University of Kentucky Regulations

Administrative Regulation

Responsible Office: Information Technology Services

Date Effective: 8/1/2018

Supersedes Version: n/a

Administrative Regulation 10:8

Security of Information Technology Resources

Index

I. Introduction

This *Administrative Regulation* outlines the role and authority of Information Technology Services (ITS) in supporting and upholding the security and integrity of the University's information technology environment.

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. Protected Data

"Protected data" means data or information that has been designated as private or confidential by law or by the University. Protected data includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other individually identifiable information), research data, trade secrets, and classified government information. Protected data does not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any data constitutes protected data, the data in question will be treated as protected data until a determination is made by the University.

a. Private data - Private data is any information that the University is under legal or contractual obligation to protect. Examples of private data include employment, research, and student data.

b. Confidential data - Confidential data is data that by law is not to be publicly disclosed. This designation is used for highly sensitive data whose access is restricted to authorized employees. Examples of confidential data include personally identifiable information in student education records, and personally identifiable non-public information about University employees.

These categories of private and confidential data enumerated above are specific to data residing in University systems. Governing Regulation XIV.B.3, Confidentiality of Information, governs the release of information from the University to the public.

D. Public Data

"Public Data" means data that any person or entity either internal or external to the University can access. The disclosure, use, or destruction of public data should have no adverse effects on the University nor carry any liability. Examples of public data include readily available news and information posted on the University's website.

E. Security Breach

"Security breach" means any known or suspected compromise of the security, confidentiality, or integrity of data or technology resources that results in the unauthorized acquisition of or access to data. Good faith access or acquisition of data by an user or unit is not a breach of the security of the system, provided that the information is not improperly used, or subject to subsequent unauthorized access, use, or disclosure.

F. 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.

G. Units

"Units" means any college, program, service, department, office, operating division, vendor, facility user, or other entity or defined unit of the University that has been authorized to access or use technology resources or data.

H. Users

"Users" means anyone who uses a University technology resource.

IV. Policy

A. The University is subject to various regulatory requirements designed to protect the privacy of education records, financial information, medical records, and other personal information maintained by the University. Further, the University maintains confidential research data, intellectual property, and other proprietary information owned, licensed, or otherwise maintained or used by the University. University systems must therefore be properly secured and protected against misuse and unauthorized access. Users must be diligent in their protection of data, use of technology resources, administration and maintenance of systems, response to security threats, and compliance with AR 10.1 and other policies and directives. Information related to intrusions, attempted intrusions, unauthorized access, misuse, or other abnormal or questionable incidents must be reported as soon as possible to ITS Information Technology Services, so the event can be recognized, mitigated, and avoided.

B. Units operating or utilizing technology resources are responsible for managing and maintaining the security of their data, technology resources, and protected information. This requirement is especially important for those technology resources that support or host critical business functions or protected information.

C. The Chief IT Security & Policy Officer (CISO) of ITS has the authority to:

   a. Develop and implement policies necessary to minimize the possibility of unauthorized access to protected information and the University's information technology infrastructure;
   b. Consult and educate users and units about their individual and collective responsibilities to protect data and secure technology resources; and
   c. Take reasonable actions to mitigate incidents or concerns relating to security of data or technology resources. This responsibility includes establishing guidelines, procedures, standards, and security resources, conducting security audits, and providing consulting services to units for all University computer systems or other technology resources.

D. Users are required to report any suspected or known security breaches or flaws relating to the security of University technology resources to the CISO. The CISO will assess reported breaches and flaws and provide advice on an appropriate response. A failure to report suspected or known security breaches or flaws is cause for disciplinary action, including termination of employment. Users should immediately discontinue any use of technology resources or practice that could reasonably lead to a security breach.

V. Procedures

A. The CISO has the authority to assume control over the response to any suspected or known security breach or flaw involving the University's information technology infrastructure, data, and technology resources, regardless of the unit involved. Appropriate remedies may be taken to secure the technology resources and mitigate any unauthorized use, disclosure, or access to data, including the removal of

devices to more secure facilities and denying access to technology resources and/or data. This authority will be exercised if the CISO determines that the unit does not have the means or ability to access or react appropriately to a specific security incident. The CISO may draw upon the experience, expertise, and resources of other University units when necessary and as appropriate.

B. Intrusion attempts, security breaches, and other security related incidents or flaws perpetrated against or involving technology resources either attached to a University operated network or unit must be reported **immediately** to the CISO through either the IT Security & Policy Office at cybersecurity@uky.edu or ITS User Services at 218help@uky.edu or 859-218-4357. Immediate reporting is **critical** for systems supporting vital functions and/or hosting institutional or protected information. Users must:

   a. Report any security breaches in order to obtain advice and assistance;

   b. Report any systematic unsuccessful attempts (i.e., log in attempts, probes, or scans); and

   c. When feasible, send detailed reports as soon as the situation is detected.

C. Upon receiving a report, the CISO will respond according to ITS procedures.

D. In order to protect University data and systems, as well as to protect threatened systems external to the University, the CISO may place limits or restrictions on technology services provided on or from any technology resources.

   a. Limitations may be implemented through the use of policies, standards, or technical methods, and could include (but may not be limited to) usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.

   b. Restrictions may be deployed permanently based on continuing threat or risk after appropriate consultation with affected constituents, or they may be deployed temporarily, without prior coordination, in response to an immediate and serious threat.

   c. Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the effect on University functions caused by the restriction approaches or exceeds risk associated with the threat.

E. In order to protect University data and systems, as well as to protect threatened systems external to the University, the CISO may unilaterally direct that a specific computing resource be isolated from University campus or external networks if:

   a. Information reasonably points to the system as having been compromised;

   b. There is ongoing activity associated with the system that is causing or will cause damage to other University technology resources or data, or to systems of other internal or external users, or where there is significant risk of such damage occurring; and

   c. All reasonable attempts have been made to contact the responsible technicians or unit management, or contact has been made, but the technician or unit managers are unable to or choose not to resolve the problem in a reasonable time.

F. Isolation will be removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as determined between the responsible functional unit and the CISO.

XI. References

Digital Millennium Copyright Act
UK Copyright Resource Center
10:1 Use of Technology Resources
AR 10:7 Security of Data
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

Version History

This is a new regulation. The subject of this regulation was previously part of AR 10:1.

For questions, contact: Office of Legal Counsel