Information

Policy Exception Management Process

Effective

July 23, 2007

Number

ISO-004 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 Compliance 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/update content and update to template format

2.0 / June 23, 2022 / Minor edit

2.0 / May 29, 2026 / Minor edit

Reviewed Date(s): September 29, 2014; March 8, 2016; June 12, 2017; May 18, 2018; September 16, 2021; June 23, 2022; October 15, 2025

Categories

Reason for Policy:

The purpose of this policy is to allow university entities the ability to do what is needed to further their area's mission while, at the same time, have reasonable assurance that solutions adopted are in compliance with applicable laws, regulations

and university requirements.

Statement:

Information security considerations such as regulatory, compliance, confidentiality, integrity and availability requirements are most easily met when university constituents employ centrally supported or recommended standards. The University understands that centrally supported or recommended technologies are not always feasible for a specific school, division or other university sub-division. Deviation from centrally supported or recommended technologies is discouraged. However, an information security policy exception may be considered where a justifiable business and/or research purpose exists and where resources are sufficient to properly implement and maintain alternative technology or processes that meet or exceed existing university policies and standards. All policy exceptions must follow the process outlined within this policy.

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.

Forms/Online Processes:

Policy Exception Initial Request Form
Policy Exception Request Template (Word Doc)
Policy Exception Process web page