Policy Name: Policy on Privacy of University Information Technology Resources

Responsible Department: Information Technology

Approving Body: Policy Committee

Approved Date: Tuesday, December 15, 2014

Purpose:
N/A

Policy:
Stored computer information, voice and data network communications, and personal computers may not be accessed by someone outside of the provisions of this policy. No one other than the person to whom the computer account in which the information has been stored is assigned, or from whom the communication originated, or to whom the device has been assigned may access this data. This policy covers:

- Data and other files, including electronic mail and voice mail, stored in individual computer accounts on University-owned centrally-maintained systems;
- Data and other files, including electronic mail and voice mail, stored in individual computer accounts on systems managed by the University on behalf of affiliated individuals or organizations;
- Data and other files, including electronic mail or voice mail, stored on personally-owned devices on University property (e.g., residence hall rooms);
- Data and other files, including electronic mail or voice mail, stored on University-owned computers assigned to a specific individual for their use in support of University job functions; and
- Telecommunications (voice or data) traffic from, to, or between any devices described above.
- A technician or administrator may access or permit access to the resources described above, if he or she
  1. Has written (verifiable email or paper) permission from the individual to whom the account or device or communication has been assigned or attributed; or
  2. In an emergency situation, has a reasonable belief that a process active in the account or
on the device is causing or will cause significant system or network degradation, or could cause loss/damage to system or other users' data; or

3. Receives a written authorization from the appropriate campus Vice President, for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has perpetrated or is involved in illegal activities using the accounts or device in question; or

4. Receives a written authorization from the appropriate campus Vice President, for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has perpetrated or is involved in violations of University policy using the accounts or device in question; or

5. Receives a written request from the senior executive officer of a department to access the account of a staff or faculty member who is deceased, terminated, or is otherwise incapacitated or unavailable, for the purposes of retrieving material critical to the operation of the department; or

6. Receives a written request from the appropriate Vice President or equivalent, on behalf of the parents or estate manager of a deceased student; or

7. Receives a written authorization from the appropriate Vice President, for situations where there is reasonable belief that a student to whom the account or device is assigned or owned has perpetrated or is involved in illegal activities using the accounts or device in question; or

8. Receives a written authorization from the appropriate Vice President, for situations where there is reasonable belief that a student to whom the account or device is assigned or owned has perpetrated or is involved in violations of University policy using the accounts or device in question; or

9. Receives a directive from the Vice President of Business Affairs when Audit staff are engaged in investigations of fiscal misconduct;

10. Receives a legal court order and subsequent direction from University Counsel, or

11. Receives other legal documents and subsequent direction from University Counsel. In the event that University officials are notified of a University or law enforcement investigation for alleged misconduct or illegal activity on the part of a member of the IT community, contents of an individual's e-mail, other computer accounts, office computer, or network traffic may be copied and stored to prevent destruction and loss of information, pending formal review of that material. Subsequent release of the stored materials must be in accordance with the above-specified criteria.
Except when inappropriate or impractical, all efforts will be made to notify the involved individual prior to accessing the computer account or device, or before observing network traffic attributed to them. Where prior notification is not appropriate or possible, all efforts will be made to notify the involved individual as soon after the access as is possible.

System-generated, content-neutral information (“metadata”) may be used for the purposes of monitoring system and storage utilization, problem troubleshooting, security administration, technology abuse or misuse incident investigation, and in support of formal audits. This information includes operating system logs (i.e., record of actions or events related to the operation of the system or device), user login records (i.e., what usernames were used to connect to WNMU systems, from where, and when) dial-up logs (i.e., who connected to University modems, from where, and when), network activity logs (i.e., what connections were attempted or completed to University systems, from where, and when), email logs (i.e., who sent email to or from University email systems, and when), and auditing logs (i.e., records of what actions were taken on University systems, against what resources or applications, and when).

Any intrusive or restrictive actions taken by the University related to information technologies will be in accordance with guidelines and procedures set forth in other applicable University policies, codes, or laws. University policies include (but are not limited to) administrative procedures and policies, and technology appropriate use policies. Laws include (but are not limited to) the Health Information Portability and Protection Act (patient medical information), Family Educational Rights and Privacy Act (student records), Electronic Communication Privacy Act, the No Electronic Theft Act, and the Digital Millennium Copyright Act.

This policy applies to all Western New Mexico University faculty, students, and staff, including employee supervisors and administrators and computer and network technicians who have been assigned the task of maintaining University information technology systems.

**Procedures:**

None