Information
Web and E Commerce

Effective
July 23 2007

Number
ISO 011 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 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 / Content Update
2.0 / March 8, 2016 / Review/update content and update to template format
2.0 / July 31, 2018 / Review and update grammar and punctuation
2.0 / June 23, 2022 / Minor edit

Reviewed Date(s): September 29, 2014; March 8, 2016; June 13, 2017; July 31, 2018; September 16, 2021; June 23, 2022

Categories

Statement:

The web presence of the university is to securely provide information, allow for interactive functions and promote a positive image of the university to other universities, accrediting agencies, funding agencies, the media, prospective students, their families, and the public.

Reasoning:

To establish standards and responsibilities regarding the use and creation of web pages and e-commerce sites.

Definitions:

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.