Information

Protection from Malicious Software

Effective

July 23, 2007

Number

ISO-014 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 Update

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

2.0 / August 13, 2018 / Review and update grammar (should/must, division/department) and punctuation.

2.0 / September 13, 2019 / Update Reason for Policy.

2.0 / May 29, 2026 / Minor Revisions

Reviewed Date(s): September 29, 2014; March 8, 2016; June 13, 2017; August 13, 2018; November 16, 2025

Categories

Reason for Policy:

Protection from malicious software (viruses, worms, trojans, root kits, hostile Active X controls, etc.) must be utilized within the university network.

Statement:

All computing devices must be configured with appropriate safeguards against malicious software. Anti-virus, anti-malware and firewall software must be enabled on all windows based computing devices that attach to the University networks. Non-Windows computing devices should use equivalent safeguards. Servers must be configured so that they are protected by the university's enterprise firewall and meet all other enterprise class configuration, administration and maintenance requirements. All exemptions must follow IS0-004 Policy Exception Management Process.

Responsibilities:

The **Dean of each School or Administrative Department Head** is responsible for the implementation of these security policies and standards so that all computing devices in their areas of responsibility have implemented the appropriate virus protection, anti-malware and firewall controls as outlined in this document and that all such tools are kept current with the most recent updates installed.

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:

Policy exception process: ISO-004 Policy Exception Management Process.

Security Incidents Policy: ISO-006 Security Incidents