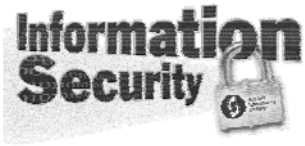


Computer Incident Handling Procedure

I Purpose

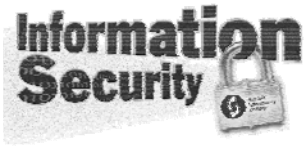
This procedure provides an incident handling process for use when the SCC network, servers, desktops, or other computing devices are compromised. Being prepared for an incident and following the process detailed below will enable support personnel to handle incidents consistently and appropriately.

II Scope

The primary audience for this procedure is the staff members likely to be incident 'first responders'. Generally these will be ITS staff, Laboratory Coordinators, or other staff with systems/technical support responsibilities for SCC-owned or managed computing devices.

This procedure applies to all SCC-owned or managed computing devices and the SCC network in general.

Ordinarily, the procedure does not apply to personally-owned computers or devices. However, incident handling processes may extend to personally-owned computers or devices when they are found to be part of an incident involving SCC resources. Owners of these devices are required to cooperate with systems support personnel to limit damage to SCC resources.



III Definitions

Incident—Incidents include but are not limited to:

- Theft/Denial of Service – theft, loss, or loss of access to systems, network, storage, or other information assets.
- Malicious code/software - Software or code intentionally created or introduced into a system with a purpose or payload of causing harm or loss to the system, its data, or other information assets. Example include, but are not limited to, viruses, worms, keystroke loggers, rootkits, logic bombs, spam relays, remote control bots, spyware, adware, and 'potentially unwanted programs.' Discovery of non-persistent malicious code/software that is blocked/remediated by the College's automated security policy enforcement tools with no adverse consequences to the system is considered a non-significant incident.
- Unacceptable use – any action that violates the College Acceptable Use policy, other College policy, or violations of civil/criminal law.
- Unauthorized access - gaining access into any user account, system, network, storage, or other information asset without the express permission of the owner of the asset. This includes authorized users who intentionally elevate their permissions.
- Other – Any incident not meeting above criteria, such as critical or widespread vulnerabilities or mis-configuration that might lead to compromise.

High Risk – An incident is high risk if it involves one or more of the following:

- Criminal activity.
- Unauthorized external access to personal identifying information
- Lost or compromised device containing, or possibly containing, confidential, sensitive, critical data
- Potential unauthorized access due to discovery of a keystroke logger, rootkit, remote access agent, password cracking agent, or similar exploit
- Disrupts continuity of critical business processes or communication.

Low Risk – Any incident not meeting the criteria for a high risk incident.

Personal Identifying Information - A person's first name (or initial) and surname, in combination with any of the following:

- Social Security Number.
- Driver's license number or state identification card number.
- Financial account, debit, or credit number.
- Other information that creates a material risk of the commission of the offense of identity fraud or other fraud to the individual.

IV Basic Incident Handling Process

A Preliminary Activities

1 Incident first responders must be trained in the use of and have access to evaluation, diagnostic, and remediation tools appropriate to the devices and operating system(s) they support.

B Detection, Initial Reporting.

1 In the event of the loss of an SCC-owned or leased computing device, the loss shall be reported to the Campus Police, the Information Security Officer, and the Director of Information Technology Services in a timely manner.

2 If any loss or compromise of sensitive or critical information is suspected, the incident first responder must evaluate and document the incident risk and actions taken.

a If criminal activity is suspected, Campus Police must be notified.

b If a compromise is high risk, then it must be reported, as soon as reasonably possible, but no later than eight hours, to the Information Security Officer and/or the Director of ITS. They will determine the need and notify the appropriate secondary incident responders as appropriate.

c If the compromise is low risk, the responder may contain, eradicate, and recover the system. The responder must document the nature of the problem and resolution, and submit a copy to the Information Security Officer.

C Containment

1 If criminal activity is suspected, the isolation and containment process must forensically preserve evidence.

2 If a compromise is high risk, the incident first responder will take action to isolate and contain the affected device until such time as the threat is mitigated.

D Eradication

1 If the compromise is high risk, before beginning eradication procedures, the first responder should forensically create and retain an image of the compromised/infected system when possible (to aid in future analysis).

2 If the compromise is high risk, and there are multiple incidents of the same type of compromise, the first responder should coordinate activities with the Director ITS and Information Security Officer. The first responder should still forensically create and retain an image of a representative compromised system when possible.

3 The responder will use the appropriate methods, in increasing order of system impact, to eradicate the compromise/infection.

4 If eradication is unsuccessful or the compromise/infection reoccurs with 48 hours, the first responder shall notify the Director of ITS

to obtain second level support and await further instructions.

E Recovery

1 If eradication is successful, the first responder should clean and restore the data and availability of the affected system in order to return the system to normal operations.

2 If the system is a server, the systems administrator must reformat and re-image (or rebuild), unless the incident was low risk and the eradication was accomplished through the use of standard anti-virus tools.

F Post-Incident Activities

1 The documentation describing the problem and resolution of all incidents will be submitted to and reviewed by the Information Security Officer for tracking, trending, and reporting. Additionally:

a Incidents involving new vectors or difficult to resolve exploits will be reviewed by the first responder(s) and Information Security Officer for ‘lessons learned’ and effective practice development.

b High-risk incidents will be reviewed by the Information Security Officer, Director of ITS, first and secondary responders, and other involved personnel as appropriate, for ‘lessons learned’ and effective practice development.

c Incidents involving a breach of personal information will be thoroughly analyzed to determine extent of the loss and the specific individuals affected. The Information Security Officer will notify the appropriate personnel to initiate the individual disclosure/notification process IAW with Chapters 1345, 1347, and 1349 of the Ohio Revised Code.