Information

Network Service

Effective

July 23, 2007

Number

ISO-010 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 / August 19, 2011 / Link change in wireless section

1.2 / January 29, 2013 / Content Update

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

2.1 / June 12, 2017 / Review and clarify remote connection verbiage

2.1 / August 2, 2018 / Review and update grammar, punctuation and removed modem references

2.1 / May 29, 2026 / Minor Revision

Reviewed Date(s): September 29, 2014; March 8, 2016; June 12, 2017; August 2, 2018; November 16, 2025

Categories

Reason for Policy:

The university will provide the required infrastructure for enterprise-wide local area network services, (including wireless) and connections to the internet, internet-2 and other external networks. This policy sets forth standards and requirements for configuring and connecting to the university network in order to maintain security, integrity and availability of resources.

Statement:

The Information Technology division is responsible for the provision and management of enterprise-wide local area network services, including wireless networks. All connections to the network must be via university-approved mechanisms. Only authorized Information Technology staff may access, install, manage, or make changes to network infrastructure equipment including but not limited to enterprise servers, routers, switches or telecommunications equipment.

Related Information:

Related Links:

Wireless support - http://louisville.edu/it/departments/communications/wirelesshttps://louisville.edu/it/departme

ISO-007 User Accounts and Acceptable Use

ISO-008 Passwords

ISO-012 Workstation and Computing Devices

ISO-013 Server Computing Devices

Definitions:

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).*

Spoofing

The use of software or other techniques to appear on the network as something other than reality (masquerading as something you are not). Example: The hacker tricked the system into allowing him onto the trusted network by spoofing the identity of a trusted server.

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.