Security Incident Response Procedure

The University of Akron is strongly committed to maintaining the privacy and security of the personally identifiable information of its students, employees and customers and has several University Rules related to privacy and data security, including:

3359-11-08: Policies and procedures for student records
3359-11-10.3: Information technology security and system integrity policy
3359-11-10.4: Customer information security policy
3359-11-10.6: Social security number use policy
3359-11-10.7: Privacy policy
3359-11-10.8: Identity theft detection, prevention and mitigation policy
3359-11-19: Policies and procedures for release, privacy and security of selected health information

Objective:
The objective of this procedure is to outline the escalation process for security incidents that effect a University of Akron (UA) owned PC or device. Anytime a security incident has been identified or is suspected, the UA Security team should be notified based on the contact list provided below.

Definition of a security incident:
End-user/System Administrator reports an unauthorized activity that results in the disruption of a University-owned system(s), such as the following:

- Unauthorized access/change to UA information or data
- Active malicious software that effects multiple PCs, (e.g. a worm that is spreading malicious code to other UA systems: existence of a Key logger on one or more UA PCs, etc.)
- Denial of Service attack
- Possible compromise of sensitive information including credit card numbers, social security numbers, or other personally identifiable information (PII)
- Website defacement
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- The unauthorized use of a system for the processing or storage of data
- IP Spoofing
- Commercial use of UA IT resources
- Social engineering activity — Unknown people asking for information which could gain them access to UA’s data (e.g. a password or other details)
- Unauthorized disclosure of sensitive or confidential information electronically, in paper form or, verbally
- Connecting unauthorized third party equipment to the organization’s network
- Giving sensitive or confidential information to someone who should not have access to it — verbally, in writing, or electronically
Security Incident Response Procedure

Contact List:
Please use the numbers provided on the following list until you get in touch with an individual “live in person” based on the following order:

1. John Corby – x7345 or (330) 283-1861
2. Kurt Eckert – x5235 or (330) 760-1023
3. Neal L’Amoreaux – x7535 or (330) 417-0468
4. Chris Muller – x6070
5. Keith Piepho – x6130
6. Jason Bowling – x6646

In reference to the following priorities, the “incident handler” is defined as the UA ITS staff member responsible for the fulfillment of the remediation priorities outlined below and may not be the individual first notified of the potential incident.

Remediation priorities:

1. Containment:
   - 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.
   - 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.
   - All user privileges will be suspended immediately after the originating UID is determined until such a time that future risks are non-existent.
   - Once a threat is verified, the incident handler will notify CIO and continue to priority 2 and proceed sequentially through all remaining priorities.
   - 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.

2. Data Collection/Recovery:
   - The incident handler will collect data from system administrators in order to quickly assess the scope of the incident, including:
     - Preliminary list of compromised systems
     - Preliminary list of storage media that may contain evidence and/or compromised data
     - Preliminary attack 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

3. Analysis:
   - The primary goal of analysis is to establish whether there is reasonable belief that the attacker(s) successfully accessed restricted/sensitive data on the compromised system or any network resources.
Secondary analysis goals are to generate an attack timeline and ascertain the attackers’ actions with the end goal of identifying details of the compromise (trojan vs modes of account compromise vs malware, etc.) An image of the compromised machine may be necessary for the analysis as determined by the incident handler.

All analysis steps are primarily driven by the incident handler, who coordinates communications between other stakeholders, including system owners, system administrators, database administrators, and relevant compliance officers.

4. **Notification:**

- The incident handler will notify the CIO, system administrators, Information Security in writing the following:
  - Complete list of compromised systems and associated UIDs
  - Complete list of storage media that may contain evidence and/or compromised data
  - Attack timeline based on initially available evidence
  - All results of the analysis
  - In cases where malice is suspected and/or sensitive data has been leaked, and by directive of the CIO, the UAPD and General Counsel is to be notified for their action.

5. **Reporting:**

- 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.
- 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.
- 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.
- For critical incidents involving FERPA and/or other sensitive 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.
- Information Security will schedule a meeting to deliver the final report to the system administrator, the system owner, as well as to responsible officials.
- Information Security 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. **Data Retention:**

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