The primary goal of the information security program is to protect the confidentiality, integrity and availability of University information assets.

Components of the program include:

- Development and communication of information **security policies, standards** and guidelines
- Information **security awareness** and Training
- Information security **incident response**
- Identification, assessment and mitigation of information **security risks**
- Support of University **compliance efforts** and programs related to information security

Overview

The Information Security Office (ISO) serves as the University's resource for guidance on information security compliance and administers the University's Information Security Program. The ISO oversees information security policies and standards; provides compliance oversight, and assessments; coordinates information security efforts, user awareness and incident response. The ISO works in conjunction with IT Enterprise Security, Audit Services, Institutional Compliance and officials in compliance areas such as HIPAA, FERPA, PCI and Export Controls to maintain regulatory compliance and to protect the confidentiality, integrity and availability of all University information assets.

http://louisville.edu/security

Contact Information:

Email: isopol@louisville.edu

Tel: 852-6692 - Kim Adams, CISO

Tel: 852-0567 - Lisa Cooper, Info Sec Analyst

UNIVERSITY OF LOUISVILLE®

UNIVERSITY OF LOUISVILLE®

INFORMATION SECURITY OFFICE

The Information Security Office serves as the University's resource for guidance on information security compliance.

InfoSec

To report a violation or suspected information security incident contact the Information Security Office at: isopol@louisville.edu.

Information Security is everyone's responsibility!

University Policies and Standards

Consistent University Information Security policies and supporting standards provide a common approach to compliance, regulatory and operational requirements and support the University in its research and academic missions. The University's Information Security Policies and Standards were originally approved by the Compliance Oversight Council on July 23, 2007.

University policy details can be found at: http://louisville.edu/security/policies

ISO-001 Information Security Responsibility
ISO-002 Business Continuity / Disaster Recovery
ISO-003 Intellectual Property
ISO-004 Policy Exception Management Process
ISO-005 Sanction Policy
ISO-006 Security Incidents
ISO-007 User Accounts & Acceptable Use
ISO-008 Passwords
ISO-009 Data Facility Security
ISO-010 Network Service
ISO-011 Web Page Guidelines
ISO-012 Workstation and Computing Devices
ISO-013 Server Computing Devices
ISO-014 Protection from Malicious Software
ISO-015 Backup of Data
ISO-016 Inventory/Tracking of Computing Devices
ISO-017 Firewalls
ISO-018 Encryption of Data
ISO-019 Email Archiving
ISO-020 Sponsored Accounts
ISO-021 Voice Mail Policy
ISO-022 Cloud Computing
ISO Glossary
Data Classification and Management Standard

Policy Scope and Applicability

The University's policies are applicable to **all persons** while conducting/performing work, teaching, research or study activity or otherwise using university resources. Also includes all facilities, property, data and equipment owned, leased and/or maintained by the University or affiliates.

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.

What is '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 or 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.

User Responsibilities

Never share or post your user **password** and keep security codes, keys, equipment, etc. secure

Know your **data's sensitivity** level and any regulations that apply to it — handle and safeguard accordingly

Immediately notify your supervisor or the Security Office if you suspect or become aware of an **incident or information breach**

Never share or store 'sensitive' data with **external parties** without appropriate agreements and University approval (includes cloud storage and texting)

University and personal **mobile devices** (laptops, flash drives, tablets, smart phones) must be encrypted if receiving or storing sensitive data

Ensure all University and personal devices are updated with approved **anti-virus software and patches**

Email—always **encrypt 'sensitive' data** when sending outside of the University system by using [SEND SECURE]

Work with your Tier I and follow proper sensitive **data destruction** procedures.

Familiarize yourself with all the University Information Security **Policies** and other responsibilities located at:

http://louisville.edu/security/policies