Information

Data Facility Security

Effective

July 23, 2007

Number

ISO-009 v2.0

Applicability

This policy applies to all persons while conducting/performing work, teaching, research or study activity or otherwise using university resources. Scope/Applicability also 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 annually to determine if the policy addresses University risk exposure and is in compliance 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 per the Policy Management process.

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. / June 21, 2011 / Link Update

1.2. / January 29, 2013 / Content Update

1.3. / September 26, 2013 / Content Review

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

2.0 / June 23, 2022 / Minor edit

Reviewed Date(s): March 8, 2016; June 12, 2017; July 31, 2018; June 23, 2022

Categories

Reason for Policy:

To establish access and environmental controls for areas housing University servers, networking equipment and other computing devices.

Statement:

Data Facilities are controlled facilities devoted to housing servers, networking equipment and other computing devices. Access to the university, school, division or other data facilities must be controlled and restricted to appropriate personnel as

required by their position and job responsibilities.

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.