Incident Response Plan for Self-managed Asset

Definition of an Incident

A security incident can be defined as any potential unauthorized access or exposure to sensitive or confidential information. Exposure means that the information was in a state where it is possible that unauthorized access may have occurred. An exposure is sufficient cause to report an incident.

Confidential information can include:

1. Research data
2. Student educational records including academic performance data, disciplinary records, race, or ethnicity, gender, nationality or grades.
3. Controlled Unclassified Information (CUI)
4. Any involvement with a Technology Control Plan (TCP) computer system
5. Social Security Numbers
6. Banking or Financial account numbers with passwords or PIN numbers
7. Driver’s license number or state identification card number
8. HIPAA data

For complete guidance on institutional data, you may reference the Institutional Data Policy.

Widely used attack vectors for incidents include but are not limited to:

1. Loss or Theft of Equipment – stolen computer, tablet, phone, or external media.
2. Unpatched and out-of-date or end of life software and operating system vulnerabilities.
3. External/Removable Media – an attack executed from removable media such as an infected flash drive.
4. Brute Force – brute force methods used to degrade or bring down networks and/or computer systems.
5. Web – web site based or web-based application, exploitable vulnerability
6. Email – a phishing message or potential malicious attachment.
7. Improper Usage – an incident that violates OSU's acceptable usage policy.
8. Non-compliance with established security protocols

Anytime confidential information is exposed to a potential attack, it must be reported. If a person loses equipment, or "clicks" in a phishing message, or suspects someone unauthorized person might have accessed confidential information, it must be reported.

Reporting an Incident

If you feel a security incident may have occurred, please use the outlined information below to properly report the incident. ETS security should be notified as soon as possible, and at least within 16 business hours, of the occurrence of a suspected incident.

1. Report the incident by email to all of the following:
   - Andy Greicius – Director, Security  greicius.1@osu.edu
   - Dan Watkins – Security Engineer  watkins.222@osu.edu
   - Corey Steele – Research Security  Steele.586@osu.edu
   - Vincent Juodvalkis - Security Ad Hoc  juodvalkis.1@osu.edu
   - ETS Help  etshelp@osu.edu

   Alternatively, the incident can be reported to – etshelp@osu.edu

2. If no acknowledgement is received after 4 hours from the initial contact, please call the ETS security team lead:
   - Andy Greicius – Director, Security
   - Cell phone – (614)-407-9360
   - Email – greicius.1@osu.edu

3. If no acknowledgement is received after 8 hours from the director, then contact OCIO Security directly:
   - OCIO Security
   - Phone – (614)-688-5650
   - Email – security@osu.edu
The above individuals from COE or OCIO Security will additionally report the incident to:

- All suspected incidents will be reported to OCIO Security – security@osu.edu
- Suspected incident involving research related data will be reported to the Office of Compliance and Integrity and/or Office of Secure Research
- Suspected incidents involving Payment Card Industry (PCI) data will be reported to the Office of Treasury

**Preservation of Evidence**

It is very important that evidence is preserved to allow for proper investigation and data discrimination. When reporting an incident please;

1. Preserve all data and refrain from running any type of malware/anti-virus tools on the suspected machine.
2. As soon as possible, isolate the computer from the network by either unplugging the network cable or having the ETS network team disable the relevant switch port.
3. If the machine cannot be disconnected from the network, please power off the suspected machine by disconnecting the power.

All evidence and steps taken to preserve evidence should be properly documented and a chain of custody procedure should be followed.