Administrative Regulation

Responsible Office: Information Technology

Date Effective: 8/1/2018

Supersedes Version: n/a

Administrative Regulation 10:7

Security of Data

Index

I. Introduction

This *Administrative Regulation* establishes the responsibilities of all users for the security of data at the University. All users are responsible for protecting the confidentiality, integrity, and availability of data from unauthorized generation, access, modification, disclosure, transmission, or destruction. Specifically, this regulation establishes guidelines and restrictions regarding any and all use of data at or through the University.

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. Data Stewards

"Data Stewards" means the units responsible for the collection, maintenance, and integrity of the data.

C. Peripherals

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

D. Permission Levels

"Permission levels" means the level of privileges granted to each person or unit. The default permission level granted should always be least privileged (i.e., the most restrictive set of privileges needed for the performance of authorized tasks).

E. 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.

F. 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.

G. 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.

H. 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.

I. Users

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

IV. Policy

A. Units operating or utilizing technology resources are responsible for managing and maintaining the security of their data, technology resources, and protected data. Units are responsible for implementing appropriate managerial, operations, physical, and technical controls for access to, use of, transmission of, and disposal of data. This requirement is especially important for those technology resources that support or host critical business functions or protected data.

B. Protected data will not be disclosed except as provided by University policy and procedures or as required by law or court order.

C. All electronic data is classified as public, private, or confidential. Please see Data Classification for a general guide to determine which data classification is appropriate for a particular information or infrastructure system.

D. Although some protected data the University maintains may ultimately be determined to be public records subject to public disclosure under KRS 61.800-884, public records status does not determine how the University classifies and protects data until such a designation is made. Often public records are intermingled with protected data, so all the information and data should be treated as protected until it becomes necessary to segregate any public records.

E. It is the responsibility of data stewards to classify data with input from appropriate University administrative units and legal counsel. However, all users accessing data are responsible for the protection of the data at the permission level determined by data stewards or as mandated by law. Data stewards are responsible for communicating the level of classification to users granted access. Any data not yet classified by data stewards will be deemed confidential. Beyond the classification systems of the University, access to data may be further restricted by law.

F. All data access must be authorized based on minimal need. Enforcing least privileged permission levels limits the damage that can result from accident, error, or unauthorized use. All permissions to access confidential data must be approved by an authorized individual. Written or electronic records of all permission levels must be maintained.

G. Private data may be copied and distributed within the University only to authorized users. Any private data disclosed to authorized, external users must be done in accordance with a Non-Disclosure Agreement.

H. Recipients of confidential data have an obligation not to reveal the contents to any individual unless that person has a valid need and authorized permission from the appropriate authority to access the data. The user revealing such confidential data must have specific authority to do so. Confidential data must not be copied without authorization from the identified custodian.

I. Protected data must not be provided to external parties or users without approval from the appropriate data steward. In cases where the data steward is not available, approval may be obtained by the director or department head of the unit in which the data is maintained, or by an official request from a senior executive officer of the University (e.g., President, executive vice president, Provost, or vice president).

J. When a user who has been granted access either changes responsibilities or leaves the University, all access rights should be reevaluated and any access to protected data outside of the scope of their new position or status should be revoked.

K. Data that is critical to the mission of the University must be located or backed up on centralized servers maintained by the University.

L. The Division of Networking & Infrastructure within Information Technology Services (ITS) is responsible for ensuring that all University communications and network infrastructure are consistent with University standards and follow best security practices. As a result, all University entities planning any IT or infrastructure projects must engage ITS for acquisition of data, voice, video, cybersecurity, and other communication or infrastructure needs. Please see the Business Procedures Manual - Section Q. Information Technology for additional details.

M. Violations of this Administrative Regulation (AR) may lead to disciplinary action up to and including dismissal, expulsion, and/or legal action.

V. Procedures

Complaints or concerns about violations of this or other technology policies should be sent to cybersecurity@uky.edu. After verification of any issues is complete using system or other logs, and in accordance with other applicable policies and procedures, any alleged violation will be reported to the appropriate dean, director, or department head for review and possible action.

VI. References

Business Procedures Manual - Section Q. Information Technology
Digital Millennium Copyright Act
UK Copyright Resource Center
AR 10:1 Use of Technology Resources
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

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