15.11 – Acceptable Use of ICT Equipment and Resources

arp.nmsu.edu/chapter-15/15-11.html

Policy Details

Responsible Executive: Provost and Chief Academic Officer
Responsible Administrator: Chief Information Officer
Scope: NMSU System
Last Updated: 08/22/2011

PART 1: PURPOSE

This Rule defines appropriate and inappropriate use of NMSU-owned and controlled resources, such as electronic devices, software, computer systems and networks that are directly, or through a third party, used to transmit, receive, process or store information or data such as computers, servers, databases, Personal Data Assistants (PDAs), telephones, wireless devices, e-mail systems, voice messaging systems and Internet connectivity. Also included is the use of non NMSU-owned electronic resources storing or connecting to NMSU data. In addition, the Rule defines privacy of data, copyright/intellectual property rights to data, and data ownership and access.

PART 2: RULES

A. **Ownership and Use:** NMSU computing equipment and resources are owned and/or administered by the Board of Regents of New Mexico State University. Access to NMSU equipment and resources is a privilege granted to students and employees to facilitate instruction/learning, research and administration. All users of NMSU computing equipment and resources are required to affirm the following:
I have read the Acceptable Use Rule, and I understand and agree to abide by the terms of the Rule. I also understand that my use of NMSU equipment and resources must be in accordance with the Rule. I recognize that violations of this Rule may cause restriction or elimination of my access to NMSU computer resources, other disciplinary action, or civil or criminal penalties.

B. **User Responsibilities**
   1. NMSU computing equipment and resources are used to support the mission of the university and may not be used for commercial or profit-making purposes.
   2. NMSU computing equipment and resources may only be used by users in ways that do not violate the law or NMSU policies.
   3. The willful transmission of known destructive applications and viruses by a user is prohibited.
   4. Users whose activities place high loads on the NMSU system must conduct these activities in off hours or in low system demand times.
   5. Users are responsible for protecting university data and technologies from unauthorized uses and security threats.
   6. Users must be considerate of the rights of other users.

C. **Copyright Compliance**
   1. NMSU shall comply with the Copyright Law of 1976 and its amendments (Title 17, United States Code), including the Digital Millennium Copyright Act of 1988. Faculty, staff, and students should be aware that copyright infringements occurring on university networks may result in termination of networking privileges as well as other penalties under federal law.
   2. Users must be in compliance with copyright laws and licensing agreements. The University's Office of Information and Communication Technologies may block access to information alleged to be in violation of copyright laws. If a user is found to be in violation of copyright laws, the information found to be in violation shall be deleted from the university's computing system(s). Also, the violator may be subject to other sanctions.

D. **Misuse of Information and Technology Services:** The university reserves the right to sanction a user for the misuse of university information and technology equipment and resources. In addition to other standards specified in NMSU policy or rules and procedures; examples of misuse include, but are not limited to:
   1. Intentionally altering, disabling, destroying or stealing electronic resources.
   2. Unauthorized access.
   3. Use of illegal software or data.
   4. The development and/or use of programs which impede the use or the network or cause damage.
   5. Attempting to defeat or circumvent any security measures, controls, accounts, or record-keeping systems.
   6. Using information and technology equipment and resources for unlawful purposes including fraudulent, defamatory or harassing acts, acts of violence, etc.
   7. Invading privacy and confidentiality rights protected under the law.

E. **Incidental Personal Use of Electronic Resources by Employees**: Incidental personal use of electronic university-owned resources is covered in **ARP 3.14 Non-Work Related Use of University Resources**, which prohibits, in part: *"…viewing, displaying, downloading, printing, procuring, or transmitting of sexually explicit material; nor of any other material that would violate university policy, rule, procedure, or the law, including but not limited to, those relating to sexual harassment, fraud, hostile workplace, obscenity, libel, defamation, or hate/violent misconduct."*

F. **Privacy:** Notwithstanding users' rights to privacy, and any rights under the Electronic Communication Privacy Act of 1986, FERPA HIPAA and GLBA, users grant specific permission to university to inspect users' accounts and file space for investigation of violation of university policy or rules and procedures or as needed for maintenance functions. When investigating a possible abuse of the system, Information and Communication Technologies has the authority to examine files, passwords, accounting information, printouts, tapes, or other material that may aid in the investigation. Investigations must follow university procedures. Use of university equipment or resources implies consent to this Rule.

G. **Access – Investigative Purposes:** The university reserves the right to access a user's account when there is reasonable suspicion that a law or university policy, rule or procedures have been violated. The following steps for a request to access a user's account include:
    1. Requests for access based on a reasonable suspicion must be in writing and approved prior to access being granted by President/President, provost, general counsel, human resources, internal audit department or law enforcement.
    2. Each request must specify the purpose for which access is being requested.

H. **Access – Non-Investigative Purposes – Work Related:** Access to work-related files is permitted as long as there is a work-related need and the users are, by the nature of their work, approved to access these files. When an employee separates from the university, all work-related files remain the property of the university.

I. **Sanctions:** Use of information technology equipment or resources in violation of applicable laws, university policy, rule or procedures may result in sanctions, which include, but not limited to, the sanctions listed below:
    1. Withdrawal of use privileges.
    2. Disciplinary action, up to and including, expulsion or discharge from a position.
    3. Legal prosecution.

Related

Cross-Reference:

ARP 3.14 – Non-Work Related Use of University Resources

Revision History:

2017 Recompilation, formerly Rule 2.35.1.1.1