ST. LOUIS COLLEGE of PHARMACY

College Services & Information Technology
Security Incident Response Policy

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

Faculty , Staff , Students , Contractors_Vendors

Policy Overview:

Issued: 09-28-2016

Next Review Date: 06-15-2022

Frequency of Review: Annually

University of Health Sciences and Pharmacy in St. Louis ("University") has adopted this policy to establish an Incident Response Plan ("IRP") to manage the process for responding to a possible Security Incident involving Customer Information ("CI") or Personally Identifying Information ("PII") as defined below. The policy is intended to ensure a consistent process to follow when responding to any Security Incident, to mitigate potential risk and harm to affected parties, and to provide for post-incident review to facilitate appropriate changes to improve business practices for safeguarding and handling of Personal Information.

This policy applies to all faculty, staff, student workers, temporary employees, consultants, and vendors.

Definitions:

Customer Information ("CI") means any record containing nonpublic, personally identifying information about a student or a Customer that is handled or maintained by or on behalf of the University or its affiliates. The term includes Personally Identifying Information ("PII") that is: (i) provided to obtain a financial service from the University, or (ii) financial service with the University. Examples of a covered financial product or service include offering or providing credit or debit cards and student loans, grants, or scholarships. Examples of CI related to a financial product or services include tax or financial information obtained from a student or the student's parent in connection with a financial aid award or application, income and credit histories relating to a credit card or loan application, account balances, the amount of funds transferred or disbursed to a student, and debt collection activity. Generally, nonfinancial information about students or information related to employee group benefits such as retirement plan participation levels are subject to other privacy or security requirements under other laws such as FERPA or ERISA.

Security Incident means the attempted or unauthorized access or acquisition of CI or PII that compromises the security, confidentiality, or integrity of such information. Good faith acquisition of CI or PII by a University employee or agent for a legitimate purpose is not a breach provided that the information is not used in a manner that violates the law or harms or poses an actual threat to the security, confidentiality, or integrity of the information.

Incident Response Team ("IRT") means the Director, IT, 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.

Incident Response Team Coordinator means, in the case of electronically stored or transmitted CI or PII, the Director, IT, and with respect to CI or PII in physical form, the Vice President Operations.

Information Security Program (ISP) means the policies and practices implemented by the University to secure CI or PII.

Personally Identifying Information ("PII") means the following information or data that is stored or transmitted in any form that involves an individual's first name or first initial and last name in combination with any one of the following: social security number, driver's license or unique identification number created or collected by a government body, financial account number, credit or debit card number in combination with any required security code, access code, or password, medical information, or health insurance information. PII also includes information that consists of direct or indirect identifiers covered under the Family and Educational Rights to Privacy Act including the name and address of the student or family member, unique identifiers, date or place of birth, parent's names, or other information which can be used to determine the identity of the student directly or indirectly through linkages to other information.

Details:

The IRT is responsible for identifying, and coordinating the University's response to any suspected or actual Security Incident including completing a post-incident assessment and report, and making recommendations to the President for improving the ISP.

Procedures:

1. Incident Detection, Containment, Remediation
    a. Anyone suspecting or noting a potential Security Incident should immediately contact the appropriate IRT Coordinator.
    b. The IRT Coordinator will work with the appropriate internal or external resources to determine if there has been a Security Incident. The IRT will classify the incident as a low-risk or high-risk incident based on the factors listed in Appendix A.
    c. The IRT Coordinator will report any high-risk incident to the IRT for handling and notify the President, President's Staff member(s), and department manager(s) responsible for the affected unit(s). The IRT Coordinator will engage IT and department management for the affected units to assist in handling any low-risk incidents.
    d. In the event that a system is compromised, containment may include, but is not limited to, the following:
        - Aggressive monitoring of all systems to determine the extent and severity of the breach and initiate appropriate containment protocols.
        - Isolating the compromised systems.
        - Disabling compromised accounts and related processes.
        - Compiling a list of IP addresses involved in the incident, including log entries if possible, and forward the data to IRT Coordinator.
        - Changing passwords or credentials.
        - Backing up local password files and searching password change activity.
        - Notifying the IRT Coordinator to authenticate users.
        - Notifying the owners of the compromised accounts and reissuing credentials.
        - Identifying the cause of the incident and removing the threat.
        - Rebuilding and re-establishing the system.
        - Performing a network vulnerability scan to identify and resolve security issues that might be used in future attacks against the system.
        - Comparing the system's original baseline against information gathered during the investigation phase and to test and verify functionality and restore to operating environment level.
        - Performing ongoing system monitoring to ensure system integrity and detect incident recurrence.
    e. In the event that a physical storage space has been accessed or compromised, containment may include, without limitation, the following:
        - Taking an inventory of any CI or PII that has been compromised
        - Reestablishing security of CI or PII until an investigation has been completed
        - Changing locks, keys, card readers, or security codes for existing storage space or move CI or PII to a more secure location
2. Incident Response – Breach Notification
    a. If a Security Incident involves a suspected privacy breach, the IRT Coordinator will immediately notify the IRT and the President.
    b. The General Counsel will notify the University's insurance carrier or administrator to coordinate covered loss prevention services.
    c. When appropriate, the General Counsel will coordinate engagement of an incident response expert or law enforcement authorities to conduct an investigation and Coordinate any legal notification requirements (statutory or contractual
3. Post–incident Review and Report
    a. The IRT Coordinator will convene a meeting of the IRT within forty-eight (48) hours of completion of the incident response to prepare an Incident Report as outlined in Appendix B. The Incident Report will be submitted to the President and Chair of the Enterprise Risk Management Committee.

Responsibilities:

Position/Office/Department	**Responsibility**
Director, IT	Serves as the IRT Coordinator and is responsible for managing and responding to any Security Incident involving IT, prepares the incident report, and maintains related audit records and any logs or documentation.
General Counsel and Chief Compliance Officer	Provides legal advice throughout the discovery, investigation and remediation process on compliance, insurance claims reporting, privacy, security, and reporting issues, including assisting in developing the communication plan to impacted individuals and notifying law enforcement and governmental authorities as required by law.
Vice President, Operations	Serves as the IRT Coordinator and is responsible for managing and responding to any Security Incident involving CI or PII in physical

	form, prepares the incident report, and maintains related audit records and any logs or documentation.

Resources:

Family Educational Rights to Privacy Act, 20 USC Section 1232g, 34 CFR Part 99

UHSP Academic Catalog, Family Educational Rights to Privacy Act Policy

Information Technology Customer and Personally Identifying Information Security Policy

Missouri Revised Statutes 407.1500

Policy Contacts:

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