CMU
CENTRAL MICHIGAN UNIVERSITY

MANUAL OF UNIVERSITY POLICIES
PROCEDURES AND GUIDELINES

Title/Subject: **INFORMATION SECURITY INCIDENT RESPONSE POLICY**

Applies to: ☒ faculty ☒ staff ☒ students ☒ student employees □ visitors ☒ contractors

Effective Date of This Revision: November 1, 2021

Contact for More Information: Office of Information Technology

□ Board Policy ☒ Administrative Policy ☒ Procedure □ Guideline

BACKGROUND:

A formal information security incident response process allows the Office of Information Technology to identify, investigate, and respond promptly and appropriately to information security concerns. The process mitigates for possible harmful effects, protects the University data and information technologies, improves response in future events and incidents, and ensures the University fulfills its response obligations. This policy requires the University to follow a formal response procedure for identifying, investigating, tracking, and properly responding to information security concerns.

DEFINITIONS:

A. ***Security event*** means any unconfirmed or reported concern or complaint related to the inappropriate access, misuse, theft, or compromise of the University's information, information technologies, or information systems.

B. ***Security alert*** means any confirmed event or concern, related to the inappropriate access, misuse, theft, or compromise of the University's information, information technologies, or information systems that merits follow-up tracking and reporting, or action to remediate. Security alerts also include trusted, automated-alarms or other reported detections of known-malicious activity or high-risk, exploitable vulnerabilities. Security alerts requiring investigation and/or significant follow-up or non-routine action are escalated to incident status.

C. ***Security incident*** means any confirmed inappropriate access, misuse, theft, or compromise of the University's information, information technologies, or information systems, requiring investigation and/or significant follow-up, and/or non-routine action. Security incidents requiring formal breach response are escalated to breach status.

D. ***Security breach*** means any confirmed inappropriate access, misuse, theft, or compromise of the University's Protected or Restricted data or information technologies requiring formal breach response, reporting, and/or notification(s).

POLICY:

The Office of Information Technology will follow a formal incident response procedure for identifying, investigating, tracking, and properly responding to University information security concerns.

Information security concerns will be responded to promptly and appropriately to ensure proper handling and consideration, and to mitigate for harmful effects, including escalation to technical response and/or administrative teams as necessary, to protect the University data and information systems, and meet University response obligations.

Authority: Robert O. Davies, President
History: 2018-07-1;
Indexed as: information technology; information system; security alert; security breach; security event

PROCEDURE:

Information security concerns, complaints, and inquiries shall be reported to the OIT help desk. OIT staff will then create a ticket to begin formal tracking and resolution, or re-assignment. Security events not immediately resolvable will be assigned to the OIT Information Security Office (ISO) for evaluation. Security events that become security incidents will follow the formal response through the process(es) described in Information Security Incident Response Procedures.

RELATED POLICIES AND OTHER RESOURCES:

Responsible Use of Computing Policy
Data Stewardship Policy
Information Security Policy
Information Security FAQ

AMENDMENTS AND ADDITIONS:

The Chief Information Security Officer ("CISO") may approve exceptions to this policy. All amendments and additions to this policy will be drafted by a committee convened by the CISO and will be reviewed by the President and his cabinet. Changes in this policy will be appropriately publicized.

Central Michigan University reserves the right to make exceptions to, modify or eliminate this policy and or its content. This document supersedes all previous policies, procedures or guidelines relative to this subject.