



Policy & Procedures

Information Disclosure Policy

Issued by: Technology Steering Committee

Applies to: All University Employees

Effective date: June 17, 2003

The University does not endorse the systematic inspection of electronic files or monitoring of network activities related to individual activities. However, there are legitimate reasons for persons other than the account holder to access computer files or computers or network traffic: ensuring the continued integrity, security, or effective operation of University systems; to protect user or system data; to ensure continued effective departmental operations; to ensure appropriate use of University systems; or to satisfy a lawful court order.

Policy

Stored computer information, data network communications, and personal computers may not be accessed by someone 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, outside of the provisions of this policy. This policy covers:

- Data and other files stored in individual computer accounts on University-owned systems;
- Data and other files, stored in individual computer accounts on systems managed by the University on behalf of affiliated organizations;
- Data and other files stored on personally-owned devices on University property (e.g., residence hall rooms);
- Data and other files stored on University-owned computers assigned to a specific individual for their use in support of job functions; and

A Support Analyst or Administrator may access or permit access to the resources described if:

1. There is 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. In an effort to resolve a call made to the help desk, the analyst receives permission from the caller to remotely connect to the computer for problem resolution; or
4. 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

5. Receives a written authorization from the appropriate campus Dean of Students or equivalent, 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

The University considers any violation of appropriate use principles to be a serious offense and reserves the right to copy and examine any files or information resident on University systems allegedly related to inappropriate use. Violators are subject to disciplinary action including loss of all University computing privileges and possible criminal charges including civil damages. Offenders also may be prosecuted under various state & federal laws including (but not limited to) the Privacy Protection Act of 1974, The Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication of 1989, Interstate Transportation of Stolen Property, and the Federal Electronic Communications Privacy Act. Access to the texts of these laws is available through the Reference Department of the Library. Violators may also cause the University to be liable to civil or criminal penalties.