Plain English Guide to the Computer Incident Handling Standard

This guide presents an overview of the requirements of the Computer Incident Handling Standard. The standard is needed to minimize the risks and losses that can result from a computer incident. The requirements were developed and reviewed by a team representing the RIT community. This Plain English Guide provides explanation and illustration of the Standard and is provided as an aid to help you understand and implement the requirements of the Standard. The Standard itself is authoritative. The standard is effective on November 15, 2005.

Why we issued this standard

The adoption of a computer incident handling standard enables us to prepare successfully for incidents and better resolve incidents quickly and effectively. Learning from our incident handling successes will enable us to strengthen the RIT network by improving preventive measures and incident handling skills.

Who do the requirements apply to?

The requirements apply to administrators of RIT-owned or leased computing devices (i.e., systems administrators and to a lesser extent, users that are self-supported).

Privately-owned computing devices may be included in the process if they are involved in a computer incident and pose significant risk to the Institute.

Although this is a Computer Incident Handling Standard it extends to a wide range of portable and other computing devices including but not limited to mobile phones, PDAs, Pocket PCs, thumb drives and other USB devices. Essentially, any device capable of storing data may potentially hold Private, Confidential, or Operationally Critical information and as such is covered by the Computer Incident Handling Standard.

What do I have to do?

Everyone

- All cases involving lost or stolen devices or portable media containing sensitive information must be immediately reported to Campus Safety. Otherwise, your course of action depends on your role in the administration of the device at risk.

Self-supported users

- If you are using a computer that contains Private, Confidential, or Operationally Critical information, immediately contact your support organization.
- If you are using a computer that does not contain Private, Confidential, or Operationally Critical information, attempt to use appropriate software tools to remove or disable any malicious software on your device. (Many of these tools are listed at [http://security.rit.edu/desktop.html](http://security.rit.edu/desktop.html) and [http://security.rit.edu/server.html](http://security.rit.edu/server.html).) If you are unable to successfully identify and recover from a compromise, you should contact your support organization or the Help Desk. If they discover high risk threats on your computer, such as keystroke logging programs or programs that disable security programs, they will engage the Computer Incident Handling process.
Users supported by Systems Administrators

- If your computer is supported by a systems administrator you should report any suspicious computer activity, such as your computer suddenly slowing down, the mouse moving on its own, etc. to your support organization (FAST, ITS, COB, etc.). Your support organization will determine the correct course of action based on the risk level of the incident.

Systems/server Administrators

- The Computer Incident Handling process is designed to protect Private, Confidential, and Operationally Critical information. Systems/server administrators must follow the Computer Incident Handling process outlined below and detailed in the standard at [http://security.rit.edu/articles/incidenthandling.pdf](http://security.rit.edu/articles/incidenthandling.pdf). You are also responsible for securing any help needed to follow the process. Communicating with the Information Security Office about the incident and its resolution is critical to keeping the incident confined to as few computing devices as possible.

Where do I go for more information?

Visit our website at [http://security.rit.edu](http://security.rit.edu) to read the standard, get links to security vendors that classify viruses, worms, phishing, rootkits, and other threats, and discover how to implement the standard. For more information, contact RIT Information Security at infosec@rit.edu.

Appendix: Computer Incident Handling Process Overview

The Computer Incident Handling process consists of six steps. The steps are based on the SANS Step-By-Step Guide, *Computer Security Incident Handling*. The guide is available to systems administrators on request from the Information Security Office at infosec@rit.edu.

The six steps are:

1. Preliminary activities
2. Identification of risks, compromise, or threat agent
3. Containment of threat
4. Eradication of compromise
5. Recovery
6. Lessons Learned

A flowchart of the Computer Incident Handling process may be found below.