Data Incident Response Policy
TEC 4.1
Office of Information Technology

Institutional Type: Administrative
Applies to: Faculty, staff, student employees, students, and volunteers

POLICY DATES

Issued: 2/8/2011
Revised Last: 10/12/2016
Edited by: Tina Stuchell
Reviewed: March 2019

This policy establishes the requirements for reporting and responding to information security incidents.

Table of Contents

Definitions

Term	Definition
Incident	An attempted or successful unauthorized access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable use policy. Examples of incidents include (but are not limited to): • Unauthorized access of systems or data • Inappropriate usage of systems or data • Unauthorized change to computer or software • Loss or theft of equipment used to store personal information or confidential University data • Unwanted disruption or denial of service • Interference with the intended use of university resources • Compromised user account
Serious Incident	An incident that may pose a threat to university resources, stakeholders, and/or services. Specifically, an incident is designated as serious if it meets one or more of the following criteria: • Unauthorized disclosure • Modification or destruction of personal information • Involves legal issues • Disruption of critical services • Involves active threats • Involves public interest
Personal Information	Is defined as a person's first name, first initial and last name in combination with any one or more of the following data elements: • Social security number • Driver license number or non-operating identification license • Financial account number or credit/debit card number in combination with any required security code.

Policy Details

This policy formalizes the requirements for reporting and responding to information security incidents. It serves to minimize the negative consequences of incidents and to improve the University's ability to promptly restore operations

affected by such incidents. It ensures incidents are promptly reported to the appropriate officials, that they are consistently and adequately responded to, and that serious incidents are properly monitored.

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.

When possible, the Office of Information IT Technical Services staff will abide by this standard and the Incident Response Plan to mitigate the threat. In an urgent situation requiring immediate action and leaving no time for collaboration, the Executive Director of IT & CIO, VP of Business Affairs or Director of IT for Security or designated staff is authorized under this Policy to disconnect any affected device from the network, and to assess vulnerabilities and verify safeguards of university resources.

Roles and Responsibilities

University-related persons have the following primary roles and responsibilities in connection with incidents:

Users of University Resources

- Promptly report actual or suspected incidents to the Office of Information Technology.
- If the Office of Information Technology is unavailable or unable to correct an incident, disconnect any affected device's network connection (the Ethernet cable, disable wireless, but not the power supply) and report the incident to the Director of IT for Security, Executive Director of IT & CIO or VP Business Affairs. In addition, if the *incident* involves –
    - Suspected unauthorized access, theft of university computing equipment or information, or another possible crime. Also report the incident to the University of Mount Union Campus Security Department and to local authorities if it occurred away from the main campus.
    - Personal identifiable information
    - Payment cardholder data.
- If a serious incident occurs, report it to Director of IT for Security, Executive Director of IT & CIO or VP of Business Affairs.
- Assist various parties to resolve the incident and help improve practices and prevent or minimize the occurrence of such incidents in the future.
- In the course of reporting, tracking, and responding to an incident, protect and keep confidential any confidential university data or personal information.
- Document any information you know while waiting for appropriate personnel. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

IT Security/Technical Services Personnel/ UMU Security Personnel

Evaluate and respond to incidents on a timely basis to prevent additional loss of or harm to university resources, in accordance with University policies.

- Assist various parties to resolve the incident and help improve practices and prevent or minimize the occurrence of such incidents in the future.
- Following initial reporting and upon performing remedial actions for any serious
- Incident notify Network Services of IT, Director of IT for Security, Executive Director & CIO or VP of Business Affairs for accurate closure of the problem report.
- Notify the affected user of remedial steps taken and recommended mitigating activities.

Applies to: Faculty, staff, student employees, students, and volunteers

- In the course of reporting, tracking, and responding to an *incident*, protect and keep confidential any confidential university information or personal information.
- Quarterly scan for unauthorized wireless devices and report any found to the Network Services department for immediate deactivation
- Maintain a problem report or other documentation of the incident.
- Communicate to the appropriate parties any actions that need to be taken by them, the reasons for them, the steps required to re-establish service and any relevant technical information about the incident.
- Initiate escalation procedures to the appropriate office or party as necessary.
- In the course of reporting, tracking, and responding to an incident, protect and keep confidential any confidential university information or personal information.

Executive Director of IT, Director of IT for Security and VP of Business Affairs

- Coordinate investigation of serious incidents and Initiate escalation procedures to the appropriate office, BOT or party as necessary
- Conduct all investigations in accordance with Federal and Ohio statues.
- All communications with law enforcement or the public will be coordinated by VP or Business Affairs or VP of Marketing.

Incident Response Steps (Plan)

Phase 1: Detect/Analysis

- Determine whether incident has occurred
  - Document any indicators (sign that an incident has occurred)
  - Look for correlating information (logs, etc.)
  - Perform research (knowledge base/search engines)
  - If evidence exist of an incident has occurred, inform Office of Information Technology and begin Phase II

Phase 2: Categorize incident

- **Identify the type of incident that occurred**
  A. Phishing/compromised credentials
  B. Malware
  C. Lost/Stolen Device/Lost or Stolen Data
  D. Compromised Device Chain of Custody
  E. Other

Phase 3: Category-Specific Containment/Eradication/Recovery/Documentation

A. Phishing/Compromised Credentials

- **Client/End User**
  - Inventory sites using those credentials
  - Change passwords for all sites
  - If any financial credentials were compromised
    - Notify credit agencies and place fraud alert on account
    - Contact Credit Card companies
    - Contact Bank(s)
    - Monitor accounts for suspicious activity
  - Check for malware on computer (see Phase 3B)
- Institution
  - Review access logs of any campus related servers
    - If accessed, determine what data has been compromised
    - Notify appropriate stakeholders affected by data breach working with VP or Marketing and VP of Business Affairs

B. Malware

- Use malware removal tools
- Document and research type of malware, and how it affects device
- Remove system restore points that may be infected
- Ensure all system/security updates are downloaded and installed

Applies to: Faculty, staff, student employees, students, and volunteers

- Ensure device has current active malware protection installed

C. Lost Device

- Determine ownership of device:
  - If University
    - University will notify police if device was stolen
  - If Client
    - Client should notify police if device was stolen
    - If device has cell-service, should contact provider to disconnect account (after tracking/wiping has been attempted)
- Is the device trackable?
  - If so, try to determine location of device for recovery of device
- Can the device be remotely wiped?
- Can the device be remotely locked?
  - If so, lock the device until it is recovered.
- Continue to Phase 3D for compromised device chain of custody

D. Compromised Device Chain of Custody

- Document length of time the device was out of chain of custody
- Was device password protected?
  - If no, assume data on device is potentially compromised
  - If yes, proceed to next step
- Was device encrypted?
  - If no, assume data on device is potentially compromised
  - If yes, proceed to next step
- Has the device been recovered?
- Prevent personal info access
  - Reconstruct a list of apps used on the device
  - Change appropriate passwords
- Inventory potential data breaches and notify stakeholders

E. Other

- Gather detailed information and decide best remediation approach

- For all categories, complete Phase 4

Phase 4: General Containment, Eradication, Recovery, Documentation

Focus on the containment, eradication and recovery of the incident. Provide documentation along the way. Keep Data Incident Log files updated.

Contact Information

- Lead IT Handler
- Affected Client
  - Name
  - Role
  - Department
  - Email Address
  - Phone Number
  - Office Location

Incident Details

- Date/Time
  - When did the incident start:
  - When the incident was discovered/detected:
  - When the incident was reported:
  - When the incident was resolved/ended:
- Physical location of the incident:
- Current status of the incident

Applies to: Faculty, staff, student employees, students, and volunteers

- Source/cause of the incident, including hostnames and IP addresses
- Description of the incident (e.g. how it was detected, what occurred):
- Description of affected resources (e.g., networks, hosts, applications, data), including systems' hostnames, IP addresses, and function:
- Prioritization factors (functional impact, information impact, recoverability, etc.):
- Mitigating factors (e.g. stolen laptop, etc.)
- Responses actions performed (e.g., shut off host, disconnected from network, etc.)
- Other organizations contracted (e.g. software vendor, credit agencies, etc.)
- Include any additional relevant information

Phase 5: Reporting

Prepare a written report to submit to Executive Director of IT, VPAA , President Council and BOT if necessary

- Current status of the incident response
- Summary of the incident
  - Incident Handling Actions
  - Lot of actions taken by all handlers
  - Contact information for all involved parties
- List of evidence gathered
- Incident Handler Comments
- Cause of the incident
- Cost of the incident
- Business impact of the incident

Responsibilities

Position or Office	Responsibilities
Office of Information Technology (Technical Services, Director of IT) Business Office Associate VP or VP)	Update of policy and response to incident

Resources

Contacts

Subject	Office	Telephone	E-mail/URL
	Office of Information Technology	330-823-2854	IT@mountunion.edu
	Business Office	330- 823-6566	businessoffice@mountunion.edu

History

This policy was established in 2011 part of PCI rules and regulations.
All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.
Issued: 2/8/2011

Revised: 10/12/2016

Edited by: Tina Stuchell

Reviewed: March 2019