Policy 4-002: Information Resources Policy

I. Purpose

To outline the University's policies for students, faculty and staff concerning the use of the University's computing and communication facilities, including those dealing with voice, data, and video. This policy governs all activities involving the University's computing facilities and information resources, including electronically or magnetically stored information. Every user of these systems is required to know and follow this policy.

II. References

Policy 5-106, Equal Opportunity and Nondiscrimination

Policy 5-107, Sexual Harassment and Consensual Relationships

Policy 5-210, Discrimination and Sexual Harassment Complaint Policy

Policy 5-111, Termination of Nonacademic Staff Employees

Policy 5-203, Employment Grievances

Policy 1-006, Conflicts of Interest

Policy 6-400.II, Student Code

Policy 6-316, Code of Faculty Responsibility

Policy 4-001, Institutional Data Management

18 U.S.C. § 2510: Electronic Communications Privacy Act

Utah Code Ann. § 76-6-703: Utah Computer Crimes Act

Utah Code Ann. § 76-10-1801: Communications Fraud

Utah Code Ann § 63-2-101 et seq.: Government Records Access and Management Act (GRAMA)

III. Scope

A. This policy applies to all members of the University of Utah community, and governs all storage and communications systems owned by the University, whether individually controlled or shared, stand alone or networked.

B. Individual departments and colleges serve diverse purposes and diverse constituencies; therefore, they have broad discretion in establishing reasonable and appropriate policies and "conditions of use" for facilities under their individual control. Departmental policies shall be consistent with this policy although they may provide additional detail, guidelines and/or restrictions.

IV. Definitions

A. Information Resources include any information in electronic, audio-visual or physical form, or any hardware or software that makes possible the storage and use of information. This definition includes but is not limited to electronic mail, phone mail, local databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

B. User includes anyone who accesses and uses the University of Utah Information Resources.

V. Policy

A. General

1. The University of Utah makes available Information Resources which may be used by University students, faculty, staff and others. These resources are intended to be used for educational purposes and the legitimate business of the University and in a manner consistent with the public trust. Appropriate use of the resources includes instruction, independent study, authorized research, independent research and the official work of the offices, departments, recognized student and campus organizations of the University.

2. Access to computer systems and/or networks owned or operated by the University of Utah imposes responsibilities and obligations on its Users. Access is granted subject to University and Board of Regents policies, and local, state, and federal laws. Appropriate use is ethical, reflects academic honesty, and shows restraint in the utilization of shared resources. Appropriate use is consistent with intellectual property rights, ownership of data, system security mechanisms, and rights to privacy and to freedom from intimidation, harassment, and annoyance.

3. It is the University's policy to maintain access to local, national and international sources of information, and to provide an atmosphere that encourages access to knowledge and sharing of information. The University also strives to create an intellectual environment in which students, staff, and faculty feel free to create individual intellectual works as well as to collaborate with other students, staff and faculty without fear that the products of their intellectual efforts will be violated, misrepresented, tampered with, destroyed, stolen or prematurely exposed. Nothing in this policy guarantees that violations of this policy will not occur or imposes liability on the University for any damages resulting from such a violation.

4. The personal use of University resources is covered in the University's Conflicts of Interest policy, Policy 1-006 and in Policy 6-316; and Policy 5-207.

5. The University retains the right to allocate its information resources and to control access to its electronic communications systems.

B. Privacy

1. Electronic communications systems have inherent limitations. No computer security system can absolutely prevent a determined person from accessing stored information that he/she is not authorized to access. Moreover, electronic documents may be disclosed pursuant to public records law or in the discovery process.

2. Users shall respect the legitimate expectations of privacy of others. However appropriate administrators and network managers may require access to records and data typically taken to be private. In particular, individuals having official computer or network responsibilities, such as system administrators, network supervisors, system operators, postmasters or others who cannot perform their work without access to documents, records, electronic mail, files or data in the possession of others, may access such information as needed for their job responsibilities. Whenever practical, prior notice should be given for other than trivial intrusions on privacy.

3. The University reserves the right to concurrently monitor an employee's electronic communications when such monitoring is necessary to the evaluation of his/her job performance quality. The University will notify employees when such monitoring or surveillance may occur. This monitoring will comply with the following restrictions:

   a. all monitoring will be relevant to work performance;

   b. employees will be given access to information about their work gained through monitoring;

   c. disclosure and use of resulting data will be restricted to University-related purposes.

C. Individual Responsibilities

1. Users shall respect the privacy and access privileges of other users both on the University campus and at all sites accessible through the University's external network connections.

    a. Users shall treat institutional data, files maintained by other Users, departments, or colleges as confidential unless otherwise classified pursuant to state or federal statutes, regulation, law or University policy. Users shall not access files or documents belonging to others, without proper authorization or unless pursuant to routine system administration.

    b. Users shall not knowingly falsely identify themselves and will take steps to correct misrepresentations if they have falsely or mistakenly identified themselves.

2. In making appropriate use of Information Resources users must:

    a. use Information Resources only for authorized purposes;

    b. protect their user ID from unauthorized use;

    c. be considerate in their use of shared resources and refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals or other resources.

3. Users must respect the integrity of computing systems and networks, both on the University campus and at all sites accessed by the University's external network connections. As such, in making appropriate use of Information Resources Users must NOT:

    a. gain, attempt to gain or help others gain access without authorization;

b. use or knowingly allow other persons to use University Information Resources for personal gain, for example, by selling access to their User-ID's, or by performing work for profit or contrary to University policy.

c. destroy, damage or alter any University Information Resource or property without proper authorization;

d. waste computing resources, for example by implementing or propagating a computer virus, using destructive software, or inappropriate game playing; or monopolizing information resources for entertainment or personal use;

e. harass or intimidate others in violation of law or university policy;

f. violate laws or University policy prohibiting sexual harassment or discrimination on the basis of race, color, religion, gender, national origin, age, disability or sexual orientation, or veteran status;

g. attempt to monitor or tamper with another user's electronic communications or copy, change, or delete another user's files or software without the explicit agreement of the owner(s); or

h. violate state and federal laws pertaining to electronic mailing of chain letters and other unauthorized use of computing resources or networks;

i. make or use illegal copies of copyrighted or patented software, store such copies on University systems, or transmit such software over University networks;

j. attempt without authorization to circumvent or subvert normal security measures or engage in any activity that might be harmful to systems or information stored thereon or interfere with the operation thereof by disrupting services or damaging files. Examples include but are not limited to: running "password cracking" programs, attempting to read or change administrative or security files or attempting to or running administrative

programs for which permission has not been granted, using a telnet program to connect to system ports other than those intended for telnet, using false identification on a computer or system or using an account assigned to another, forging mail or news messages; and

k. transfer software, files, text or pictures in violation of copyright and/or pornography laws, or transfer software or algorithms in violation of United States export laws.

D. Enforcement and Sanctions

1. A violation of the provisions of this policy or departmental policy is a serious offense that may result in the withdrawal of access and in addition may subject the User to disciplinary action or academic sanctions consistent with University policies and Procedures.

2. Incidences of actual or suspected non-compliance with this policy should be reported to the appropriate authorities. Disciplinary actions or academic sanctions will be assessed in accordance with the following:

   a. Violations of this policy by a faculty member shall be the basis for disciplinary action in accordance with Policy 6-316, Code of Faculty Responsibility.

   b. Violations of this policy by a staff member shall be the basis for disciplinary action in accordance with Policy 5-111, Disciplinary Actions and Dismissal of Staff Employees, and Policy 5-203, Staff Employee Grievances and Appeals.

   c. Violations of this policy by a student shall be the basis for disciplinary action in accordance with Policy 6-400, Student Code.

3. A systems administrator may immediately suspend the access of a User when the administrator reasonably believes:

a. the User has violated University policies or law; and

b. the User's continuing use of Information Resources will result in: (1) damage to the Information Resources systems, (2) further violations of law or policy or (3) the destruction of evidence of such a violation.

c. the User shall be informed of his/her right to immediately appeal such a suspension to the cognizant head of the department or unit. Permanent revocation of privileges shall be imposed solely through the disciplinary processes set forth in paragraph 2 above. (Section V.D.2).

4. Users who are not faculty, staff or students may have their access to Information Resources unilaterally revoked if they violate this policy.\

[Note: Parts IV-VII of this Regulation (and all other University Regulations) are Regulations Resource Information – the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

VI. Rules, Procedures, Guidelines, Forms and other related resources

A. Rules

Rule 4-002A

B. Procedures

C. Guidelines

D. Forms

E. Other related resource materials

VII. Contacts

The designated contact officials for this Policy are:

A. Policy Owner (primary contact person for questions and advice): Director of Planning and Policy/Office of Information Technology.

B. Policy Officer: Chief Information Officer

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

"A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases.... "

"The Policy Officer will identify an 'Owner' for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... .[and] bears the responsibility for determining -requirements of particular Policies... ." University Rule 1-001-III-B & E

VIII. History

Renumbering: Renumbered as Policy 4-002 effective 9/15/2008, formerly known as PPM 1-15.

Revision History:

Current version: Revision 0

Effective date: July 13, 1998

Approved: Board of Trustees July 13, 1998

Editorially revised: September 15, 2010, to include related regulations (VI.) and history (VIII.)