UMass | Dartmouth

Information Security Incident Response Policy

Policy Number	ITS-008
Effective Date	July 15, 2020
Responsible Office / Person	CITS
Related Policies	ITS-001: Acceptable Use of Information Technology Resources Policy ITS-006: Information Security Policy
Additional History	

I. Introduction

The purpose of the policy is to establish the goals and the vision for the information security incident response process. This policy will clearly define to whom it applies and under what circumstances, it will include the definition of an information security incident, as well as outline the primary elements of the incident response process along with the expectations for reporting suspected incidents. UMass Dartmouth is committed to protecting its students, employees, partners and the University from illegal or damaging actions by individuals, either knowingly or unknowingly.

UMass Dartmouth's intentions for publishing an information security incident response policy are to focus significant attention on the risk of information security incidents. It is also to document how UMass Dartmouth's established culture of openness, trust and integrity should respond to such activity. This policy further sets the expectations that any individual who suspects that a theft, breach or exposure of UMass Dartmouth's information systems has occurred, should immediately contact the University.

By approval of UMass Dartmouth's Chancellor, this policy exists in conjunction with all other institutional policy.

II. Policy Statements

A. Overview

An information security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or services used or provided by UMass Dartmouth and may occur within the UMass network or with an outside entity. An incident will meet one or more of the following:

- Any potential violation of Federal law, Massachusetts law or UMass Dartmouth Policy involving a UMass Dartmouth IT asset or sensitive or protected information in any form.
- A breach, attempted breach or other unauthorized access of a UMass Dartmouth IT Asset. *Unauthorized access* is any action or attempt to utilize, alter or degrade a UMass

MK

Dartmouth owned or operated IT resource in a manner inconsistent with UMass Dartmouth IT policies.

- Any Internet malware, viruses, or phishing attacks.
- Any conduct using in whole or in part the UMass Dartmouth Information Technology Asset which could be construed as harassing, or in violation of UMass Dartmouth Policies.
- The loss or theft of a UMass Dartmouth computing device (including desktop, laptop computers, mobile devices, and point of sale devices) or the loss of any personal computing device containing UMass Dartmouth information.

Security incidents involving UMass Dartmouth owned devices or personal devices containing sensitive UMass Dartmouth data can have serious consequences. It is the responsibility of UMass Dartmouth to investigate and respond to potential incidents promptly and efficiently. This helps protect the UMass Dartmouth's assets (e.g., data, computers, networks) and supports compliance with state and federal law, and company policy. UMass Dartmouth will develop and implement a response program to address incidents of unauthorized access to University information.

B. Program Elements

UMass Dartmouth's response program includes the following:

- a mechanism for in-scope clients and third parties to submit a potential security event for assessment
- assessment of the nature and scope of an incident, and identification of what information systems and types of information have been accessed or misused.
- an approach to prioritize incidents and bring University resources to bear to address the potential risk these incidents pose to the University and its stakeholders.
- guidelines for interaction with other organizations including regulators, state and/or federal officials, and law enforcement authorities.
- guidance for notifying impacted end users, vendors, and/or other third parties when warranted.
- high-level criteria, steps, and considerations for information across University campuses and with outside entities
- evaluation of incidents and the University's response in order to understand how to improve the University's cyber security posture as well as improvement of the incident response plan in future iterations.

In order to deliver on these elements, UMass Dartmouth may engage with other campuses and external organizations in order to share information and resources to evaluate and address the incident as well as restore the IT environment to a secure state of operations. It is expected that UMass Dartmouth will need to provide access to information security professionals from other UMass campuses, the UMass President's office, legal advisors and / or forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

mk

C. Reporting an Incident

Information security incidents involving university-owned devices or personal devices containing sensitive University data can have serious consequences. Responding to potential incidents promptly and efficiently helps protect the university's assets (e.g., data, computers, networks) and ensures compliance with state and federal law, and university policy.

Users of UMass Dartmouth IT systems must report any information security incident including unauthorized access to University data, any identified vulnerability in information assets, or any phishing attempts immediately through any one of the following channels:

- **E-mail:** it.security@umassd.edu
- **Phone:** 508-999-8900
- **In-person:** CITS Service Center, Claire T. Carney Library, 4th floor during business hours (see CITS website)
- **Online form:** http://ithelp.umassd.edu

Addition information to support University incident response is outlined in the following policies:

- Respond to Data Security Incidents – Information for Faculty & Staff
- Respond to Data Security Incidents – Information for IT Administrators
- Respond to Data Security Incidents Caused by Malware – Checklist for IT Administrators

III. To Whom This Policy Applies

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or other utilize any computing, data, and information technology resources that house University Information. This includes but is not limited to University clients, guests, and third parties as defined below.

- **University Information:** University Information is any information maintained by or on behalf of the University that is used in the conduct of University business regardless of the manner in which such information is maintained or transmitted. University Information formats include, but are not limited to oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or any other medium.

- **University Client ("Client"):**
  - any faculty, student, staff or alumni affiliated with the University, or
  - any department or College of the University, or
  - any employee (permanent, temporary and contract personnel)

- **Third Party:** Any entity having a relationship with the University not described as a client (e.g., business partner, research subject, vendor), or any external entity initiating contact with the University (e.g., RIAA, target of DDoS attack, student applicant, member of the general public).

IV. Responsible Parties

Every person at UMass Dartmouth can take steps to help protect university-owned computers and sensitive data and mitigate potential data security incidents through reporting of incidents to the University. It will be the University's IT department (e.g., service center staff, enterprise systems staff) who will be responsible to initially evaluate and escalate issues for further research. The Information Security officer will lead the incident response team to handle the incident investigation along with a delegated incident coordinator.

The team may include members from the following areas:

- CITS
- Finance
- General Counsel
- Communications
- Compliance/Risk
- University Department Heads, Vice Chancellors, Deans, or supervisors of functional offices
- Third Parties
- Representatives from the President's Office
- University Procurement Services
- The affected department that uses the involved system or output or whose data may have been breached or exposed

V. Approval

Approved: ______________________ Date: 7/14/20
David Gingerella, VCAF

Approved: ______________________ Date: 7/14/20
Dr. Mohammad Karim, Provost / COO

Approved: ______________________ Date: 7-29-2020
Dr. Robert E. Johnson, Chancellor