Information

Information Security Responsibility

Effective

July 23, 2007

Number

ISO-001 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

Thanks and appreciation to University of California, Berkeley for elements of this document (http://security.berkeley.edu/IT.sec.policy.html)

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 / January 29, 2013 / Updated policy content

1.2 / September 24, 2014 / Reviewed content

2.0 / March 8, 2016 / Reviewed content modified for template format

2.0 / July 18, 2018 / Grammar and punctuation updates

2.0 / January 18, 2021 / Review with content clarity updates, add reference to Information Mgt Standard

2.0 / June 23, 2022 / Minor edit

Reviewed Date(s): March 8, 2016, June 12, 2017, July 18 ,2018, January 18, 2021; June 23, 2022

Categories

Reason for Policy:

The university recognizes the role of information security and is committed to the protection and safeguarding of the confidentiality, integrity and availability of university information resources. In conjunction with the university's Information Management and Classification Standard, this policy provides a framework for the management and responsibility of information security throughout the university.

Statement:

Each member of the university community is responsible for the security and protection of information resources over which they have control. Resources to be protected include networks, devices, software, systems, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

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 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.