Information

Server Computing Devices

Effective

July 23, 2007

Number

ISO-013 v2.0

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 / January 29, 2013 / Content Review

1.2 / September 24, 2014 / Content Review

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

May 29, 2026 (minor revision)

Reviewed Date(s): September 24, 2014; March 8, 2016; November 16, 2025

Categories

Statement:

The University maintains enterprise class secured data centers for the housing of university servers. All servers used to store, process or transmit sensitive information must be registered with the Information Security Office.

All server computing devices must:

- Be maintained in an environment and manner designed to physically and logically restrict access to authorized users;
- Be used in a manner designed to maintain data, system and network integrity; and
- Have operating systems and other software maintained in the most up-to-date and secure manner reasonably possible.

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.