Security Standard: Computer Incident Handling Process
Effective 11/15/05 (rev. 1/18/10)

1.0 Purpose
This standard provides an incident handling process for use when the RIT 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.

2.0 Scope
This standard applies to all Institute-owned or leased computing devices and the RIT network in general.

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

The incident handling processes are content neutral, and may extend to scholarly research or teaching of information security when these programs or actions are found to be part of an incident involving RIT resources.

3.0 Audience
The primary audience for this standard is systems and end user administrators of RIT-owned or leased computing devices.

4.0 Definitions
Incident—Incidents include but are not limited to:
- Loss or theft of computing devices or portable media
- Detection or discovery of a program agent including, but not limited to viruses, worms, Trojan horse programs, keystroke loggers, rootkits, logic bombs, spam relays, remote control bots.
- Detection or discovery of unauthorized users, or users with privileges in excess of authorized privileges.
- Detection or discovery of critical or widespread vulnerabilities, or misconfiguration that might lead to a compromise affecting the confidentiality, integrity or availability of Institute information.

High Risk – An incident is high risk if it meets one of the following criteria:
- involves a keystroke logger, rootkit, remote access agent, password cracking agent, or a new threat from an unknown vector;
- Loss or compromise of Private or Confidential information
- Loss of operationally critical data

Low Risk – An incident is low risk if it does not meet the criteria of a high risk incident.

5.0 Minimum Standard
By November 15, 2005 and all times thereafter, each department must maintain and document an incident handling process with the following minimum components:

5.1 Preliminary Activities
5.1.1 Systems administrators must have diagnostic and cleaning tools appropriate to the operating system(s) they support.
5.2 Identification of risks, compromise, or threat agent
5.2.1 In the event of the loss of a RIT-owned or leased computing device or portable media, the loss shall be reported to Campus Safety, the respective Information Security Coordinator, and the Information Security Office in a timely manner.
5.2.2 If any compromise has occurred, the systems administrator must evaluate the risk with the Information Security Coordinator,
5.2.2.1 If the compromise is low risk, the systems administrator must send a problem description of the incident to the Information Security Office.
5.2.2.2 If a compromise is high risk, then it must be reported to the Information Security Coordinator for the area, the Information Trustee responsible for the information, and the Information Security Office, as soon as reasonably possible, but no later than six hours.

5.3 Containment of threat
5.3.1 If a compromise is high risk, the systems administrator may contain the affected device until such time as the device is remediated.

5.4 Eradication of compromise
5.4.1 If the compromise is high risk, before beginning eradication, the systems administrator should create and retain an image of the compromised/infected operating system when appropriate.
5.4.2 If the compromise is high risk, and there are multiple incidents of the same type of compromise, the systems administrator should contact the Information Security Office. The systems administrator must still provide a representative image of a compromised device where appropriate.
5.4.3 If eradication is unsuccessful or the compromise/infection reoccurs with two days, the systems administrator shall notify the Information Security Office and await further instructions.

5.5 Recovery
5.5.1 If eradication is successful, the systems administrator should clean and restore the data and availability of the affected system in order to return the system to normal operations.
5.5.2 If the system is a server, the systems administrator must create a backup image of the restored system unless the remediation was accomplished through the use of standard anti-virus tools.

5.6 Lessons Learned
5.6.1 If a high risk compromise resulted from a new vector or was difficult to eradicate, it is the responsibility of the systems administrators and Security Coordinators to work with the Information Security Office to collect lessons learned and extract best practices. The ISO will post best practices on the Information Security website and communicate their availability to coordinators and systems administrators.

A “Plain English Guide” providing explanation and illustration of this standard may be found at https://www.rit.edu/security/content/computer-incident-handling-standard. In all cases, it is the standard itself, and not the “Plain English Guide,” which is authoritative.

For detailed support of computer incidents, RIT has arranged for the SANS Step-By-Step Guide, Computer Security Incident Handling to be available to all systems administrators employed on campus. The guide is available on request from the Information Security Office.
6.0 Roles and Responsibilities
This section identifies roles and responsibilities for implementation and compliance.

- **Information Security Office**—issues security standards based on threats and the needs of the Institute for protection. The ISO champions implementation efforts, offers acceptable alternatives, and provides exceptions as appropriate. The Information Security Office provides communication and training materials as appropriate. The ISO is available for participation in Institute disciplinary processes.

- **Information Trustee (VP or Provost)**—comprehends the risks associated with the security standard and provides direction to appropriate students, faculty, and/or staff to ensure full compliance with the *Standard*. Must ensure their departments adopt this incident handling process or submit an alternative process to the Information Security Office.

- **Information Security Coordinator**—acts as an information security liaison to their colleges, divisions, or departments. Responsible for information security project management, communications, and training for their constituents.

- **Systems Administrator**—ensures that the incident handling processes detailed in Section 5.0 is followed. If an alternate plan is proposed, the SA must review the plan with the respective Information Trustee and the Information Security Office by the compliance date of the standard.

- **End Users with Administrative Rights**—end users with administrative rights on RIT-owned or leased computing devices whose failure to comply with relevant RIT Security Standards results in an incident are subject to the sanctions provided in RIT’s *Code of Conduct for Computer and Network Use*.

7.0 Non-Compliance and Exceptions
For Systems or Network Administrators—If any of the *Minimum Standards* contained within this document cannot be met on systems you support, an Exception Process must be initiated that includes reporting the non-compliance to the Information Security Office a plan for risk assessment and management. For more information, see [https://www.rit.edu/security/content/exception-process](https://www.rit.edu/security/content/exception-process).

Noncompliance with information security standards will result in disciplinary actions up to and including termination.

8.0 Related RIT Policies, Procedures, Standards, Best Practices and Applicable Laws (not all inclusive)

- RIT Information Security Policy (C8.1)  
  [https://www.rit.edu/academicaffairs/policiesmanual/sectionC/C81.html](https://www.rit.edu/academicaffairs/policiesmanual/sectionC/C81.html)

- RIT Code of Conduct for Computer and Network Use (C8.2)  
  [https://www.rit.edu/academicaffairs/policiesmanual/sectionC/C82.html](https://www.rit.edu/academicaffairs/policiesmanual/sectionC/C82.html)

- RIT Information Access and Protection Standard (2009)  
  [https://www.rit.edu/security/content/information-access-protection-standard](https://www.rit.edu/security/content/information-access-protection-standard)

- RIT Server Security Standard  
  [https://www.rit.edu/security/content/server-security-standard](https://www.rit.edu/security/content/server-security-standard)
- RIT Desktop and Portable Computer Security Standard
  https://www.rit.edu/security/content/desktop-and-portable-computer-security-standard

- RIT Portable Media Security Standard
  https://www.rit.edu/security/content/portable-media

- RIT’s Information Security Exception Process
  https://www.rit.edu/security/content/exception-process

Date Issued: August 16, 2005

Revised: January 18, 2010