Date Published: 11-30-2018

Data Protection Standards - Information Security Policy

UNIVERSITY OF HEALTH SCIENCES & PHARMACY in St. Louis

Information Technology
Data Protection Standards - Information Security Policy

Applies to: (examples; Faculty,Staff, Students, etc)

Faculty , Staff , Students , Contractors_Vendors

Policy Overview:

Issued: 11-30-2018

Next Review Date: 03-08-2023

Frequency of Review: Annually

The University recognizes that in certain instances it must collect, store and use Sensitive Information relating to its students, employees, and individuals associated with the University as well as certain types of research data. The University is dedicated to collecting, handling, storing and using Sensitive Information properly and securely.

University Roles Affected by Policy

Any member of the University community, including all faculty, staff, and students, who have access to University records that contain Sensitive Information covered by this Policy must comply with this Policy.

Applies to all active members of the University community, including faculty, students, staff, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University. This policy also applies to campus visitors who avail themselves of the University's temporary visitor wireless network access, and to those who register their computers and other devices through Conference and Event Services programs or through other offices, for use of the campus network.

Definitions:

Term	Definition
Breach of Security	The unauthorized acquisition or use of Sensitive Information that creates a substantial risk of identity theft or other harm. This definition includes the unauthorized acquisition or use of encrypted electronic Sensitive Information where the confidential process or key has been compromised.
Chief Information Security Officer (CISO)	The Information Technology employee designated to serve as the primary person responsible for management of information security.
Electronic	Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.
Employee	Includes all University faculty, staff and students, volunteers, trainees, visiting researchers, and any other individual who provides services to the University, whether compensated or not, and who, in connection with such services, has access to University records that contain Sensitive Information.
Encryption	Transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key.
Information Security Team	Members of the IT department that have been designated to handle security-related questions and issues pertaining to the University. The CISO ("Chief Information Officer") is a member of this team.
Incident Response Team	("IRT") Means the Chief Information Security Officer, the Vice President, Operations, the General Counsel and Chief Compliance Officer, and such other individuals as the IRT may appoint to assist with a Security Incident or Breach.
Record	Any material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics that contain Sensitive

	Information. The term Record includes both paper and electronic material.
Sensitive Information	Information that is designated as Restricted Use, Confidential or Internal Data under the Data Protection Standards.
Users	Anyone that uses our technology services.

Details:

The University is committed to collecting, handling, storing and using Sensitive Information properly and securely. This Policy establishes an Information Security Program to create administrative, technical and physical safeguards for the protection of Sensitive Information throughout the University. The purpose of this Program is to comply with applicable laws and to:

1. Provide a framework for comprehensive stewardship of Sensitive Information;
2. Increase awareness of the confidential nature of Sensitive Information;
3. Eliminate unnecessary collection and use of Sensitive Information;
4. Protect against anticipated threats or hazards to the security or integrity of Sensitive Information; and
5. Protect against unauthorized access to or use of Sensitive Information in a manner that creates a substantial risk of identity theft, fraud or another misuse of the data.

Procedures:

1. **CISO and Enterprise Risk Management Committee**
   a. CISO
      The University's CISO shall, in consultation with the Enterprise Risk Management Committee, maintain a list of categories of information that will be included within the definition of Sensitive Information and prescribe appropriate levels of protection in a series of procedures collectively known as the Data Protection Standards. The CISO may consult with the ERM Committee concerning the administration of this Policy. The CISO may assign responsibility for developing more specific Information Security Guidelines to appropriate central University offices with responsibility for and expertise concerning the collection, use, storage and disposal of particular types of Sensitive Information. The CISO shall provide a mechanism for reporting any suspected Breach of Security and shall respond to any reported Breach of Security as outlined below.
   b. University Common Services and Information Security Team
      The CISO shall convene an Information Security Team to assist with the administration of this Policy and to help ensure compliance. In addition, the Information Security Team may advise University offices charged with the development of Information Security Guidelines and review Information Security Guidelines.
   c. Data Protection Standards
      The CISO, in consultation with the Enterprise Risk Management Committee, shall identify categories of Sensitive Information and the appropriate safeguards required to protect each category defined in the Data Classification Policy. The Data Protection Standards shall specify administrative, technical and physical safeguards for the protection of Sensitive Information. The ERM Committee may review and the CISO shall approve the Data Protection Standards.
   d. Training
      The CISO or the CISO's designee, together with the Enterprise Risk Management Committee, shall develop a training program for Employees who will have access to Sensitive Information.
   e. Vendors and Service Providers
      The CISO or the CISO's designee, together with the Information Security Team, will recommend that University vendors, service providers or any other third-party to whom the University provides Sensitive Information be required to meet appropriate criteria or agree to appropriate contract terms before being granted access to Sensitive Data.
   f. Program Review
      At least annually the CISO, together with the Information Security Team, shall review the Information Security Program and the Data Protection Standards. During the course of the review, the CISO and the Information Security Team shall review any Breach of Security that is reported to outside authorities, including the results of any investigation and the University's response to any Breach.
2. **Incident Response Team**
   a. The Incident Response Team shall review any suspected Breach of Security of Sensitive Information as specified in the Security Incident Response Policy.

Responsibilities:

Position/Office/Department	**Responsibility**

The University's Chief Information Security Officer (CISO)	The University's Chief Information Security Officer is responsible for the administration of this Policy and the Information Security Program across departments and units that maintain Records in any format. The University's CISO shall oversee, with the assistance of the Enterprise Risk Management Committee the administration of this Policy, including developing procedures concerning the review, oversight, and governance of this Policy, and including any necessary training. University Employees may request, collect, store or use Sensitive Information only as permitted by this Policy, the Data Protection Standards and practices required by his or her unit or department. Every member of the University community should strive to minimize the collection, handling, storage and use of Sensitive Data. Only those who have a legitimate business need to access Sensitive Data should do so, and for as limited as time as possible. Minimize or eliminate the collection, handling, storage and use of Sensitive Data whenever and wherever possible.

Resources:

Data Protection Standards policies

Digital Millennium Copyright Act Policy

Policy Contacts:

Name	**Contact Information**
Lewis, Zachary, AVP IT	Zachary.Lewis@uhsp.edu, 314-446-8402
Knoll, Eric, Vice President Operations	Eric.Knoll@uhsp.edu, 314-446-8375