

Information

Security Incidents

Effective

July 23, 2007

Number

ISO-006 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 / September 24, 2014 / Content Update

2.0 / March 8, 2016 / Review content and update to template format

2.0 / July 31, 2018 / Grammar and punctuation updates

2.0 / June 23, 2022 / Minor edit

Reviewed Date(s): March 8, 2016; June 12, 2017; July 31, 2018; September 16, 2021; June 23, 2022

Categories

Reason for Policy:

Compromises in information security can include both electronic and hard copy information. Electronic compromises can potentially occur at every level of computing from an individual's small mobile device to the largest and best-protected systems on campus. Incidents can be accidental incursions or deliberate attempts to break into systems and can range from benign to malicious in purpose or

consequence. Regardless, each incident requires careful response at a level commensurate with its potential impact to the security of individuals, [sensitive information](#) and the campus as a whole.

The accelerated pace of technological change and concurrent reliance on electronic information systems has greatly increased both the potential exposure of sensitive information to the world at large via electronic means and the motivation of some to exploit computing devices, computing infrastructure and software either for gain or to cause organizational difficulties. Governmental authorities, regulatory bodies and standards organizations have recognized this new reality and responded with laws, regulations and other measures to motivate organizations to take the steps necessary to minimize or prevent information security incidents before they occur.

This environment means that all persons within the University have an active role in preventing security incidents or in minimizing them if they occur.

For the purposes of this policy an "Information Security Incident" is any accidental or malicious act with the potential to:

- Result in misappropriation or inappropriate modification or disclosure of sensitive information;
- Affect the functionality or continuity of information technology including the infrastructure of the University;
- Provide for unauthorized access to university resources or information; or
- Allow university information technology resources to be used to launch attacks against either other internal resources or the resources and information of other individuals or organizations.

Statement:

The policy of the University of Louisville is to minimize both the frequency and the severity of information security incidents within the University environment. All [users](#) are responsible for and must maintain their university computing/mobile devices and data in as safe a manner as is reasonably possible. In the event of an incident, the standards outlined in this document as well as the related procedures must be followed.

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.

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](#)).

Procedures:

Reporting and Responding to IT Security Incidents

Individuals

- Immediately report lost or stolen computer devices (including mobile devices) to ITS support and the ULPD. The ISO will follow up to determine if there are information security issues related to sensitive or regulated data.
 - Attempt to stop any further damage from an IT security incident by *disconnecting the computer from the campus network (do not turn the computer off)*.
 - Report IT security incidents to ULCIRT at SecureIT@louisville.edu. ULCIRT will help you assess the problem and determine how to proceed.
 - If the incident has potentially serious consequences and requires immediate attention, individuals should report the incident to the ITS Help

Desk at 502-852-7997 and request 'priority one' status.

- Following the report, individuals should comply with directions provided by ITS support staff or ULCIRT to repair the system, restore service, and preserve evidence of the incident.
 - No retaliatory action should be taken against a system or person believed to have been involved in the IT security incident. All response actions should be guided by the ITS security policy and all other applicable university policies.
 - All incidents should be kept confidential unless otherwise instructed by ITS or the ISO. Incidents involving criminal investigation must be kept strictly confidential. University counsel or other officials should be informed of employee subpoenas or requests for documents before any action is taken.
-
- Attempt to stop any further damage from an IT security incident by *disconnecting the computer from the campus network (do not turn the computer off)*.
 - Report IT security incidents to ULCIRT at SecureIT@louisville.edu. ULCIRT will help you assess the problem and determine how to proceed.
 - If the incident has potentially serious consequences and requires immediate attention, individuals should report the incident to the ITS Help Desk at 502-852-7997 and request 'priority one' status.
 - Following the report, individuals should comply with directions provided by ITS support staff or ULCIRT to repair the system, restore service, and preserve evidence of the incident.
 - No retaliatory action should be taken against a system or person believed to have been involved in the IT security incident. All response actions should be guided by the ITS security policy and all other applicable university policies.
 - All incidents should be kept confidential unless otherwise instructed by ITS or the ISO. Incidents involving criminal investigation must be kept strictly confidential. University counsel or other officials should be informed of employee subpoenas or requests for documents before any action is taken.

IT Support Professionals (Tier 1)

Department, college, or unit information technology support professionals have additional responsibilities for IT security incident handling and reporting for both the systems they manage personally for their units and the systems of users within their units. In the case of an IT security incident, Tier 1 support staff should:

- Respond quickly to reports from individuals.
- Take immediate action to stop the incident from continuing or recurring including deactivating or disconnecting the device if required. Lost or stolen devices should be deactivated/disabled immediately and remotely wiped when feasible.
- Report IT security incidents to ULCIRT at SecureIT@louisville.edu. They will help you assess the problem and determine how to proceed.
- If the incident has potentially serious consequences and requires immediate attention, individuals should report the incident to the ITS Help Desk at 502-852-7997 and request priority one status.
- Notify the appropriate college, department or unit administrator that an incident has occurred and that ULCIRT has been contacted.
- Refrain from discussing the incident with others until a response plan has been formulated and restrict information to only those with a need to know.

Follow ULCIRT guidance to repair the system, restore service, and preserve evidence of the incident.

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.

Forms/Online Processes:

[ISO-014 Protection from Malicious Software](#)

Information Security Incident Response Team (ISIRT) [isopol\(@\)louisville.edu](mailto:isopol(@)louisville.edu)

Computer Incident Response Team (ULCIRT) SecureIT@louisville.edu