Information

Backup of Data

Effective

July 23, 2007

Number

ISO-015 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 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 / July 18, 2011 / Backup retention time changed from 30 days to 15 days per the Strategic Technology Executive Committee

1.2 / January 29, 2013 / Content Update

1.3 / April 1, 2014 / Update backup retention time from 15 to 30 days per Enterprise IT Management

1.4 / September 29, 2014 / Content Review

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

2.0 / May 29, 2026 / Minor Revision

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

Categories

Reason for Policy:

Backups are an essential part of disaster recovery and business continuity planning and in ensuring the availability of university information.

Statement:

Regular backups are required for all University related data not hosted on the University enterprise systems and classified as sensitive or proprietary or needed during the course of normal operations. Backups of data must be retained in accordance with University, State or Federal retention guidelines as appropriate for the data being backed-up.

Information Technology must conduct regular backups of all data stored on enterprise servers.

Definitions:

Valuable Information: Information that has significant value to the University's mission and/or result in possible harm to the University, its staff, clients or students if lost. This information may or may not be sensitive information (see Sensitive Information definition).

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).

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.