Information

Cloud Computing and 3rd Party Vendor Services

Effective

November 17, 2014

Number

ISO-023 v2.2

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 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 November 17, 2014 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 / November 17, 2014 / Original Publication

1.1 / February 3, 2015 / Addition of MS 365 to Cloud examples

1.2 / September 3, 2015 / Addition of Syncplicity

2.0 / March 3, 2016 / Modify format for new template

2.1 / June 16, 2017 / Content review/update to MS 365 reference due to migration and University use approval

2.2 / September 4, 2018 / Content review and modification to address all third party services and use of personally acquired services for university business

2.2 / September 17, 2021 / Content update for clarification and to reflect current technology, regulatory and university environment

2.2 / June 23, 2022 / Minor edit

Reviewed Date(s): March 3, 2016; June 16, 2017; September 24, 2018; September 17, 2021; June 23, 2022

Categories

Reason for Policy:

The purpose of this policy is to ensure that university sensitive data is appropriately and securely stored, accessed, or shared when using cloud computing and/or file sharing services or when using the services, software or hardware of third-party vendors and that sensitive data is appropriately protected from misuse or breach in compliance with applicable regulations, laws and university policy.

Statement:

This policy applies to persons using third party service to access, transmit, store or share university sensitive (confidential or proprietary) data. Any such use must maintain the ability to protect the confidentiality, integrity and availability of the data in compliance with applicable regulations, laws and university policy.

Definitions:

Cloud computing is a computing model that allows for easy, on-demand computing resources (networks, servers, storage, applications and services) that can be quickly provisioned and de-provisioned with minimal interaction and is accessible to users via the internet. Cloud computing can be defined as the utilization of servers or information technology hosting of any type that is not controlled by the university. Examples include: Dropbox, Google Drive/Docs, third party email providers such as Gmail and other products that have not been sanctioned by the university.

Responsibilities:

The **Dean of each School or Administrative Division Head** is responsible for the promotion of these security policies and standards.

Procedures for complying with these policies and standards, as well as any additional school or division policies, standards and procedures will be developed and maintained by the designee for each school, division, or other subsidiary unit. All school or division policies, standards and procedures should be well documented, up-to-date and meet the minimum requirements established in this policy and

accompanying standards. Each school or division is expected to ensure compliance with these policies and standards as well as their own policies, standards and procedures.

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 Services, 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:

Information Security Vendor Assessment Form

Information Management and Classification Standard (pdf)

Information Classification and Handling Guide (pdf)