POLICY GOVERNING ACCESS TO AND USE OF UNIVERSITY INFORMATION TECHNOLOGY RESOURCES

I. Introduction

Computers, network systems, and other associated technologies offer powerful tools for creating, communicating, and managing data, and for a host of other activities. Taxpayers, students, and other groups providing sources of funding that support information technology resources at the University expect that these assets will be used in support of the University's mission of instruction, research and other creative activity, and service.

The University expects all individuals using information technology resources to take appropriate measures to manage the data stored on technology resources. The University is expected to preserve and protect administrative data transmitted and stored on its systems and comply with applicable federal and state legislation.

The University generally does not monitor or restrict the content of material transmitted, stored, or posted on University-owned information technology resources , but reserves the right to limit or remove access to its networks and to material posted on its computers, when applicable University regulations, contractual obligations, or state or federal laws are violated. Individuals who use University technology resources and email for any work-related or personal matters do not acquire an absolute right of privacy for data, documents and communications transmitted or stored on University information technology resources.

II. Scope

A. This policy applies to users of University information technology resources irrespective of whether those resources are accessed from on-campus or off-campus locations. Persons having the following affiliations with the University are eligible to access and use the University's information technology resources:

1. Current faculty and staff, including post-doctoral fellows;

2. Currently enrolled students (including undergraduate, graduate, and non-degree students);

3. Upon request, retired faculty and staff, and their surviving spouses or sponsored dependents;

4. Upon request, spouses or sponsored dependents of faculty or staff who become deceased while employed by the University;

5. Certain persons affiliated with external agencies collaborating with the University; and

6. Any other person authorized by the Vice President for Information Technology or designee to use University information technology resources.

An individual's access to specific resources shall be limited due to University licensing or contract limitations.

For groups 3, 4, and 5, access is generally limited to electronic mail. If resources become constrained, this practice may be reviewed and may be restricted or eliminated in favor of allocating required resources to uses by active faculty, students, and staff. Unless eligible though another affiliation, alumni of the University are not eligible to access and use University information technology resources, except when such resources are available to the general public.

B. This policy applies to all University information technology resources, including:

1. Data and other files, including electronic mail and voice mail, stored in individual computer accounts on University-owned centrally-maintained systems;

2. Data and other files, including electronic mail or voice mail stored on departmentally-maintained systems;

3. 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 organizations;

4. Data and other files, including electronic mail or voice mail, stored on personally-owned devices on University property (e.g., residence hall rooms);

5. Data and other files, including electronic mail or voice mail stored on University-owned systems assigned to a specific individual for use in support of job functions; and

6. Telecommunications (voice or data) traffic from, to, or between any devices described above.

III. Confidentiality

A. In general, information stored on information technology resources is considered confidential, whether protected by the computer operating system or not, unless the owner intentionally makes that information available to other groups or individuals.

The University assumes that individual users wish the information they store on central and campus shared information technology resources to remain confidential. Requests for disclosure of confidential information may be reviewed by the senior administrator of the information technology systems involved. Such requests shall be honored only when approved by the University officials authorized by the University, or when required by state or federal law. Except when inappropriate or impractical, computer users shall receive prior notice of such disclosures.

B. Free expression of ideas is central to the academic process. The University acknowledges the importance of the diversity of values and perspectives prevalent in an academic institution, and is respectful of freedom of expression of ideas. The University does not condone censorship nor does it endorse the inspection of electronic files or monitoring of network activities related to individual activities.

C. Legitimate reasons for persons other than the account holder to access computer files, computers, or network traffic, or to disclose data to third parties, include:

1. Ensuring the continued integrity, security, or effective operation of University systems;

2. Protecting user or system data;

3. Ensuring continued effective departmental operations;

4. Ensuring appropriate use of University systems;

5. Satisfying a legal obligation;

6. Complying with the Kentucky Open Records Act;

7. Complying with the Federal Rules of Civil Procedure for E-Discovery; or

8. Health and safety emergencies.

D. In any case where it becomes necessary for persons other than the account holder to access computer files or computers or network traffic for one or more of the purposes outlined above, all reasonable attempts shall be made to limit the access to the related purpose and to preserve confidentiality of any personal identifiers.

IV. Security

A. Although the University takes reasonable measures to protect the security of its information technology resources and accounts assigned to individuals, the University does not guarantee absolute security.

B. The University helps users of its central and campus shared information technology resources to protect the information they store on those resources from accidental loss, tampering, unauthorized search, or other access. In the event of inadvertent or non-malicious actions resulting in the loss of or damage to information, or the invasion of the user's identity or privacy, the University's information technology department shall make a reasonable effort to mitigate the loss or damage.

C. The University provides industry-standard security on University maintained systems. Users are responsible for properly safeguarding the information technology resources under their control, specific to files associated with their computer accounts.

D. Users may request that arrangements be made to protect information stored on such resources. These requests may be honored at the discretion of the unit that manages the resources.

V. Information Technology Users' Privileges and Responsibilities

A. The University grants access to its information technology resources to an individual solely for the individual's own University mission-related use. User access shall not be transferred to or shared with another without explicit written authorization by the Vice President for Information Technology, a designee, or the appropriate system administrator.

B. All users of University information technology resources are expected to exercise common sense and decency, including due respect for the rights of others in public areas.

C. User access to information technology resources is contingent upon prudent and responsible use, which includes following appropriate security measures. The user shall not use information technology resources to violate any state or federal laws, Governing Regulations and Administrative Regulations, Code of Student Conduct, Human Resources Policy and Procedures, or Rules of the University Senate. Incidental personal use is an accepted and appropriate benefit of being associated with the University's technology environment. The senior management of each unit is authorized to determine the nature and amount of incidental personal use by members of the unit. An employee's supervisor may require the employee to cease or limit any incidental personal use that hampers job performance, adversely affects or conflicts with University operations or activities, or violates University policy. All direct costs (for example, printer or copier paper and other supplies) attributed to personal incidental use shall be assumed by the user.

D. The user shall not use information technology resources for any individual commercial purpose or for personal gain, except as approved pursuant to other

applicable University regulations, or approved by the Vice President for Information Technology, or a designee.

E. Information technology resources shall be shared among users in an equitable manner. The user shall not participate in any behavior that unreasonably interferes with the fair use of information technology resources by another.

F. Information technology resource users shall facilitate computing in the University environment by:

1. Regular deletion of unneeded files from one's accounts on central or shared machines in accordance with the University's record retention policy.

2. Refraining from overuse of information storage space, printing facilities, or processing capacity, and interactive network connections.

VI. System Administrator Responsibilities

A. Both University and departmental system administrators of information technology resources are responsible for the security of information stored on those resources, for making appropriate information on security procedures available to users of those systems, and for keeping those systems free from unauthorized access. Administrators of departmental and individual information technology resources shall not implement any policy or procedure that is less restrictive than University requirements.

B. University and departmental system administrators are prohibited from removing any information from individual accounts unless the system administrator finds that:

1. The presence of the information is illegal (e.g. copyrighted material, software used in violation of a license agreement, or child pornography);

2. The information in some way endangers University information technology resources or the information of other users (e.g. a computer worm, virus, or other destructive program); or

3. The information is inappropriate because it is unrelated to or is inconsistent with the mission of the University, is in violation of University policy, or is otherwise not in compliance with the legal and ethical usage responsibilities listed in the Information Technology Usage Policy.

4. Prior to transfer of equipment from one unit to another, or when equipment is declared surplus, all files shall be wiped clean from the hard drives. See: http://www.uky.edu/Regs/BPM/E-12-4.pdf.

5. After an employee leaves the unit's employment or a student discontinues their enrollment at the University, the individual's computer account may be inactivated or files may be wiped clean from the hard drives.

C. Departmental system administrators (or University system administrators) 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;

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 or damage to system or other users data; or

3. 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, transferred, or is otherwise incapacitated or unavailable for the purposes of retrieving material critical to the operation of the department.

D. University system administrators may access or permit access to the resources described above, if he or she:

1. Receives a court order or direction from University Counsel;

2. Receives a written authorization from the appropriate executive vice president or Provost, 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

3. Receives a written request from the Dean of Students, for situations where there is a reasonable belief that a student to whom the account or device is assigned or owned has perpetrated or is involved in illegal activities, or is in violations of University policy using the accounts or device in question.

VII. Violations

A. Legitimate use of an information technology resource does not extend to whatever an individual is capable of doing with it. Just because an individual is able to circumvent restrictions or security, does not mean that the individual is permitted to do so.

Alleged violations of this policy can be reported directly to the Office of the Vice President for Information Technology. If the person responsible is not affiliated with the University, or cannot be identified, the incident should be reported to <itresource abuse@uky.edu>.

B. Examples of Violations

Violations generally consist of downloading or posting to University computers, or transporting across University networks, material that is illegal, proprietary, in violation of University policies or contractual agreements, or otherwise is damaging to the institution. Examples of specific violations include, but are not limited to:

1. Sharing passwords or acquiring another's password without prior written authorization from University Technology Services or the appropriate system administrator;

2. Unauthorized accessing, using, copying, modifying, or deleting of files, data, user ids, access rights, usage records, or disk space allocations;

3. Accessing resources for purposes other than those for which the access was originally issued, including inappropriate use of authority or special privileges;

4. Copying or capturing licensed software for use on a system or by an individual for which the software is not authorized or licensed. Misappropriation of data or copyrighted materials, including computer software, may constitute theft;

5. Use of information technology resources for remote activities that are unauthorized at the remote site;

6. Causing computer failure through an intentional attempt to "crash the system," or through the intentional introduction of a program that is intended to subvert a system, such as a worm, virus, Trojan horse, or one that creates a trap door;

7. Intentional obscuring or forging of the date, time, physical source, logical source, or other header information of a message or transaction;

8. Interception of transmitted information without prior written authorization from University Technology Services or the appropriate system administrator;

9. Failure to reasonably protect one's account from unauthorized use (e.g., leaving one's terminal publicly logged on but unattended);

10. Violation of priorities for use of information technology resources as established by an individual facility within the University system;

11. Excessive use of information technology resources, especially when it impedes the mission-related activities of other users, or adversely affects system availability or performance;

12. Use of information technology resources for individual commercial activities that are not approved by the University, for personal private gain, or for political campaigning and similar activities that are inconsistent with the University's tax-exempt status;

13. Violation of software license agreements, including making more copies of licensed software than the license allows (i.e. software piracy); or

14. Sending a crippling number of files across the network (e.g. email "bombing" or "spamming").

VIII. Response, Investigation, and Sanctions

A. Response

1. In the event that University officials are notified of alleged misconduct or illegal activity on the part of a member of the University community, after consultation with Human Resources or the Dean of Students and Legal Counsel, contents of an individual's e-mail, other computer accounts, office computer, or network traffic may be copied and stored to prevent the destruction and loss of information, pending formal review of that material.

2. Except when inappropriate or impractical, 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, efforts will be made to notify the involved individual as soon as possible after the access.

B. Investigation of Allegations

1. When the Vice President for Information Technology, a designee, or the appropriate university system administrator has reason to believe that a violation of this policy may have occurred, he or she may initiate an investigation and suspend technology privileges for the individual(s) involved, pending further investigation.

2. If significant University sanctions are imposed, such action, together with an explanation of the causal events, shall be reported by the Vice President for

Information Technology or the appropriate system administrator to the Dean of Students, in case of students; or, to the Provost or appropriate executive vice president for all others.

C. Sanctions

1. University sanctions are imposed by the appropriate University authority and may include, but are not limited to, limitation or revocation of access rights, and reimbursement to the University for the technology and personnel charges incurred in detecting and proving the violation of these rules, as well as from the violation itself. Reimbursement may include compensation for staff work time related to the violation and for archiving information related to the incident.

2. Disciplinary actions as defined in the Code of Student Conduct, Human Resources Policy and Procedures, and Administrative and Governing Regulations, and Rules of the University Senate may also include any combination of disciplinary action, or civil or criminal liability. The usual rights and privileges of appeal apply.

3. Violation of this policy may also result in the University referring the violation to the appropriate state or federal agency. Violations of KRS 434.840 (Kentucky statutes dealing with unlawful access or use of a computer) shall be referred to the Commonwealth Attorney or the police for investigation and prosecution. Similarly, violations of 18 U.S.C. Sec.1030 (Federal laws related to unlawful access or use of a computer) shall be referred to the Federal Bureau of Investigation.

IX. Appeals

A. In cases where a user's technology privileges are limited or revoked by Information Technology, a user may request a review of the action. The review shall be conducted by Information Technology according to established procedures.

B. In cases where a user’s information is removed by Information Technology or the departmental system administrator, a user may appeal the removal through the relevant administrative process appropriate to the status of the user (i.e., faculty, staff or student).

GLOSSARY

Access right: permission to use University information technology resources according to appropriate limitations, controls, and guidelines.

Commercial purpose: activities by an individual or department where the goal or end involves the buying and/or selling of goods or services for the purpose of making a profit.

Data: a representation of facts, concepts, or instructions suitable for communication, interpretation, or processing by human or automatic means.

E-Discovery: a generic term used to encompass how the legal world of litigation, regulation, and criminal investigation searches, collects, preserves, processes, and produces electronic files. E-Discovery is governed by the Federal Rules of Civil Procedure.

Equitable use: use of information technology resources in accordance with this policy and with the rules of an individual University facility; use of information technology resources so as not to unreasonably interfere with the use of the same resources by others.

File: a collection of data treated as a unit.

Incidental Personal Use: use of information technology resources by members of the University community of support of activities that do not related to their university employment or studies or to other activities involving and approved by the university. Examples include use of email to send personal messages to friends, family, or colleagues, including messages relating to one-time minimal sales or purchase transactions, and occasional use of the web to gain information about personal interests.

Information Technology Resources: information technology devices (personal computers, printers, servers, networking devices, etc.), computing systems and applications, involved in the processing, storage, and transmission of information.

Kentucky Open Records Act: a state law that requires public records to be made available to any person who requests them, subject to certain exemptions.

Password: a string of characters that a user shall supply to meet security requirements before gaining access to a particular technology resource.

Prudent and Responsible Use: use of information technology resources in a manner that promotes the efficient use and security of one's own access right(s), the access rights of other users, and University information technology resources.

Remote Activity: any technology action or behavior that accesses remote site facilities via a University information technology resource.

Remote site: any information technology/network equipment, facility or service not part of, but connected with, University information technology resources via a communications network.

Software Piracy: unauthorized duplication, distribution or use of someone else's intellectual property, including computer software, constitutes copyright infringement and is illegal and subject to both civil and criminal penalties.

Sound Recording Piracy: another form of copyright infringement is the unauthorized duplication or distribution of sound recordings. Federal copyright law grants the copyright owner in a sound recording (typically, a record company) the exclusive rights to reproduce, adapt, distribute, and in some cases, digitally transmit the owner's sound recordings. Sound recording piracy is illegal and subject to both civil and criminal penalties.

System Administrator: any individual authorized by the Vice President for Information Technology, the Provost or appropriate executive vice president, or a designee to administer a particular technology hardware system or its system software.

User: an individual, including student, faculty, staff, or individual external to University, who uses University information technology resources.

User id: a character string that uniquely identifies a particular user to a University technology resource.