Eastern Kentucky University
Policy and Regulation Library

Administrative Regulation: 11.2.4ADR

Responsible Office(s): Information Technology

Effective: February 22, 2019

Next Review Date: March 1, 2021

Administrative Regulation: 11.2.4ADR
Information Security

Statement

The University reaffirms its commitment to safeguarding University Information Technology (IT) assets in light of evolving technology, communication, and collaboration.

The purpose of this policy is to provide a security framework that will ensure the protection of Eastern Kentucky University information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. University Information may be verbal, digital, and/or hardcopy, individually-controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes. The entire University Community has a responsibility for proper handling and protection of Confidential Information as set out in these procedures.

The University will:

1. Ensure the Chief Information Officer (CIO) designates one or more individuals to identify and assess the risks to Non-Public or Business-Critical Information within the University and establish a University Information Security Plan.
2. Develop, publish, and maintain Information Security policies and procedures for protection of University information, Information Systems and supporting infrastructure.
3. Provide training to Authorized University Users in the responsible use of, but not limited to: information, Applications, Information Systems, Networks, and computing devices.
4. Encourage the exchange of Information Security knowledge, including threats, risks, countermeasures, controls, and best practices both within and outside the University.
5. Periodically evaluate the effectiveness of Information Security Controls.
6. Provide for the confidentiality of Personally Identifiable Information (PII) in accordance with Laws, Regulations, and Policies.

7. Perform a comprehensive risk assessment in regards to the safeguarding of Non-Public or Business-Critical data.

Entities Affected

The entire University Community.

Background

It is the University's responsibility, in compliance with Laws, Regulations, and Policies, to protect the Confidential Information of its constituents and mission-critical functions.

Procedures

I. CONFIDENTIAL INFORMATION

A. All Users are responsible for protecting University Confidential Information that they use in any form from unauthorized access and use.

B. All Users are responsible for protecting their University passwords and other access credentials from unauthorized use.

C. No User shall share their password(s).

D. All access to and use of University Confidential Information must only be for authorized purposes.

E. All access to systems containing University Confidential Information must be for authorized purposes.

F. All persons accessing University Confidential Information must be trained in protecting such information.

G. All Users of University Confidential Information resources must be accurately and individually identified.

H. University Confidential Information must be protected on any user computer or portable device.

I. All servers storing University Confidential Information must be protected against unauthorized access.

J. Electronic and physical records containing University Confidential Information must be appropriately protected when transported or transmitted.

K. Software must be kept up to date on all computers and devices that process or store University Confidential Information.

L. Mechanisms must be implemented to limit the number of unsuccessful attempts to log into an Application or server that processes or stores University Confidential Information.

M. Electronic and physical records containing University Confidential Information must be properly retained until final disposition per University Policy 11.3.1P, Records Management.

N. The University must conduct appropriate due diligence to ensure that third parties that store or have access to University Confidential Information are capable of properly protecting the information and must require such third parties to protect the information.

O. Any actual or suspected loss, theft, or improper use of or access to University Confidential Information must be reported immediately.

II. POINT OF SALE (POS) DEVICES

A. The University will maintain a list and location of such devices.

B. The University will periodically check devices for tampering and substitution.

C. The University will conduct training for personnel utilizing POS devices, to include awareness of suspicious behavior and reporting of suspected or actual tampering or substitution.

Definitions

- **Application(s):** Programs, or groups of programs, that are designed for the end user.
- **Authorized University User:** Anyone who has followed account application procedures and has been granted access to any or all of the computing or Network resources of Eastern Kentucky University for reasons consistent with the mission of the University, and consistent with this policy.
- **Confidential Information:** Personally Identifiable Information or sensitive information including, but not limited to, social security numbers, EKU identification numbers, student grade information, sensitive reports, medical records, military records, student disciplinary records, personnel records, and counseling and disability records.
- **Information Security:** Protection of information by recognizing, removing, and defending against any malicious effects on the University's information.
- **Information Security Controls:** Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.
- **Information Security Plan:** Formal, detailed plan enumerating the steps required to achieve University goals with regard to Information Security.
- **Information Systems:** A combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization.

- **Laws, Regulations, and Policies:** Federal or state laws, administrative regulations, and University policies, regulations, or procedures.
- **Network:** A series of points, or nodes, interconnected by communication paths for the purpose of transmitting, receiving and exchanging data, voice and video traffic.
- **Non-Public or Business-Critical Information:** Information protected from disclosure by federal and state law and regulations.
- **Personally Identifiable Information (PII):** An individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
    - An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
    - A social security number;
    - A taxpayer identification number that incorporates a social security number;
    - A driver's license number;
    - state identification card number;
    - A passport number or other identification number issued by the United States government; or
    - Individually identifiable health information as defined in 45 C.F.R sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g (KRS 61.931 (6) (a-f))
- **Point of Scale (POS) Device:** Electronic device used to process card payments.
- **University:** Eastern Kentucky University
- **University Community:** Students, faculty and staff, as well as anyone doing business for or with the University.
- **Users:** Anyone who uses computing or Network facilities.

Responsibilities

- Chief Information Officer (CIO)
    - Ensure that institutional policies are developed and enforced in accordance with this policy.
    - Responsible for the University's security program and for ensuring that all institutional policies, procedures, and standards are developed, implemented, maintained, and monitored for compliance.
- Students, Faculty and Staff
    - All University employees (students, faculty and staff) are required to ensure compliance with this policy, detailed in the Procedures section.

- Information Technology (IT)
    - Develop, publish, and maintain Information Security policies and procedures for protection of University information, Information Systems and supporting infrastructure.
- University
    - Eastern Kentucky University will provide secure, reliable, and accessible systems for students, faculty, and staff.

Violations of the Policy

Compliance with Information Security procedures developed pursuant to this policy is mandatory. Violations of the procedures constitute violations of this policy. Any division within the University may have additional, more restrictive Information Security policies or procedures which must be followed.

Violations of this policy and the procedures will be handled under normal University disciplinary procedures applicable to the relevant persons or departments. The University may suspend, block or restrict access to information and Network resources when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University resources or to protect the University from liability. The University may refer suspected violations of applicable law to appropriate law enforcement agencies.

Violations of this policy and the procedures can result in disciplinary action up to and including separation from the University and/or exclusion from University programs, facilities and privileges. Violations of law may result in fines and imprisonment.

Regulation Adoption Review and Approval

Regulation Issued

Date	Entity	Action
09/17/20	Dir. Policy Development	Editorial Update
02/22/19	Board of Regents	Approved & Adopted
12/03/18	Faculty Senate	Recommend Approval
09/05/18	Provost's Council	Recommend Approval
07/10/18	Staff Council	Recommend Approval
06/01/18	President Benson	Approved Interim