IT Security Incident Management Policy (ISP-14)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all staff and contractors administering information systems that process University data within the IT Department or other departments.

Table of Contents

Introduction

In todays interconnected world it is no longer realistic to rely on a protection only strategy all IT security programs must now ensure entities are able to handle data and system compromise as a result of a range of threat actors and methods ranging from viruses, malware, ransomware, targeted attack, and insider threat be it malicious or miss configuration. As such modern IT security management plans cover the Protect, Detect, Respond, and Recover continuum of operations.

Objective

The Objective of this policy is to define roles and responsibilities, plus the process the University IT department must have in place to implement Detection and Response operations to rapidly contain and recover from IT security events and incidents, thereby reducing the impact on University finances and operations as well as those individuals that may be impacted by loss or compromise of personally identifiable information.

Definitions

A Cyber or IT Security Incident is defined by the Department of Homeland Security (DHS) as an occurrence that:

A) Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits;
or
B) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

An incident could be either intentional or accidental in nature.

Policy Statement

General

1. IT security incident response is a university wide activity requiring active planning, exercising and participation of a wide range of departments including but not limited to University Executive Leadership, Student Affairs, Finance, Employee Relations/HR, Legal, Marketing, Student Admissions, Facilities, Police and Communications.

2. To ensure effective, efficient, and timely handling of IT Security Incidents the following documents and plans are to be in place in addition to this governing policy document:

3. IT Security Incident Response Plan – provides an overview of how to handle Incidents.
4. Incident Response and Handling Check List
5. Incident Play Books for likelihood of occurrences:
6. Malware on small number of devices
7. Ransomware – “Hack and Lock”
8. Ransomware – “Hack and Leak”
9. Internal and external communications plans covering minor, major and extensive IT Security Incidents
10. External Reporting Guide that defines the Federal, State, and educational bodies, plus individual

notifications that are legally required during and after an incident has been identified.

11. These documents, plans, and policies are to be tested at least annually through a tabletop simulation exercise. The results of which are to be captured as lessons identified and fed back to update the plans.

12. In addition to the response and handling playbooks and plans, the IT team is to define and maintain an incident response go bag of tools and devices stored off network for use during any incident response activity.

13. If cyber insurance is not in place a cyber investigation company or entity is to be maintained on a retainer, this reduces the time to engage such an entity during an incident.

Process

The IT Security Incident Response Plan is to follow the NIST recommended model and include the following phases or stages:

- **Preparation:** Maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.
- **Identification:** Confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.
- **Containment:** Minimizing loss, theft of information, or service disruption.
- **Eradication:** Eliminating the threat.
- **Recovery:** Restoring computing services quickly and securely; and
- **Lessons Learned:** Assessing response to better handle future incidents through utilization of reports, "Lessons Learned," and after-action activities, or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

Organizational Structure

When an incident is identified, the Computer Incident Response Team (CIRT) will be formed and if the incident is characterized as serious enough, they will request the establishment of the Cyber Incident Management Group (CIMG).

1. Membership of the **CIRT** will include the following:
   - CIO, CISO, or Qualified Individual (QI)
   - Others as necessary to pursue investigation and execution of the plan

2. Membership of the **CIMG** will be as follows:
   - University President
   - Legal Counsel
   - CIO, CISO or QI
   - Executive VP of Administration and Finance
   - VP of Student Development
   - Director of Communications and Marketing
   - Provost and VP of Academic Affairs
   - Data stewards
   - Privacy Officer
   - Captain of Campus Police
   - IT Director

Communications

Communication is an essential part of cyber incident response. Because communications regarding a cyber-incident often need to occur quickly, it is vital to build relationships, have templated communication materials and understand the process for review and release of communication materials.

Once an incident is confirmed, the CIO or CISO and the CIRT Cyber Incident Management Group will coordinate information sharing so that only the appropriate information is shared with the appropriate parties.

A communication plan is mandatory whenever a breach of Personally Identifiable Information (PII) has been confirmed.

A communication plan should identify internal and external communication needs, and how these needs will be addressed. Smaller events may only require internal communications, while larger events may require interaction with external stakeholders. The approach to communications should be tailored depending on the stakeholders.

Legal Considerations and Confidentiality of Information

All incident response activities are to be under the supervision of Legal Counsel to ensure client confidentiality is maintained and that all actions are in accordance with forced laws. Information is to be shared on a need-to-know basis to prevent inadvertently notifying an adversary and to maintain the status quo until such time plans are in place to communicate in an orderly manner.

Roles and Responsibilities

Members of the incident response organization are responsible for representing their business areas when assessing, planning, and taking actions to remediate the issues. Specific responsibilities are listed below:

- Legal Counsel – providing current and timely legal guidance as well as contracting for and directing external forensic and technical response activities. Maintaining the incident and data breach notification guides and performing the same.
- Director of Marketing and Communications – maintain communication plans, procedures, and template materials (approved by legal) for common event types.
- VP of Administration and Finance – maintaining access to crypto currency accounts should the need arise to make payment.
- CIO, CISO or QI – Accountable for oversight of the end-to-end IT security response process and advising on areas of weakness or improvement.
- Data Trustees – maintaining and accurate inventory of data, by criticality and classification.