

## **University of Utah Network Connection Acceptable Use Policy August 2001**

Network connectivity provided through the University of Utah Network, referred to hereafter as "the Network", either through a Web-Authenticated Network Access (WANA) connection or a Virtual Private Network (VPN) connection, is governed under the University of Utah Policy and Procedure 1-15 Information Resource Policy, and can be accessed at <http://www.admin.utah.edu/ppmanual/1/1-15.html>. The University of Utah Office of Information Technology (OIT) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University of Utah's network should be reported by calling the Campus Help Desk at 581-4000, or via e-mail at [helpdesk@utah.edu](mailto:helpdesk@utah.edu).

In compliance with state, federal, and international copyright and intellectual property rights laws, OIT takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property. OIT reserves the right to disconnect client machines where illegal or potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance. Access to remote networks using a University of Utah network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University of Utah Network connects. University of Utah network and computer resources are not to be used for personal commercial purposes.

Individuals connecting to the Network through a WANA port or VPN connection may not run server software, e.g., HTTP/Web server, SMTP server, FTP server, DHCP server, etc. Activation of these types of services is a direct violation of this agreement, and will result in termination of their connection to the Network. These users will be limited to TCP/IP protocol services only. For more information or clarification of these restrictions, please see <http://www.it.utah.edu/services/connected/wana.html>.

University of Utah departments or divisions connecting to the Network should refer to PPM 1-15 Information Resources Policy (<http://www.admin.utah.edu/ppmanual/1/1-15.html>) for policies governing their use of the Network.

Network traffic will be monitored for security through the University's Information Security Office (ISO) and for performance reasons through the OIT Network Operation Center (NOC). For more information on Network traffic monitoring, see the Network Monitoring Policy at <http://www.it.utah.edu/leadership/policies/NetworkMonitoring.pdf>.

Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

### **Campus Network Services Policy and Use Agreement**

Read the following policies before entering your password at the bottom of this form. By entering your password, you agree to act in accordance with the policies and guidelines of the Office of Information Technology (OIT). Failure to comply with these policies may result in the termination of your account.

For the remainder of this document, the term User refers to you, the person using the University Network ID (uNID) and services on the campus networks. A University Network ID is the combination of a username and a password whereby you gain access to University of Utah computer systems, services, e-mail campus networks, and the Internet.

### **I. Accounts and Passwords**

The User of a uNID guarantees that the uNID will not be shared with anyone else. In addition, the uNID will only be used for educational purposes. The User guarantees that the uNID will always have a password. The User will not share the password or uNID with anyone (not even family members). uNIDs will only be established for students, staff and faculty who are currently affiliated with the University.

uNIDs which are not active (no reading or sending of mail) during the semester (with the exception of Summer Semester) may be deleted during the following semester. Students, staff and faculty who leave the University will have their uNID and associated files deleted. No User will be allowed more than one uNID at a time.

### **II. Limitations on the use of resources**

OIT reserves the right to arbitrarily delete files or close the uNID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources. This includes the sending of unsolicited bulk e-mail messages.

### **III. Computer Ethics and Etiquette**

The User will not attempt to override or break the security of the University of Utah computers, networks, or machines/networks accessible therefrom. Services associated with the uNID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used.

Your uNID gives you access to e-mail, individual WWW pages, and campus computing resources. The use of these resources must comply with University policy and applicable Federal and State Law. Such electronically available information (1) may not contain copyrighted material or software unless the permission of the copyright owner has been obtained, (2) may not violate University policy prohibiting sexual harassment, (3) may not be used for commercial purposes, (4) should not appear to represent the University of Utah without appropriate permission, or to represent others, (5) may not appear to represent other organizations or companies, (6) may not contain material which violates pornography laws, or algorithms or software which if transferred violate United States export laws, (7) may not contain scripts or code that could cause a security breach or permit use of resources in opposition to OIT or University policy, and (8) WWW pages should clearly show identifying information of the owner of the page and we suggest that it also show date of last revision and an address (e-mail or postal) for correspondence. OIT equipment does not support use of scripting in individual pages.

### **IV. Data Backup, Security, and Disclaimer**

OIT will not be held liable for the loss or corruption of data as a result of the use and/or misuse of its computing resources (hardware or software) or from any damage that may result from the advice or actions of an OIT staff member.

Although OIT makes a reasonable attempt to provide data integrity, security, and privacy, the

User accepts full responsibility for backing up files in the assigned uNID, storage space or Computer Account. In addition, OIT makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to pay for any damages their actions cause. The User also agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold OIT harmless for any such liability or expenses. OIT retains the right to change and update these policies as required without notification to the User.

#### **V. Account Termination and Appeal Process**

Accounts on OIT systems may be terminated or disabled with little or no notice for any of the reasons stated above or for other inappropriate use of computing and network resources. When an account is terminated or disabled, we will make an attempt to contact the user (at the phone number they have on file with us) and notify them of the action and the reason for the action. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may appeal to: 1. a designated member of the appeals board so that a clear understanding of the events leading to the infraction is understood by the user and OIT: 2. An appeal coordinator who will review the evidence and hear reasons why an appeal should be considered: 3. The Director of OIT, after the appeals board has determined why the action was taken and stated an opinion on the severity thereof.

Users are advised that a history of infractions is kept. Any history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate University committee.

Last revised 8/9/01