Information Security Incident Response Procedure

1. Overview
Information security incidents are occurring more frequently than ever. The University of Akron must take appropriate steps in the event of an information security incident to minimize the impact and scope of the incident.

2. Purpose
This procedure outlines the escalation process for information security incidents related to UA information. The UA Information Security Services team must be notified immediately of any information security incidents.

3. Scope
This procedure applies to any system, service, device, process, or media that is used to access, store, or transmit institutional data in electronic, audible, or physical formats. This procedure applies to personally owned systems, devices, and media; University owned systems, services, devices, and media; and third-party service providers.

4. Definitions

- **Information Security Incident** – Any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information including, but not limited to, interference with information technology operation and violation of University Rules, ITS policies and standards, and applicable laws and regulations.
  - Examples of Information Security Incidents include, but are not limited to:
    - Computer system breaches
    - Theft or loss of systems, devices, or media
    - Unauthorized access to, or use of, systems, software, or data
    - Unauthorized changes to systems, software, or data
    - Website defacement
    - Denial of service attacks
    - Impersonation of systems or people
    - Interference with the intended use of IT resources
    - Compromised user accounts

- **Incident Response Team** – The individuals responsible for investigating data breaches and other information security incidents. These individuals may include, but are not limited to UA Information Security Services, UA Office of General Counsel, and local, state, and federal law enforcement agencies.

- **Incident Handler** – The Information Security Services staff member assigned by the Incident Response Team to lead the incident response effort.
• **Institutional Data** – Any information or data that is gathered, analyzed, or published by any department of the University of Akron in support of its mission(s).

• **Protected Institutional Data** – Any information classified as more restricted than Public Use by the Data Owner, or appointed Data Steward(s), according to ITS Data Classification Standards.

5. **Reporting**

5.1 It is important that actual or suspected information security incidents are reported as early as possible to limit the damage and cost of recovery.

5.2 To report an actual or suspected information security incident, contact:
   a) Email: security@uakron.edu
   b) Phone: (330) 972-6888
   c) Important: If the incident poses an immediate danger, contact UAPD at (330) 972-2911

5.3 Information to include in the report:
   a) Your contact information including name, department, email address if calling in, and telephone number
   b) A description of the information security problem
   c) The date and time the problem was first noticed (if possible)
   d) Any other known resources affected

5.4 Do not, under any circumstances, attempt to investigate the incident on your own.

5.5 Preserve any evidence you can and disturb as little as possible.

6. **Response**

6.1 The Incident Response Team will immediately identify an Incident Handler for the suspected information security incident.

6.2 The incident response effort is comprised of six prioritized activities: Containment, Data Collection/Recovery, Analysis, Notification, Reporting, and Data Retention.

6.3 Containment

   6.3.1 Whenever possible, the incident handler will perform a network quarantine at the time of a reported/suspected incident and/or instruct the system administrator to unplug the network cable of the suspected machine.

   6.3.2 The incident handler will quarantine potentially compromised host(s) at the time of containment and promptly reach out to the system administrator or system owner to create a plan to contain the incident. Note that the incident handler may quarantine/notify additional hosts based on suspicious behavior pending verification. In cases where the impact of system downtime is very high, the incident handler will work with system administrators to determine the level of account privilege and eliminate their access safely.

   6.3.3 All user privileges will be suspended immediately after the originating UID is determined until such a time that future risks are non-existent.

   6.3.4 Once a threat is verified, the incident handler will notify CIO and continue to priority 2 and proceed sequentially through all remaining priorities.
6.3.5 Once a threat is ruled non-existent, the incident handler will reinstate user privileges and continue to priority 5 and proceed sequentially through all remaining priorities.

6.4 Data Collection/Recovery

6.4.1 The incident handler will collect data from UA system administrators or third-party service providers to quickly assess the scope of the incident, including:

- Preliminary list of compromised systems and/or services
- Preliminary list of storage media that may contain evidence and/or compromised data
- Preliminary incident timeline based on initially available evidence
- Examination of logs should begin
- Modes of data recovery, if needed, should begin being examined after the scope of the incident is realized with the goal being a return to departmental productivity with minimal data loss
- Data recovery should begin once the threat is quarantined and deemed to be non-threatening

6.5 Analysis

6.5.1 The incident handler will establish whether there is reasonable belief that an attacker(s) successfully accessed Protected Institutional Data.

6.5.2 The incident handler will generate an incident timeline and ascertain the impacts and/or actions of all parties to identify the details of the compromise. When possible, a full back-up or system image may be necessary for analysis.

6.5.3 The incident handler will coordinate the communication between stakeholders including data owners, data stewards, data custodians, and any relevant compliance officers.

6.6 Notification

6.6.1 The incident handler will notify the Incident Response Team, CISO, CIO, data owners, and when appropriate, the incident reporter, with the following information:

6.6.1.1 Complete list of compromised systems and/or services and associated UIDs

6.6.1.2 Complete list of storage media that may contain evidence and/or compromised data

6.6.1.3 Incident timeline based on initially available evidence

6.6.1.4 All results of the analysis

6.6.1.5 In cases where malice is suspected and/or Protected Institutional Data has been disclosed, and by directive of the CIO, the UAPD and Office of General Counsel will be notified.

6.7 Reporting

6.7.1 The incident handler will draft the final incident report after the analysis and notification priorities are complete and submit it to Information Security for discussion. Preliminary reports should be avoided whenever possible since working conclusions can change substantially through the course of an investigation.
6.7.2 Technical personnel participating in the containment, data collection/recovery, or analysis can offer incident reports for their participation to be included within the final incident report, but typically technical issues should be resolved by this stage.

6.7.3 For critical incidents involving payment card data, the PCI Compliance Manager will receive a copy of the report and appropriate entities will be notified in the event that cardholder data is accessed without authorization. The PCI Compliance Manager will be responsible for all communication with the payment card brands and will be responsible for coordinating the activities mandated by the payment card brands with respect to the incident.

6.7.4 For critical incidents involving HIPAA related data, the Privacy Officer will receive a copy of the report. The Privacy Officer will follow the HIPAA Breach Notification Rule requirements for notifying appropriate parties of the incident.

6.7.5 For critical incidents involving FERPA and/or other Protected Institutional Data, the report will include examples of each impermissible use. If appropriate, given the analysis, the CIO will obtain sign-off from the Office of General Counsel on the report.

6.7.6 Information Security Services will schedule a meeting to deliver the final report to the system administrator, the system owner, as well as to responsible officials.

6.7.7 Information Security Services will ensure that the final report includes the details of the investigation and mid-term and long-term recommendations to improve the security posture of the organization and limit the risk of a similar incident occurring in the future.

6.7.8 It is the data and/or application owner’s responsibility for breach notification when no established regulatory notification requirements exist.

6.8 Data Retention

6.8.1 Information Security will archive the final report in case it is needed for reference in the future; reports must be retained for twelve (12) months.

6.8.2 Incident notes should be retained by the incident handler for twelve (12) months from the date that the report is issued.

6.8.3 Raw incident data should be retained by the incident handler for thirty (30) days from the date that the report is issued. This includes disk-images, unfiltered netflow-content, raw file-timelines, and other data that was collected but deemed not relevant to the investigation.

7. Related Documents

University Rule 3359-11-08: Policies and Procedures for Student Records

University Rule 3359-11-10: Acceptable Use Policy

University Rule 3359-11-10.3: Information Security and System Integrity Policy

University Rule 3359-11-10.4: Customer Information Security Policy

University Rule 3359-11-10.6: Social Security Number Use Policy
University Rule 3359-11-10.8: Identity Theft Detection, Prevention, and Mitigation Policy


ITS: Data Classification Standards

ITS: Secure Access and Data Storage Standards