

15

VPN ACCESS REQUEST



date

USER INFORMATION

first name		last name	
phone #	room #	email	
project name		principal investigator	
employment status <input type="checkbox"/> paid <input type="checkbox"/> unpaid		computer platform <input type="checkbox"/> pc <input type="checkbox"/> Mac	

PLEASE READ

*VPN access is available for users with a demonstrated need that cannot be met through other connectivity options. Technical Services reserves the right to install campus-approved anti-virus software on approved machines prior to setup. Due to the fact that each VPN account compromises network security, **Technical Services reserves the right to refuse VPN access** if a user's connectivity needs can be met through other means (e.g., SSC Terminal Services).*

JUSTIFICATION

Please provide a specific description of why your offsite computing needs require VPN access and why these needs are not sufficiently met through SSC Terminal Services:

*VPN use is subject to the same policies as network use. Violation of University rules governing appropriate use of IT resources may result in loss of access privileges, University disciplinary action, and/or criminal prosecution. I have read and will abide by the **Guidelines for Appropriate Use of University Information Technology Resources** as listed on the back of this form.*

Employee Signature _____ Date _____

TECHNICAL SERVICES USE ONLY

tech. services approval: yes no tech: _____ doit static ip: _____

The following guidelines apply specifically to use of IT resources:

1. *General Guidelines*

Access to University IT resources is a privilege granted to members of the University community which carries with it the responsibility to use them for University related activities, exercising common sense and civility.

2. *Individual Responsibility*

Authorization for use of IT facilities is provided to each individual for his or her own use. No person may use an authorization which belongs to someone else. In many cases the University has obtained access to these resources exclusively for the use of members of the University community.

3. *Security*

The protection of University IT resources depends heavily on each user's careful handling of "keys" to these resources, since any account can serve as an entry point for theft, damage or unauthorized use. Users must protect the confidentiality of their personal identification codes and passwords and are expected to exercise reasonable care to ensure that others cannot use their accounts.

4. *Intellectual Property*

Illegal downloading, distribution, copying of copyrighted materials or other activities that violate copyright law are strictly prohibited.

5. *"Hacking"*

Persons may not obtain or use--or attempt to obtain or use--passwords, IP addresses or other network codes that have not been assigned to them as individuals or authorized for their use as University employees. Persons may not obtain--or attempt to obtain--unauthorized access to computer accounts, software, files, or any other University IT resources.

6. *Malicious Activity*

Persons may not alter or intentionally damage software or data belonging to someone else or interfere with another person's authorized access to IT resources. Users may not intentionally disrupt or damage University computers or networks in any way.

7. *Impersonation and Anonymity*

Users of University IT resources may not send electronic messages with the sender's identity forged or send anonymous messages unless the recipient has agreed to receive anonymous messages.

8. *Commercial, Political, and Non-University Activities*

Persons may not use University IT resources to sell or solicit sales for any goods, services or contributions unless such use conforms to UW-Madison rules and regulations governing the use of University resources. University employees may not use these resources to support the nomination of any person for political office or to influence a vote in any election or referendum. No one may use University IT resources to represent the interests of any non-University group or organization unless authorized by an appropriate University department.

9. *De Minimus Usage*

In the interest of making the use of IT resources a natural part of the day-to-day learning and work of all members of the University community, incidental personal use is tolerated. However, one should use non-University sources of e-mail, Internet access, and other IT services for activities of an extensive nature that are not related to University purposes.

10. *State and Federal Laws*

Persons may not use University computing facilities to violate state or federal laws.

* as published in the University of Wisconsin System Administrative Code and UW-Madison policies. For example, disruption of University activities, damage to facilities, physical threat, theft or harassment as described in UWS 17 and 18; student academic misconduct in UWS 14; selling, peddling and soliciting in UWS 18; and ethical standards for use of facilities by faculty and staff in UWS 8.