



Computer and Network Use

Policy Statement

NOTE: The Administrative Interpretation provides additional guidance as to the meaning of the Policy. It does not limit the plain meaning of the terms of the policy, but, rather, seeks to provide additional information and further explain University requirements and expectations. The Policy is numbered and Administrative Interpretation of each numbered Policy paragraph is denoted by letter.

The University of Vermont provides a wide array of computing and networking resources to students, staff and faculty. These resources are intended to advance the educational, scholarly, and service missions of the University.

By accepting and/or using any UVM computer or network account, the user understands and agrees to the following:

1. Users are responsible for all use of computers and network accounts provided to them by the University, including data backup and password maintenance.
 - a. Responsible use includes choosing passwords that are not easily deduced by others.
 - b. Voluntary unauthorized disclosure of a password may result in suspension, revocation and/or denial of computing privileges. Disclosure of passwords to persons responsible for departmental computing, local LAN supervisors and the Office of Computing and Information technology ("CIT") is considered authorized disclosure.
 - c. Users who suspect that their University-provided computers or network accounts have been accessed without their permission are expected to change their passwords and are strongly encouraged to report the suspected activity to CIT.
 - d. University-provided computers and network accounts may only be used by the user to whom they are assigned unless otherwise authorized by the University. Access to such computers and network accounts for maintenance/service purposes by persons responsible for departmental

- computing, local LAN supervisors and CIT is considered authorized.
2. The University will seek to maintain system security, but users should not assume that information in their accounts, or on University-owned or -administered computers they use, is private. Authorized University personnel may obtain access to computing and networking resources as necessary to service the computing system, retrieve or modify University work, and to investigate suspected violations of this policy, including unlawful activity. Files will be disclosed to third parties as required by law. Users will be notified of access when notification is required by law and/or University policy.
 - a. The University cannot and does not guarantee the confidentiality of electronic information. In addition to accidental and intentional breaches of security, the University may be compelled to disclose electronic information as required by law.
 - b. As part of its necessary routine operations, the University occasionally gains access to network accounts and other computing services it makes directly or indirectly available to the campus community. Suspected policy violations discovered during such routine operations will be reported to the Director of CIT and/or law enforcement officials. All other information accessed during such routine operations will be treated as confidential, except as otherwise required by this policy or law.
 - c. The University will report suspected criminal activity to law enforcement authorities.
 - d. Unless otherwise prohibited by law, and subject to legal requirements, the University and law enforcement personnel may access computers, network accounts or any other electronic information or technology necessary to investigate suspected violations of this policy or unlawful activity.
 - e. For accounts granted to University employees, and University-owned or -administered computers they use:
 - i. Access to files can be granted on request of the department head.
 - ii. Termination of accounts can be requested by the department head.
 - iii. Department heads are responsible for moving needed files off terminated employees' accounts and University-owned or -administered computers within one month of termination.
 3. Users agree not to violate system security; interfere with system performance or another user's use of the system; or access network accounts, files or passwords intentionally and without authorization.
 - a. Users may not intentionally send email or develop other electronic information inaccurately attributed to another person.
 - b. Properly configured computers and printers may be attached to the UVM network without explicit permission. To safeguard network security and performance, no other device or network service, such as routers, hubs, sniffers and wireless access points, may be placed on the network without approval from CIT Network Services.

4. Users agree to use the computers and network accounts only for lawful purposes which are consistent with University policies and procedures.
 - a. Unlawful use of computers or network accounts includes, but is not limited to, defamation; obscenity; discrimination; violation of copyrights, trademarks and/or licenses; and/or violation of other rights arising under the law.
5. The University does not monitor and is not responsible for the content of the accounts and other computing services it provides. Each user is responsible for all information s/he accesses, makes available or distributes using the computer/network account.
6. Users may use their computers and network accounts for non-University matters except as otherwise prohibited by this or other University policy or where such use unreasonably interferes with academic uses, job performance, or system performance/operations. Such use is subject to the terms of this Policy, including without limitation terms regarding access to information on University computers and accounts.
 - a. Any and all information maintained on University-owned computers/network accounts, whether University-related or not, is accessible by the University. Other than to perform routine operations or as may be legally required, the University will not monitor accounts or access the information stored in computers/network accounts, unless such action is necessary to enforce this policy.
 - b. Students and employees are strongly encouraged to remove any "personal" information they may have stored on their computers/network accounts prior to ending their relationship with the University. Generally, the University will destroy information left on computers/network accounts. Information will be retained if retention is in the University's best interest. If the University extends an individual's account access beyond enrollment or the employment separation date, the account is not subject to this provision until the extension has ended.
7. Users agree not to use their computers or network accounts for non-University fundraising, commercial purposes or personal financial gain. Users are permitted to advertise personal items for sale on electronic forums which allow such postings, but the advertisement (s) should not interfere with the intended purposes of those forums.
 - a. University personnel may engage in fundraising and commercial activity on behalf of the University in connection with official University-related duties or University-sanctioned activities.
8. Users understand that violation of this Policy may result in suspension or termination of computer, network account and other access and, depending upon the circumstances, may result in disciplinary action including, but not limited to, academic expulsion or employment termination. Policy violations will be processed through normal University channels. If the activity is also unlawful, it may result in criminal prosecution.

- a. The University may temporarily suspend a user's computing privileges for security or other administrative reasons. Computing privileges suspended pursuant to this provision will be restored as soon as the threat or concern has been addressed or within three business days, whichever is shorter. Accounts which are suspended for more than three days will be handled as outlined in paragraph 8.c., below, irrespective of whether disciplinary action has been initiated. Absent extenuating circumstances, no account may be suspended pursuant to this Policy for more than 10 business days, unless the disciplinary process has been invoked.
 - b. Suspected violations by students will be reported to the Student Affairs judicial system. Suspected violations by University employees, whether faculty or staff, will be reported to the employee's supervisor and handled through normal channels established for disciplinary action.
 - c. Pending resolution of the disciplinary process, the Director of CIT or designee may suspend University computing privileges if the alleged violation is reasonably perceived to constitute unlawful activity, pose a substantial risk to the integrity of University Computing or present an imminent threat to the safety or welfare of the campus or members of the University community. In the event of a perceived emergency or where other exigent circumstances demand immediate action, the Director of CIT or designee may immediately suspend computing privileges and notice will be given to the user as soon after as reasonably possible. In non-emergency situations, the Director of CIT or designee will provide the user with notice of the perceived problem and an opportunity to be heard before privileges are suspended. A suspension may be appealed in writing to the Provost or designee within three business days of the effective date of the suspension. The Provost or designee will provide a written decision to the Director of CIT and the user within five business days of receipt of the appeal. The Provost's or designee's decision will remain in effect pending final resolution of the disciplinary proceeding.
 - d. Sanctions for violations of this Policy will be imposed by the administrative official with final responsibility for resolution of the disciplinary process in use, following consultation with the Director of CIT in the event that sanctions involve University Computing Services. Sanctions with respect to University Computing Services may include, but are not limited to, suspension or permanent revocation of computing privileges. If a user who loses his/her computing privileges cannot perform his/her job without those privileges, the user's employment may be suspended or terminated. The University reserves the right to seek restitution and/or indemnification from a student or employee for damage (s) arising from violations of this policy. In addition, the University and/or third parties may pursue criminal and/or civil prosecution for violations of law.
9. Users agree to read and abide by this policy and its administrative interpretation as they may be amended from time to time. The Provost is responsible for providing administrative interpretation, which will be modified periodically in

light of experience gained and legal and administrative developments. Users are responsible for reviewing this policy and its administrative interpretation on a routine basis.

Contacts

Questions related to the daily operational interpretation of this policy should be directed to:

Chief Information Officer
Enterprise Technology Services
(802)-656-4141

The Vice President for Finance and Administration is the official responsible for the interpretation and administration of this policy.

Effective Date

January 1, 2001