Coppin State University

Information Technology Division
Policies and Procedures

Policy #: **ITD – GEN – 007** **Version: 04**

Subject: **CSU Incident Reporting and Escalation Policy** **Effective Date:** **10/01/2017**

Approved by: **Approval Date:** **04/04/2018**

Review Date: **04/04/2018**

I. Purpose

This policy governs the University's general response, documentation and reporting of incidents affecting computerized and electronic communication information resources. Incidents may include: theft; intrusion; misuse of data; denial of service; corruption of software; computer-and electronic communication-based FERPA violations; other activities contrary to the University's Acceptable Use Policy; and incidents reported to Coppin State University by other institutions and business entities**.**

II. Policy

With regard to incidences involving campus systems, all users are required to comply with appropriate Computer User and Internet Access Policies as well as all USM and state notification laws.

Any member of the CSU community as well as individual or organization outside of CSU may refer a suspect activity or concern to the Information Security Office. Once identified, the Information Security Office will use standard internal procedures to log and track incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, and refer to others or otherwise address as appropriate.

III. Procedure

The Information Security Office representative will be responsible for communicating the incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the incident. A detailed description of the Incident Response Procedure including contacts may be found in the Incident Response Procedure, ITD-GEN-007P.

The Information Security Office will establish a response team comprised of the CIO and representatives from each relevant IT department. Additional personnel may be included as needed.

The Information Security Office maintains internal procedures for incident logging, tracking and reporting, for evidence custody and related practices.

The Information Security Office will ensure that incidents are appropriately logged and archived. Incident reporting will be provided by the Information Security Office to the CSU Chief Information Officer (CIO).

A response or remediation plan defined by this policy may be preempted as required or at CSU's discretion by the intervention of law enforcement or federal and state executive officials.

Wherever possible, the University will undertake to prevent incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its IT resources.

As per USM BOR requirements, incidents involving the compromise of personal information (as defined under State Government Article 10-1031, see Section III) must be reported to the USM CIO's Office.

IV. Definitions

The following terms apply for the purpose of this policy. Definitions for these terms may be found at https://lookup.coppin.edu/cpd/Pages/Home.aspx:

Computer

Cyber-Attack

Denial of Service

FERPA

Incident

Network

Network Infrastructure

Policy

Protected Resource

Risk

Scanning

Server

Severity

Software

Trusted Entity

Un-trusted Entity

Vulnerability

V. References

- Policy: ITD-CNS-002, CSU System Monitoring Policy
- Policy: ITD-CNS-003, CSU Firewall Policy
- Policy: ITD-GEN-004, CSU Illegal File Sharing Prevention Policy
- Policy: ITD-GEN-005, CSU Student Computer Use and Internet Access Policy
- Policy: ITD-GEN-006, CSU Faculty/Staff Computer Use and Internet Access Policy
- Policy: ITD-GEN-011, CSU IT Security Program
- Policy: ITD-CNS-012, CSU Intrusion Prevention and Detection
- Procedure: ITD-GEN-007P, Incident Response Procedure