3-26-2015

UAP 2500: Acceptable Computer Use

University of New Mexico

UNM | Policy Office

This version was in effect for the period of 3-26-15 to _____

Administrative Policies and Procedures Manual - Policy 2500: Acceptable Computer Use

Date Originally Issued: 08-28-2000
Revised: 07-01-2011, 03-26-2015

Authorized by Regents' Policy 3.1 "Responsibilities of the President"
Process Owner: Chief Information Officer

1. General

As an institution of higher learning, the University of New Mexico encourages, supports, and protects freedom of expression as well as an open environment to pursue scholarly inquiry and to share information. Access to information technology (IT), in general, and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. The computing and network resources, services, and facilities of the University are limited and should be used wisely and carefully with consideration for the needs of others. As with any resource, there is a possibility of misuse. In an attempt to prevent or mitigate such misuse, this policy outlines proper and improper behaviors, defines misuse and incidental use, explains rights and responsibilities, and briefly reviews the repercussions of violating these codes of conduct.

The University of New Mexico provides computing services to University faculty, staff, students, retirees, and specified outside clients of the University and periodically to visitors and guests. These services are intended primarily for furthering the education, research, and public service mission of the University and may not be used for commercial purposes or profit-making. This Policy is applicable to all individuals using University-owned or -controlled computer equipment, communications equipment, data network (wired and wireless), storage devices, and computer-related facilities, whether such persons are students, staff, faculty, or third-party users of University computing resources and services. All University policies including, but not limited to, intellectual property protection, privacy, misuse of University equipment, sexual harassment, hostile work environment, data security, and confidentiality shall apply to the use of computing services.

1.1. Departmental Computer Use Policies and Procedures

Individual departments within the University may define "conditions of use" for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines, and/or restrictions. Such policies may not relax, or subtract from, this policy. Where such "conditions of use" exist, the enforcement mechanisms defined within these departmental statements shall apply. Individual departments are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. In such cases, the department administrator shall provide the cognizant vice president and the University Director of IT Security with a copy of such supplementary policies prior to their implementation. Where the use of external networks is involved, policies governing such use also are applicable and must be adhered to.

1.2. Computing Services

For the purposes of this policy computing services include the following:

- All University data, information, and information systems (including computer applications used by the University that are hosted elsewhere),
- All University computer hardware, software, multi-media, and communication services including all computer resources, communications equipment, and data networks—wired and wireless,
- All University telephones, mobile phones, smart phones, storage devices, and personal digital assistants, and
- All digital assets owned, managed or leased by the University and any that may be entrusted to the University by other organizations (e.g., cloud computing services as well as any other future computing device, service, system, or application.)

2. Rights and Responsibilities

The use of University computing services is a privilege. Users who have been granted this privilege must use the services in an appropriate, ethical, and lawful manner. Unauthorized access is prohibited and may be monitored and reported to the proper authorities. The University does not provide a warranty, either expressly or implied, for the computing services provided. The University reserves the right to limit a computer user's session if there are insufficient resources, and to cancel, restart, log, record, review or hold a job, process, network connection or program to protect or improve system or network performance if necessary.

The University network is large and complex and supports mission critical functions such as patient care, payroll, academic classes, Internet access, and electronic mail. To ensure the integrity of the network and maximize the availability of network services, all users connected to the University's network must follow IT requirements which can be found at http://it.unm.edu/network/policy.html.

Aside from publicly accessible computing resources such as the UNM main campus and branch campus public-access computers and any University-sanctioned unsecured wireless network, access to all University computing systems must be authorized by the cognizant department head or designee and in accordance with the terms of UAP 2520 ("Computer Security Controls and Guidelines").

2.1. User Responsibilities

Users are responsible for all their activities using computing services and shall respect the intended use of such services. Whenever a computing facility has specific rules and regulations that govern the use of equipment at that site and users shall comply with those rules and regulations governing the use of such computing facilities and equipment in addition to any over-arching University policies such as this one. Users must understand and keep up-to-date with this policy and other applicable University computer policies and procedures.

Users shall respect all copyrights including software copyrights. Users shall not reproduce copyrighted work without the owner's permission. In accordance with copyright laws, including the Digital Millennium Copyright Act, the Office of University Counsel, upon receipt of official notice from a copyright owner, may authorize blocking access to information alleged to be in violation of another's copyright. If after an investigation information is determined by the Office of University Counsel to be in violation of another's copyright, such information will be deleted from University computing systems.

2.1.1. Copyrights and Software Licenses

Users of University computing resources must comply with copyright law and the terms of licensing agreements,

including software licenses, before accessing or using copyrighted material on the Internet. Users are responsible for determining what licenses or permissions are necessary and for obtaining such permissions or licenses before using University computing resources. Purchased music, movies, software, and other multi-media files usually include a license that gives you permission to make copies, change formats or to share the file with others.

Generally, software which the University is not permitted or not licensed to use shall not be installed on University computing services; however, software which has been personally-acquired is permitted to be installed on University computing services so long as the user who has installed the software is able to prove s/he is legally permitted to do so. (This is usually done by retaining and providing the license upon request.)

File-sharing applications often involve the unlawful copying or distribution of copyrighted material without permission or license from the copyright owner. Anyone who sends or receives files using file-sharing software may be engaging in an unlawful act unless (a) the user is the copyright owner or has permission from the copyright owner, (b) the material is in the public domain, or (c) fair use or another exception to copyright law applies.

Upon receipt of information alleging that a user may be engaged in unauthorized file sharing of copyrighted material or is in violation of licensing obligations or other copyright law, the University may, without notice, immediately suspend, block, or restrict access to an account. The University may take such action when it appears necessary in order to protect the security or integrity of computing resources, or to protect the University from liability.

Users who violate copyright law or license terms may be denied access to University computing resources, and may be subject to other sanctions and disciplinary actions, including but not limited to expulsion or discharge from the University.

In accordance with its legal obligations, the University will continue to develop plans to combat the unauthorized use and distribution of copyrighted materials, including the possible use of technological deterrents. The University will also continue to provide information on alternatives to illegal file-sharing.

2.1.2. Site Licenses

The University enters into site license agreements with commercial vendors for campus-wide use of certain software products. The University currently has site licenses for products, including word-processing, spreadsheet, and database management applications software. In addition, many software applications are available at an educational discount through the UNM Bookstore or other vendors. Before buying a particular product, departments should contact the University Purchasing Department or IT Software Distribution to determine if the University has a site license or volume purchase discounts for the software in question. All users are responsible for adhering to University procurement policies and practices.

2.1.3. Software Developed Internally

University personnel may develop computer programs using University computing resources. Such software may be subject to the University's Intellectual Property Policy.

2.1.4. Computer Security

Individuals using computing services are responsible for keeping accounts and passwords confidential and for safeguarding all University data and information, especially those covered by state and federal regulations such as FERPA, GLBA, and HIPAA, regardless if it is being stored on University computing resources, stored on non-University resources, or being transmitted over communication networks.

Unless there is a legitimate University purpose, users shall keep all faculty, student, staff, and patient personally identifiable information (as defined by FERPA, GLBA, PCI, HIPAA, and any other applicable federal or state regulation) confidential and shall not transmit or request to receive such information. Examples of this type of information include social security numbers, drivers license numbers, birth dates, protected health information within the meaning of HIPAA, and insurance policy numbers. This is not an exhaustive list. When in doubt, individuals should the contact the Chief Information Officer (or designee) or the UNM Privacy Officer.

2.1.5. Computer Accounts and Passwords

The University, through IT and departments, provides computer accounts to authorized users for access to various University systems. These accounts are a means of operator identification and passwords are used as a security measure. An individual's computer account shall not be shared. Account use is a privilege, not a right.

2.1.5.1. Account Authentication

Passwords, PINs, and other identifiers authenticate the user's identity and match the user to the privileges granted on University computers, computer networks, systems, and computing resources. A password is a security measure designed to prevent unauthorized persons from logging on with another person's computer account and reading or changing data accessible to that user. Users should create passwords carefully and handle them with care and attention. Refer to http://it.unm.edu/accts/faq.html for guidance on creating passwords. For this security feature to be effective, the user must protect the secrecy of his/her password. Each user should:

- choose a password that is easy to remember but hard to guess,
- change his/her password regularly and at any time the user believes the password may have been compromised,
- avoid writing the password down, and
- not disclose or share the password with anyone.

Similar measures apply to all authentication methods such as PINs.

2.1.5.2 Account Termination and Locking

When an individual leaves the University, his or her account(s) must be locked as soon as reasonably possible and, subsequently, deleted within a reasonable time. If misuse or theft is detected or suspected, account(s) will be locked according to the University's procedures.

2.1.6. Computer and Data Security

Everyone at the University shares responsibility for the security of computer equipment, data, information, and computing resources.

2.1.6.1. Physical Security

Everyone is responsible for the proper use and protection of University computer resources. Examples of protection measures include:

- locking areas after business hours or at other times when not in use;
- taking special precautions for high-value, portable equipment;

- locking up documents and computing resources when not in use; and
- following University policies for taking computer equipment off campus (refer to UAP 7730 ("Taking University Property Off Campus")).

2.1.6.2. Information Security

Security of data and information is an essential responsibility of computer system managers and users alike. For example, users are responsible for:

- ensuring the routine backup of their files;
- using data only for approved University purposes; and
- ensuring the security and validity of information transferred from University systems.

UAP 2520 ("Computer Security Controls") should be referred to for specific information security requirements.

2.1.7. Computer Viruses and Anti-virus Software

All University departments, though department heads or designees, shall ensure anti-virus software is installed on University computing resources when technically possible and that the software is active and kept up to date. This requirement applies to all computer servers as well as all desktop and laptop computers. This will help ensure that University computing services and digital assets are not compromised, misused, deleted, or destroyed.

Assistance with virus protection and software is available from IT at http://it.unm.edu/.

3. Unacceptable Computer Use

The University reserves the right to block access to any external electronic resources that are deemed in violation of this Policy. The University reserves the right to sanction a user pursuant to Section 7. herein if it is determined, after an investigation by the appropriate office, that the user violated federal or state law, rules, or regulations or University policy by misusing University computing services. The University will disclose illegal or unauthorized activities to appropriate University personnel and/or law enforcement agencies.

3.1. Security Violations

Users shall not:

- attempt to defeat or circumvent any security measures, controls, accounts, or record-keeping systems;
- use computing services to gain unauthorized access to UNM's or anyone else's computing services;
- intentionally alter, misappropriate, dismantle, disfigure, disable, or destroy any computing information and/or services;
- knowingly distribute malware (i.e., computer viruses, worms, Trojans, or other rogue programs).

3.2. Legal Violations

Users shall not use computing services:

- for workplace violence of any kind as defined in UAP 2210 ("Campus Violence");
- for unlawful purposes, including fraudulent, threatening, defamatory, harassing, or obscene communications;
- to invade the privacy rights of anyone;
- to disclose student records in violation of FERPA;
- to access other computing services (i.e., other UNM computers or computer systems for unauthorized purposes);
- to access or disclose financial information in violation of the Gramm-Leach-Bliley Act or the University's Information Security Program;
- to access or disclose any non-public or personally identifiable information about a patient, employee, or student without having a legitimate University purpose;
- to access, use, or disclose protected health information within the meaning of the HIPAA Privacy Rule Regulation or any applicable state law relating to the confidentiality of health information about a patient, employee, or student without having a legitimate University purpose or in violation of HIPAA and applicable University policies pertaining to HIPAA privacy and security, except as permitted by University policy and applicable state and federal laws, rules, and regulations; or
- to violate University policy, state law, or federal law, including but not limited to copyright laws.

3.3. Other Misuse

Users shall not use computing services:

- in violation of any University contractual obligation, including limitations defined in software and other licensing agreements;
- in a way that suggests University endorsement of any commercial product (unless a legal agreement exists and any communication or computing activity has been pre-approved by an appropriate vice president);
- to conceal one's identity when using computing services, except when the option of anonymous access is explicitly authorized;
- to possess or distribute obscene or pornographic material unrelated to University instruction, research, or business needs (students are excluded from this provision);
- to masquerade or impersonate another,
- by physically or electrically attaching any device to a University computer, communications devices, or wired or wireless network connection that negatively impacts the performance of any other University computing service;
- to send chain letters, pyramid schemes, or unauthorized mass mailings;
- to send non-work or non-class related information to an individual who requests the information not be sent, or
- to send commercial or personal advertisements, solicitations, or promotions.

Users should understand that, due to their nature, electronic communications can be intentionally or unintentionally viewed by others or forwarded to others, and are therefore inherently not private. In addition, addressing errors, system malfunctions, and system management may result in communications being viewed and/or read by other individuals and/or system administrators. IT provides assistance in the proper use of e-mail

at http://it.unm.edu/email/index.html.

In electronic communications, users must state whether they are speaking for themselves or in an official capacity for the University. Electronic communications that represent the University sent to non UNM addresses must be done in a professional manner and comply with UAP 1010 ("University External Graphic Identification Standards").

4. Incidental Personal Use

The University allows incidental personal use of computing services. Such use must not interfere with an employee fulfilling his or her job responsibilities, consume significant time or resources, interfere with other users' access to resources, be excessive as determined by management, or otherwise violate any federal or state laws, any individual college or departmental policies or codes of conduct, or University policies. Each department should document and communicate what use is acceptable.

5. Privacy Limitations

Users of University computing services, including managers, supervisors, and systems administrators shall respect and protect the privacy of others, in accordance with all applicable state and federal laws, regulations and University policies. UAP 2520 ("Computer Security Controls") defines the limited conditions under which access to information and files can be obtained. Although the University is committed to protecting individual and information privacy, the University cannot guarantee the security or privacy of correspondence and information stored and transmitted through University computer networks and systems. Since confidential information is often stored on desktop machines, displayed on screens, or printed on paper that could be in public view, users need to control access by:

- using passwords;
- turning screens away from public view;
- logging out of systems when leaving the work area;
- shredding reports containing private information prior to disposal; and
- clearing confidential information off desks in public areas.

While the University does not routinely monitor individual usage of its computing services, the normal operation and maintenance of the University's computing services require the backup and storage of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendering of services. Similarly, the University does not, in the regular course of business, monitor the content of computing services on its various networks. However, suspicious aggregate behavior, official requests from authorities, forensic evaluation or discovery for purposes of civil litigation, or indications of a security incident, for example, can cause network activities or computing services to be reviewed. It is the right of the University to monitor and review any activities on its resources. It is best, therefore, to assume that any and all actions taken or activities performed using University computing services are not private.

The University may also access and examine the account (e.g. any and all computer accounts on any University computing resource, e-mail boxes, file shares, local or networked storage) of an individual user under the following circumstances and conditions:

- if necessary to comply with federal or state law, or
- if there is reasonable suspicion that a law or University policy has been violated and the examination of the account is needed to investigate the apparent violation, or

- as part of an investigation involving an administrative claim or charge, arbitration or litigation, or if required to preserve public health and safety.

Requests for access based on reasonable suspicion must be approved in writing, in advance, by the cognizant vice president. If access to a faculty member's account is being requested, the President of the Faculty Senate must be notified in conjunction with the request for approval. Each request must specify the purpose of access and such access will be limited to information related to the purpose for which access was granted. If such access is being requested by a vice president, access must be approved by the President. If such access is being requested by the President, access must be approved by the UNM Board of Regents. The Regents' Internal Auditing Policy authorizes the University Audit Department full and unrestricted access to all University records, including but not limited to those contained in computer files, discs, and hard drives.

Accessing an employee's computer files for work-related, non-investigatory purposes (i.e., to retrieve a file or document needed while the employee who maintains the file or document is away from the office) is permitted and does not require authorization by a vice president as long as access is limited to the work-related need. When an employee separates from the University, work-related files, including but not limited to research data, as well as all records made or kept in any University electronic medium, remain the property of the University.

Communications and other documents made or kept by means of University computing services are generally subject to New Mexico's Inspection of Public Records Act to the same extent as they would be if made on paper. Therefore, all employees are urged to use the same discretion and good judgment in creating electronic documents as they would use in creating written paper documents.

6. Reporting Procedures

Suspected violations of this policy (e.g., any incidents involving the unauthorized access to, destruction of, or misuse of computing services by employees, faculty, or students) must be brought to the attention of the cognizant dean, director, or department head, and the University IT Security Office (Security@unm.edu). In the case of a criminal violation, the IT Security Office will notify UNM Police Department. Violations by non-employees will be referred to the appropriate authorities. The Office of University Counsel should be contacted if assistance is needed to identify the appropriate authority.

7. Sanctions

The misuse, unauthorized access to, or destruction of University computing services in violation of applicable laws or University policy may result in sanctions, including but not limited to withdrawal of use privilege; disciplinary action up to and including expulsion from the University or discharge from a position; and legal prosecution.