Information Security Incident Response Policy

Effective Date: December 2018

Office: Information Technology

PURPOSE:
This Security Incident Response Policy establishes policy and procedures for responding in the event of a compromise or breach resulting from an information security incident.

REFERENCE DOCUMENTS/ RELATED INFORMATION:

Systems and Network Usage Policy

SCOPE:
All employees, students and associates of the University.

POLICY HISTORY:
2.0 – 12/3/2018

Overview

This Security Incident Response Policy establishes policy and procedures for responding in the event of a compromise or breach resulting in the unauthorized access, theft, or loss of a University data system, storage device, or records storage, including but not limited to: servers, secured PCs, hard drives and flash drives. This policy also includes physical records containing Personally Identifiable Information (PII). University employees should always err on the side of caution and report any suspected security incident or breach regardless of the content of the device or records. Incidents may be reported to the IT Help Desk at help@uindy.edu, (317) 788-3318 or to any member of Information Technology (IT).

Policy Statement

The University of Indianapolis Information Security Incident Response Policy is summarized as follows:

- All incidents or suspected incidents must be reported to a member of the Core Security Incident Response Team (SIRT).
- The SIRT member along with the Chair of the SIRT shall determine if suspected incident is considered an Information Security Incident per definition below.
- The SIRT shall expand notice to other subject matter expert teams as applicable.
- The Chair of the SIRT shall be responsible for
    - Coordinating communication
    - Leading remediation team
    - Conducting Forensics Investigation
    - Ensuring a timely closure of all security incidents
    - Ensuring any follow-up tasks or process improvements are completed
- The SIRT shall investigate and collect all details surrounding the incident.
- Evidence must be cataloged and preserved by the best possible means. Evidence might include:
    - Log files
    - Screenshots depicting pertinent details
    - Video evidence
    - Configuration files or details
    - Screenshots of any of the above
- The Response Team shall advise relevant campus departments and senior administrators and involve them in remediation as necessary.
- The Response Team along with General Counsel will activate Incident Response Professional Services if determined necessary by the SIRT and General Counsel
- Remediation steps will be performed, which may include:
    - Providing notice to relevant external organizations such as credit card processors and the Indiana Secretary of State
    - Working with affected individuals/departments to minimize further exposure
    - Notifying clients affected by the incident
    - Revoking access rights
    - Patching systems
    - Configuration changes
- The Response Team shall review existing policies and processes and provide recommendations on additional safeguards to prevent future incidents.
- An incident report shall be created and should include incident details, evidence, lessons learned and recommendations for process improvement.
- This policy shall be reviewed on an annual basis.

Response Teams

Core Team

The following individuals or their delegates shall be included in the core response team and will be notified of any incident:

- Sr. Director of Security, Systems & Security - Information Technology
- Security Specialist
- General Counsel
- VP & CTO - Information Technology
- Risk Manager
- VP for Student & Campus Affairs (as needed, if student related)
- VP of Communications and Marketing

Additional ad-hoc teams of subject matter experts may be assembled and notified depending on the type of breach. Teams may include, but are not limited to:

- *PCI-DSS Team* - cases concerning the loss of financial data including credit cards or other financial account information
- *HIPAA Team* - cases concerning the loss of patient health record data
- *FERPA & Academic Integrity Team* - incidents relating to unauthorized access to grades, exam, and transcript data
- *Network Security Team* - incidents regarding unauthorized remote access to systems
- *University Police* - incidents which include possible criminal activity

Incident Definition

For the purposes of this document, a security incident is any suspected or confirmed compromise of university data through unauthorized access, loss or theft. This extends to not only computer systems or networks where data is collected, processed, stored or transmitted, but also includes any material or records that contain university data (paper forms, records etc.). This policy extends to any university-owned equipment, storage device, physical documents, or data that may be off-campus at the time of the incident. In order to improve processes and prevent future breaches, it is imperative that any attempted breach be reported regardless of success or the content of any data obtained. Examples of incidents may include:

1. Loss of information confidentiality (data theft)
2. Compromise of information integrity (damage to data or unauthorized modification)
3. Theft of physical IT asset including computers, storage devices, printers, etc
4. Damage to physical IT assets including computers, storage devices, printers, etc
5. Denial of service
6. Misuse of services, information, or assets
7. Infection of systems by unauthorized or hostile software
8. Any attempt at unauthorized access
9. Unauthorized changes to organizational hardware, software, or configuration
10. Reports of unusual system behavior
11. Responses to intrusion detection alarms
12. Violations of campus computer security policies and standards