Information

Workstation and Computing Devices

Effective

July 23, 2007

Number

ISO-012 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 July 23, 2007 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 / July 23, 2007 / Original Publication

1.1 / March 15, 2011 / Addition of VPN access

1.2 / June 21, 2011 / Addition of Active Directory language

1.3 / January 29, 2013 / Content Update

2.0 / March 8, 2016 / Review/update content and update to template format

2.1 / June 19, 2017 / Review and updated content to include University owned device encryption per EIT 2016 standard

2.1 / October 10, 2018 / Review and update grammar (should/must, division/department) and punctuation. Add reference to HIPAA/PCI compliance.

2.1 / May 29, 2026 / Minor Revisions

Reviewed Date(s): September 29, 2014; March 8, 2016; June 19, 2017; October 10, 2018; November 16, 2025

Categories

Reason for Policy:

To ensure implementation of computing device controls (university and personal owned) in order to protect the confidentiality, integrity and availability of University data.

Statement:

All computing devices shall:

- If connected to the university network and capable of running active directory, [1] be a part of the university's Active Directory domain, to ensure password synchronization with central authentication services and to facilitate updating of security controls and enterprise software;
- Be maintained in an environment and manner so that access is reasonably restricted to authorized users only;
- Be used in a prudent manner so that data, system and network integrity is maintained to the highest degree reasonably possible; and
- Have operating systems and other software maintained in the most up-to-date and secure manner reasonably possible.

[1] Macintosh computers are capable of using Active Directory but are limited to authentication services only. Mobile devices, such as iPads, utilize synching software to connect to the university network and therefore, are exempt from the Active Directory requirement.

Note 1: All computing devices (including personal and mobile) used within the University that contain or transmit sensitive information or that attach to the university network are covered by this policy.

Note 2: If the standard is not technically possible for the specific computing device then a security exception should be filed, and mitigating controls should be employed. Non-AD connected devices should utilize automatic update processes to ensure updating of system and software security protections.

Definitions:

Computing Devices
Includes but is not limited to workstations, desktop computers, notebook computers, tablet computers, network enabled printers, scanners and multi-function devices, PDAs, email/messaging devices and cell phones, all hereafter referred to as "computing devices".

ePHI
Electronic Protected Health Information - Health information maintained or transmitted in an electronic format that:

1. Identifies or could be used to identify an individual;

2. Is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and

3. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of healthcare to an individual.

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, grant reviews, dates of birth (when combined with name, address and/or phone numbers), user IDs when combined with a password, etc. Sensitive information does not include personal information of a particular individual which that individual elects to reveal (such as via opt-in or opt-out mechanisms) (see *Information Management and Classification Standard*).

Responsibilities:

The **Dean of each school or Administrative Department Head** is responsible for implementation of these security policies and standards, including methods to: (a) Educate the school or department users on computing device security practices. (b) Configure and maintain the school or department computing devices to meet these computing device security standards.

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.

Forms/Online Processes:

VPN - Virtual Private Network

ISO-004 Policy Exception Management Process

ISO-007 User Accounts and Acceptable Use

ISO-008 Passwords

ISO-010 Network Service

ISO-014 Protection from Malicious Software

IS0-015 Backup of Data

ISO-002 Business Continuity and Disaster Recovery

Information Management and Classification Standard