculty, students, staff and others solely for the purposes of supporting teaching, learning, scholarship, service and administration within the context of the University's mission.

1. The University is a non-profit, tax-exempt organization and, as such, is subject to a number of pieces of legislation regarding sources of income, political activities, use of property, etc. The University prohibits use of University information and University Computing and Communications Resources for commercial purposes or financial gain not authorized under University Policy, partisan political activities not part of a class assignment, and for any activity prohibited by law.
2. Incidental personal use of Computing and Communications Resources, within the guidelines of this policy, is considered appropriate. Such permissible incidental personal use does not include hosting, ASP (Application Service Provider), ISP (Internet Service Provider), WSP (Wireless Service Provider) or other services for third parties. Incidental personal use does not include activities for financial gain unless such activities are authorized under University Policy. Incidental personal use does not include the use of institutional data which may be contained in or extracted from institutional computing and communications systems. Personal use is not incidental if it incurs a direct cost to the University.
3. Use of Pacific's Computing and Communications Resources by students, living on campus, in support of approved experiential learning and/or in support of their duties as compensated employees is explicitly authorized, so long as such usage does not violate any part of this policy.

Secure Use

Users of University Computing and Communications Resources are responsible for taking appropriate steps to safeguard University and personal information, as well as University facilities and services.

1. Passwords and other authentication and authorization codes, cards or tokens assigned to individuals must not be shared with others. Authorized Users must not provide access to unauthorized users. Passwords should be chosen carefully to lessen the possibility of compromise. Users are responsible for all activity that takes place under their UserID(s).
2. Activity that may compromise the system integrity or security of any on or off-campus system is prohibited. This includes any type of unauthorized access or hacking.
3. Unauthorized monitoring of individual User activity, information and communications is prohibited. See the University's Computing and Communications Confidentiality Policy.
4. Users must ensure the security of restricted, confidential, proprietary, licensed, copyrighted or sensitive information entrusted to their care or that may come into their possession. Security includes, as appropriate, protection from unauthorized disclosure, modification, copying, destruction or prolonged unavailability. Unless approved by the University Security Officer, users must not store non-university personal identification numbers including, but not limited to, Social Security Numbers, Credit Card Numbers, or Drivers License Numbers on unsecured devices or media, for any period of time.

Respectful Use

University Computing and Communications Resources should be used in a manner that respects the rights of others.

1. Users must abide by all local, state and federal laws. This includes all applicable Copyright laws and license agreements, especially software license agreements.
2. Users must abide by the University's Policy Against Sexual and Other Unlawful Harassment. That Policy prohibits verbal and visual conduct of a harassing nature. Threatening, obscene or other offensive messages or graphics that would be deemed inappropriate in other contexts are prohibited.
3. Users must not attempt to represent themselves as someone else, mask their identity, or engage in computing or communication activities using another User's UserID or other electronic credentials. Use of University resources for illegal conduct is prohibited.

4. Users accessing off-campus systems must additionally abide by the rules, regulations and acceptable use policies of those external systems. Given that User action may reflect on the University or the User themselves, ethical behavior, courtesy, civility and good etiquette is highly recommended.
5. Users are prohibited from using the logos, word marks or other official symbols of The University of the Pacific without authorization from Pacific's Marketing and University Relations. This specifically includes any such usage in connection with electronic systems, services and communications, both internal and external. This does not include the usage on physical or electronic letterhead when used for official University business.

Cooperative Use
Users of University Computing and Communications Resources are expected to cooperate so that all Users may make maximum use of facilities and services in a shared environment.

1. The University provides Computing and Communications Resources to facilitate business and academic activities of the University. Incidental personal use must not interfere with University business and academic activities. This includes personal activities that use bandwidth, occupy storage space, or slow down processing of systems, networks, or other resources needed for University business and academic activities.
2. Users must not knowingly engage in activities that would impede the activities of others including the internal or external distribution of junk email (a.k.a. Spam), chain mail, viruses, worms, remote controllers or other malicious code, or other unofficial and/or unsolicited distributions, especially to persons you do not know.
3. Users should refrain from using sounds or visuals that may be disruptive to others in shared facilities.
4. Users may not connect any device to PacificNet or the phone system that compromises security or impacts performance for others. This includes, but is not limited to, the connection of wireless access points, switches, hubs, routers, or auto dialers, not authorized by the Office of Information Technology.
5. All Users share the responsibility of seeing that University Computing and Communications Resources are used securely, respectfully, cooperatively, ethically, and for their intended purposes. If policy questions arise or if suspected policy violations are encountered, Users should take no unilateral action, but must promptly notify and/or cooperate with the appropriate University officials. Contact ITsecurity@pacific.edu

Sanctions
It is the responsibility of each User to understand his or her privileges and responsibilities regarding Acceptable Use and to act accordingly. Users failing to abide by the University's Acceptable Use Policy (AUP) may be subject to corrective action up to and including, dismissal, expulsion, and/or legal action by the University. While technical corrective action, including limiting user activity or removing information, may be taken in emergency situations by authorized Information Technology staff, other corrective action, technical and/or non-technical, will be taken in accord with applicable University policies and procedures. In particular, students who violate this policy will be referred to Judicial Affairs for judicial review.