XAVIER UNIVERSITY

Cyber Security Incident Response

Effective: 1/25/2021

Last Updated: N/A

Last Reviewed: 1/25/2021

Responsible University Office: Information Technologies

Responsible Executive: Associate Provost and Chief Information Officer

Scope: Xavier University Faculty, Staff, Retirees, Alumni, Students, and non-employee associates.

A. REASON FOR POLICY

This policy defines the responsibilities for users and Information Technologies to respond to cyber security incidents that occur within the University's scope of control.

B. POLICY

All Xavier University Faculty, Staff, Retirees, Alumni, Students, and non-employee associates must report all suspected loss of confidentiality, integrity, and availability regarding Xavier systems or data.

Xavier Information Technologies establishes and maintains a cyber security incident management plan to address a cyber security incident from a suspected loss of confidentiality, integrity, and availability regarding Xavier systems or data.

The cyber security incident management plan:

- Defines roles and responsibilities.
- Provides communication guidelines.
- Defines a high-level incident response procedure.
- Provides guidance to ensure immediate and comprehensive response to minimize the impact and scope.
- Is reviewed, evaluated, and updated as needed.

C. DEFINITIONS (if applicable)

- Confidentiality: Protection of systems or data so that only authorized users have access.
- Integrity: Making sure only authorized and approved changes are made.
- Availability: Making sure that systems are available when users need them.
- Cyber security incident: When a system or data has a loss of confidentiality, integrity, or availability through user error or intentionally by an attacker.

D. PROCEDURES

- Information Technologies provides appropriate training of resources expected to respond to security incidents, as well as the training of general employees regarding Xavier University's expectations of them in regard to cyber security safety responsibilities.
- Information Technologies executes the cyber security incident management plan upon any reported security incident.
- Any suspected loss of confidentiality, integrity, and availability regarding Xavier information systems and data must be reported to the Information Technologies Help Desk by calling (513) 745-4357 or sending an e-mail to helpdesk@xavier.edu.

F. HISTORY

Policy created: 1/25/2021