Information

Encryption of Data

Effective

March 1, 2010

Number

ISO-018 v2.1

Applicability

This policy applies to all University workforce, faculty and student members (including, but not limited to: faculty, staff, students, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, teaching, research or study activity using University resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the University or affiliates.

Administrative Authority

Vice President for Risk, Audit, and Compliance

Responsible Unit

Information Security Office
502-852-6692
isopol@louisville.edu

History

This policy is subject to change or termination by the University at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.

This policy will be reviewed in accordance with the University policy management process to determine if the policy addresses University risk exposure and complies with the applicable security regulations and University direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed.

Approved January 25, 2010 by the Compliance Oversight Council

Shirley C Willihnganz, Executive Vice President and University Provost, Chair of the Compliance Oversight Council

Revision Date(s):

1.0 / February 12, 2010 / Original Publication

1.1 / March 2, 2010 / Clarification of central IT support

1.2 / March 17, 2010/ Replaced "grant reviews" with "confidential or proprietary research data". Clarification of non-compatible devices to specifically include RAID, SCSI and dual/multi-boot platforms.

1.3 / January 29, 2013 / Content Update

1.4 / September 24, 2014 / Content Review

2.0 / March 8, 2016 / Content review/update and update to template format

2.1 / June 15, 2017 / Content review/update to included reference to encryption of university purchased/owned devices per EIT standard 2016

2.1 / August 14, 2018 /Content review/grammar and punctuation updates

2.1 / May 29, 2026 / Minor Revisions

Reviewed Date(s): September 24, 2014; March 8, 2016; June 15, 2017; August 14, 2018; November 16, 2025

Categories

Reason for Policy:

Encrypting sensitive information increases the university's ability to comply with legislation, regulation, contractual obligations, expectations of our constituents and the community at large. and reduces the risk of a data security breach.

Statement:

Encryption of sensitive information maintained on or transmitted by computing devices is mandatory. It is the responsibility of each user to ensure encryption for all University related data not hosted on University enterprise systems. Encryption of data hosted on enterprise systems is the responsibility of IT personnel.

Definitions:

1 - Sensitive information: Information of a confidential or proprietary nature and other information that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or University policy. This includes (but is not limited to) full name or first initial and last name and employee ID (in combination), identifiable medical and health records, grades and other enrollment information, credit card, bank account and other personal financial information, social security numbers, confidential or proprietary research data, dates of birth (when combined with name, address and/or phone numbers), user IDs when combined with a password, etc. See Information Management and Classification Standard.

2 - Computing Devices: Includes but is not limited to workstations, desktop computers, notebook computers, tablet computers, network enabled printers, scanners and multi-function devices, mobile devices, email/messaging devices, cell phones, removable hard drives, flash or "thumb" drives, etc. all hereafter referred to as "computing devices".

3 - Enterprise Systems: Server class computing systems physically maintained in the University's computing center by the Information Technology Department which

features multiple layers of physical security and access control, back-up power, climate control, fire suppression, data back-up and disaster recovery plans, etc. Only a few computing centers elsewhere fit the enterprise systems category. *Servers and computers located in offices, data closets and other areas that do not have the features and dedicated staffing of one of these data centers do not fit the enterprise systems criteria.* See Technical Standards section of this document for compatibility of devices with recommended software and alternative recommendations.

Responsibilities:

Policy Authority/Enforcement: The University's Information Security Officer (ISO) is responsible for the development, publication, modification and oversight of these policies and standards. The ISO works in conjunction with University Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

Policy Compliance: Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the University and/or action in accordance with local ordinances, state or federal laws.