Information
Sanction Policy

Effective
July 23 2007

Number
ISO 005 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 / June 21, 2011 / Acronym Update
1.2 / January 29, 2013 / Content Update
1.3 / December 10, 2015 / Content review, removal of "Data Center" team reference in ULCIRT2.0 / March 8, 2016 / Review content and update to template format, reference HR Disciplinary Policy
2.0 / July 25, 2018 / Grammar and punctuation updates
2.0 / June 23, 2022 / Minor edit

Reviewed Date(s): September 29, 2014; March 8, 2016; June 12, 2017, July 25, 2018; September 16, 2021; June 23, 2022

Categories

Statement:

The University of Louisville requires that users of university computing infrastructure, devices or data comply with all applicable laws, regulations, statutes and university policies relating to information security and information technology. The University must be prepared to respond fairly and appropriately (1) to violations of law, regulation or university policy relating to information security, (2) when questionable or unacceptable computing practices occur, or (3) where there is non-compliance with information security policy requirements or with reasonable requests for action or cooperation necessary to implement the university's information security policies. Lack of compliance will result in sanctions or other appropriate action.

Related Information:

Organizational Responsibilities:
UofL Faculty, Staff, Students and other Users

Knowledge of violations or of non-compliance with information security policies must

be immediately reported to the University's Information Security Office (ISO) as well as the appropriate administrator for the department or unit in which the violation occurred. Individuals who wish to remain anonymous may contact the University's Compliance Helpline. See ISO PS006 Security Incidents for more information.

The ISO will work with the reporter to determine the administrative level at which the initial advisory should occur and whether other university areas such as Institutional Compliance, Information Technology or the Information Security Incident Response Team (ISIRT) should be notified. The ISO can be reached at isopol(@)louisville.edu. Technology specific violations can be reported to the University's Computer Incident Response Team (ULCIRT) at SecureIT@louisville.edu or, if the violation has potentially serious consequences and requires immediate attention, the violation should be reported to the ITS Help Desk at 502-852-7997 with priority one status requested.

ISIRT/ULCIRT

The University has identified the ISIRT and ULCIRT teams as its authority in developing response plans to information security and technology policy violations and serious security incidents. The teams consist of personnel from the Information Security Office and Enterprise Information Technology. The appropriate team will assess the reported violation and/or incident using an established procedural framework. This framework has been established to apply a consistent methodology to all assessments. Goals of the framework include:

- Documentation of the reported violation or incident;
- Preservation of evidence;
- Impartial assessment of the accuracy of the reported violation or incident, including hearing the particulars from the personnel apparently responsible for the violation;
- Possible escalation of the violation or incident to Human Resources, UofL Department of Public Safety, outside authorities or others;
- Containment and mitigation of the violation or incident;
- Remediation of the violation or incident; and
- Imposition or recommendation of sanctions if and as appropriate.

Established procedures and guidelines are followed when investigating reported

policy violations and security incidents.

Corrective actions and sanctions applied pursuant to this policy shall not supersede or impede any regulatory authority conferred upon other compliance oversight offices at the University of Louisville to apply sanctions or take other corrective actions appropriate to their authority. Corrective actions and sanctions applied pursuant to this policy do not supersede any sanctions imposed by external regulatory bodies.

Corrective Actions and Sanctions Available:

Corrective actions and sanctions available to the University in those circumstances where a violation or non-compliance of information security or technology policy has occurred include, but are not limited to:

- Imposition of a requirement to obtain additional appropriate training;
- Temporary suspension or permanent revocation of computing accounts or computing access rights at the University;
- Requirement to bring self, unit, department or school managed computing resources up to specified and on-going standards or place these resources under the management of the information Technology Department;
- Imposition of a mandate and timetable for corrective or remediating action;
- Letter of Reprimand placed in personnel file;
- Loss of improperly collected data;
- Requirement to make financial restitution;
- Suspension of some or all activities at the University;
- Any action that may be required by applicable law, regulation or contract;
- Any other disciplinary actions available as corrective action in a case of inappropriate behavior by a student, faculty member, staff, administrator or other employee up to and including termination; and
- When appropriate and warranted, a department or unit may be held accountable for fees, charges, fines, or expenses incurred or resulting from or related to any such violation or non-compliance where the unit or department is deemed in whole or part responsible.

Related Links/Information:

The Redbook of the University of Louisville (http://louisville.edu/provost/redbook)
Human Resources Staff Disciplinary Policy

Reasoning:

Sanctions are a requirement of many information security laws and regulations. Sanctions also encourage following the policies, standards and procedures promulgated to help the university maintain the confidentiality, integrity and availability of the university's information and computing infrastructure.

Definitions:

Users - Includes students, faculty, staff, administrators and other employees of the University of Louisville and its affiliated entities and any other individual having a computer account, email address or utilizing the computer, network or other information technology services of the University of Louisville.

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.