University of Kentucky Regulations

Administrative Regulation 10:1

Responsible Office: Information Technology

Date Effective: 8/1/2018

Supersedes Version: 6/4/2008

Administrative Regulation 10:1
Use of Technology Resources

Index

Introduction

Entities Affected

Definitions

Policy

- Eligibility
- Appropriate Use
- Misuse or Abuse of Technology Resources
- Access and Breaches

References

I. Introduction

This *Administrative Regulation* establishes University requirements for the appropriate use of technology resources. This regulation outlines specific rules that each user must follow when using technology resources provided by or through the University, as well as external technology resources to which the University enables or facilitates access.

II. Entities Affected

This regulation applies to all users of technology resources at or through the University, regardless of user affiliation or relation with the University, and irrespective of where the resources are located or accessed.

III. Definitions

A. Data

"Data" means all digital information that is used by or belongs to the University or that is processed, stored, maintained, transmitted, copied on, or copied from University technology resources.

B. Peripherals

"Peripherals" means any external device, such as a flash drive, that contains or receives data from a University technology resource.

C. Technology Resources

"Technology resources" means all software and devices (including, but not limited to, personal computers, laptops, tablets, streaming devices, and smart phones) owned by the University, or the user and which are part of or are used to access:

(1) the University network peripherals and related equipment and software;

(2) data communications infrastructure, peripherals, and related equipment and software;

(3) voice communications infrastructure, peripherals, and related equipment and software; and

(4) all other associated tools, instruments, facilities, and the services that make use of any technology resources owned, operated, or controlled by the University. Technology resources or components thereof may be individually assigned or shared, single-user or multi-user, stand-alone or networked, and mobile or stationary.

D. User

"User" means everyone who is authorized to access a University technology resource.

IV. Policy

A. The University provides technology resources and access to technology resources to authorized users in order to support the University's mission. Use of technology resources must be compatible with the academic, educational, public service, patient care, and research initiatives of the University and with applicable laws, regulations, and licenses. As a condition of use and access to technology resources, each user must comply with this regulation.

B. The use of the University's technology resources and network capacity is a privilege, not a right. The University generally does not monitor or restrict the use of technology resources, but may limit access to or review and monitor technology resources and the use of technology resources when there has been a violation or alleged violation of University regulations, policies, procedures, directives, or state or federal laws.

C. The University preserves the confidentiality of certain data and information that the University maintains about individuals who attend or work at the University, or patients who receive treatment or services at the University. However, users do not acquire an absolute right of privacy regarding their use of technology resources or information or data stored on the University's technology resources. In the case of a violation or alleged violation of University policy or the law, the University may disclose information pertaining to use of its technology resources to University administration, law enforcement, investigating authorities, and others as the University deems appropriate. Except when inappropriate or impractical, users will receive prior notice of such disclosures.

D. Legitimate reasons for individuals other than the account holders to access electronic files, computing infrastructure, network traffic, or to disclose information to third parties includes, but is not limited to:

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

2. Protecting user or system data;

3. Ensuring continued effective unit or 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 federal regulations/rules (e.g., Federal Rules of Civil Procedure for E-Discovery); and

8. Health and safety emergencies.

E. Unit or University system administrators may access or permit access to a user's data if they have permission from the individual and after review or approval by a senior University official (Legal Counsel, HR Vice President, or the Dean of Students). If they receive a request to access an account where the employee cannot give permission for reasons of incapacitation, then permission must be obtained from the Office of Legal Counsel to grant access.

F. University system administrators may access a user's data if they receive a court order directing the University to provide the data, receive a notice of a violation of University policy or directives, or receive a notice of illegal activity.

G. University students, employees, contractors, and vendors will be subject to legal and corrective action as a result of any use of technology resources that is illegal, unauthorized, or in violation of this or any other University policy or directive.

H. Colleges, departments, and other administrative units may issue specific technology policies and procedures that support their organizational missions and requirements. Such policies may be more restrictive than University policy, but shall not be more permissive.

I. Eligibility

In general, access to technology resources is provided to the following users:

a. Students and employees, in support of University operations and initiatives.

i. Students may access and use University technology resources until they graduate or are not enrolled for two consecutive semesters (not including summer). A student's account will be disabled after one inactive semester, and purged after the last enrollment period of the second semester for which the student is not enrolled. Enrollment is determined using University records.

ii. Employees may access and use University technology resources until the termination of their affiliation with the University.

iii. A user whose status as a student or employee has been terminated by the University is no longer authorized to utilize technology resources, even if their access has not been blocked by technology services

1. UK's regulations, policies, procedures, and directives; and

2. Federal, state, and local laws.

b. Individuals not affiliated with the University who are engaged in research or support of University operations and initiatives. These persons may include, but are not limited to, conference attendees,

external research collaborators, external entities under contract with the University, and visitors. The eligibility of these individuals to access technology resources or data requires initial and periodic verification by a sponsor. Requests must be accompanied by the reason for the access, the name and contact information of the sponsor, and the length of time for which the access will be required.

Access to technology resources by retired employees is generally limited to electronic mail and academic or research systems. This access is a recognized benefit to the University community as long as providing these resources is economical and does not adversely affect the operations of the University. In the event that UK resources become constrained, this practice may be restricted or eliminated.

Alumni of the University are not eligible to use technology resources unless eligible under another category.

J. Appropriate Use

Each user is responsible for adhering to the highest standard of ethical, responsible, and considerate use of technology resources. Under no circumstances can University technology resources be used for purposes that are illegal, unauthorized, or prohibited by law or University regulations, policies, procedures, or directives.

a. Specifically, each user of technology resources must:

i. Use technology resources only for authorized purposes in accordance with:

1. UK's regulations, policies, procedures, and directives; and

2. Federal, state, and local laws.

ii. Secure and maintain all computer accounts, passwords, and other types of authorization in confidence, and inform the Office of the Chief Information Officer at cybersecurity@uky.edu immediately if a known or alleged violation of University regulations, policies, procedures, or directives occurs;

iii. Maintain confidential, protected, and proprietary data and information, particularly of data prescribed by law and University policy, in accordance with appropriate security measures;

iv. Be considerate in the use of shared technology resources and network capacity, coordinating with the Office of the Chief Information Officer for "heavy use" operations that may slow daily performance for other users; and

v. Maintain all data in accordance with the State University Model Record Retention Schedule.

b. 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.

c. Users of technology resources must not:

i. Obtain or use another's login credentials or otherwise access technology resources to which authorization has not been expressly given. This obligation includes, but is not limited to, using

another's login credentials to hide an identity or attribute the use of data or technology resources to another user.

ii. Copy, install, or use any software, data, files, or other technology that violate a copyright or license agreement. In particular, each user must not distribute or download copies of copyrighted material without explicit permission from the copyright owner.

Note: Copyright law applies to materials such as games, movies, music, or software in both analog and digital format. Users shall not download an illegally distributed file to a technology resource. Copyright holders regularly notify the University of Kentucky of infringing activity using the procedures outlined in the Digital Millennium Copyright Act of 1998 (DMCA) and other legal procedures. As a service provider, the University must investigate complaints and take action to remove unlawful material. The law provides means for a copyright owner to obtain the identity of a subscriber. If you illegally possess or share copyrighted materials, you may be denied access to the University's technology resources, be subject to corrective actions via the Office of the Dean of Students and Human Resources, and possibly face civil or criminal legal proceedings and sanctions.

iii. Utilize technology resources to create or transmit false or deceptive information, misguided alerts, or warnings, or to participate in any other fraudulent or unlawful activities.

iv. Monopolize or disproportionately use shared technology resources, overload systems or networks with endless loops, interfere with others' authorized use, degrade services, or otherwise misuse or misappropriate computer time, connection time, disk space, or similar resources.

v. Add, modify, reconfigure, or extend any component of the University network (e.g., hubs, routers, switches, wireless access points, firewalls, etc.) without express written authorization from the Office of the Chief Information Officer.

vi. Compromise the security of any data or technology resources or attempt to circumvent any established security measures, for any reason, (e.g. using a computer program to attempt password decoding). Users must not acquire, store, or transmit any hardware or software tools that are designed to compromise the security of technology resources without the express written authorization by the Office of the Chief Information Officer.

vii. Send unsolicited mass mailings or "spamming." Mass mailings must only be sent to clearly identified groups for official purposes, and may not be sent without proper authorization and coordination with UK Public Relations and Marketing.

viii. Install, store, or download software to University technology resources unless such conduct is consistent with the University's educational and academic policies.

ix. Engage in any acts or omissions to intentionally or unreasonably endanger or damage any data or the security or integrity of any data or technology resources.

x. Knowingly access, add, or modify any data without proper authorization.

xi. Utilize University technology resources to promote, solicit, support or engage in any commercial activities on behalf of or for the benefit of any person or entity other than the University without prior authorization from the appropriate University entity.

K. Misuse or Abuse of Technology Resources

a. Allegations of abuse or misuse must be forwarded to the appropriate office for investigation and resolution.

b. Reporting: Apparent or suspected misuse or abuse of UK technology resources must be immediately reported to the Office of the Chief Information Officer at cybersecurity@uky.edu. The IT Security & Policy Office represents the Chief Information Officer with respect to these issues. Where violations of University regulations, policies, procedures, and directives or state or federal law are alleged, appropriate University administrative offices and law enforcement may be contacted.

c. Technical Investigation: In the event of an alleged misuse or abuse of technology resources, a technical investigation or computer forensics may be required and the IT Security & Policy Office will coordinate the gathering and interpretation of relevant information. All investigations will proceed in accordance with applicable University practices, policies, procedures, and directives, and in compliance with applicable laws protecting the privacy of any records or data involved in the incident.

d. Corrective actions: Violations may result in corrective actions such as, but not limited to, terminating access to technology resources, disciplinary action, civil liability, and criminal sanctions. The University may temporarily suspend or block access to any account, data, or technology resources prior to the completion of an investigation when it is reasonable to do so in order to protect data or the integrity, security, and functionality of technology resources, or to otherwise protect the University or its constituents. Except when inappropriate or impractical, users will receive prior notice of sanctions.

L. Access and Breaches

a. Requests for access to and reports of any breaches of managed technology resources must be directed to Information Technology User Services at 859-218-4357.

b. Requests for access to technology resources not managed by ITS must be directed to the administrative office where the service is located. Additionally, requests for use of other technology services (e.g. computers and copy machines) within a specific unit must be directed to the dean, department head, or director of the department in which the service is located.

c. The IT Security & Policy Office is available to provide advice and consultation related to the eligibility of a user to access University technology resources.

References:

Digital Millennium Copyright Act
UK Copyright Resource Center
GR X Regulations Affecting Employment
AR 3:9 Consulting and Other Overload Employment
AR 10:7 Security of Data
AR 10:8 Security of Information Technology Resources
UK HealthCare Policy A13-060 Logical Access Control
UK HealthCare Policy A13-065 Information Risk Management
UK HealthCare Policy A13-070 Information Security
UK HealthCare Policy A13-120 Information Security Incident Response
UK HealthCare Policy A13-130 Information Security Audit Logging

Revision History

3/18/1993, 6/4/2008, 8/1/2018, (1/22/2024, updated contacted information)

Parts of this regulation have been moved to new *AR 10:7 Security of Data* and new *AR 10:8 Security of Information Technology Resources*

For questions, contact: Office of Legal Counsel