Cybersecurity Incident Response Policy

Created by Townsend, Jeremy W, last modified by Killian, Susan A on Sep 30, 2024

University of Maryland Eastern Shore

Office of Information Technology

Information Technology Incident Response Policy

Date: July 18, 2018

Purpose

Universities are experiencing an increase in the number of cybersecurity incidents. Incidents happen in a variety of ways including malware, ransomware, phishing attacks, denial of service attacks, or any threat that potentially compromises information technology operations or institutional data.

The incident response policy is intended to provide both guidance and procedures for the university follow in the suspected event of a cybersecurity incident.

Scope

This policy seeks to assist the university in mitigating the risks from computer security incidents by providing guidelines on responding effectively and efficiently. The primary focus of this policy is detecting, analyzing, prioritizing, and handling suspected incidents.

Policy

A suspected cyber security incident may be reported by any member of the campus community. When a potential incident has been detected the person identifying the suspected incident (the reporter) university cybersecurity officer.

Cybersecurity Officer	**Telephone**	**email**
Mark Van Pelt, Waters Hall	410-651-8200	MJVanPelt@umes.edu

1. All incidents and suspected incidents will be tracked and recorded by the Cybersecurity Officer. All incident records will be maintained for three years or longer, as required under relevant regulations.
2. The Cybersecurity Officer will assemble an ad-hoc **response team** consisting of the reporter, data steward/owner, appropriate department heads, the Chief Information Officer (CIO), the Director of Public Relations, and University Counsel.
3. The response team will determine the breadth and depth of the suspected incident based on an incident evaluation and review of appropriate logs and other information sources. External resources may be called into to assist with the analysis. The president and president's cabinet will be notified of the suspected incident.
4. The University Counsel and Chief Information Officer will determine if the incident warrants a notification of the effected individuals, campus community, or the public.
5. Incidents involving the compromise of personal information (as defined under State Government Article 10-1031) must be reported to the University System of Maryland office of the CIO.
6. Any notification of the campus community or the public will be coordinated by the UMES Office of Public Relations.

Term	**Definition**
Cybersecurity Incident	A verified event of set of events that has or may result in a change to the confidentiality, availability of university information systems, networks, or data and for which a directed response may be required to mitigate the associated damage or risk. An occurrence that constitutes a violation or imminent threat of violation security policies, security procedures or acceptable use policies may also be considered an incident.
Data Steward/Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection. Processing, dissemination, and disposal.

Related Policy References

Maryland Cybersecurity Incident Response Policy
https://dbm.maryland.gov/benefits/Documents/Attachment%20E%20-%20Maryland%20Cybersecurity%20%20Incident%20Response%20Policy.pdf

Cabinet approval pending. 12/13/18