Security Standard: Incident Handling

Scope

This standard applies to all RIT information resources.

Requirements

Any RIT person discovering an event or incident are required to follow the incident handling process below.

1. **Notification**
   - 1.1. Anyone who discovers an event should report it to the appropriate IT support personnel or the ITS Service Desk immediately and await further instructions before continuing to use the computing device or media.
     - 1.1.1. Anyone who becomes aware of the loss or theft of an RIT computing device or media should report the loss or theft to RIT Public Safety immediately.
   - 1.2. IT support personnel should follow the internally published procedures provided by the Information Security Office to determine if the event could be a security incident.
   - 1.3. If anyone suspects that an incident has occurred, they should:
     - 1.3.1. Notify the RIT Information Security Office upon discovery.
     - 1.3.2. In the event of the loss or theft of a computing device or media that contains RIT information, report the loss to Public Safety immediately.
     - 1.3.3. Work with the Information Security Office on containment and forensics imaging (memory and disk, where necessary), following internally published procedures.
   - 1.4. The Information Security Office may initiate an investigation if it becomes aware of an incident independently without being notified through the incident handling process.
     - 1.4.1. The Information Security Office will notify IT support personnel as appropriate.
   - 1.5. If necessary, the Information Security Office will invoke the RIT Critical Incident Management Process (CIMP).

2. **Information Security Investigation**
   - 2.1. The Information Security Office should initiate an investigation.
   - 2.2. The investigation will determine if there is risk of harm (e.g., Private Information or credentials have been acquired by an unauthorized party), and then determine further steps.
   - 2.3. All parties connected with the incident should cooperate with and assist the Information Security Office with the investigation according to procedures for incident handling.
     - 2.3.1. The Information Security Office may conduct an investigation, in compliance with the Privacy Policy.
     - 2.3.2. The Information Security Office will communicate appropriately with affected parties.

3. Containment

3.1. If an incident has the ability to spread to additional systems (e.g., involves credentials with administrative access to multiple computing devices, the threat is determined to be a worm, etc.), then personnel should assist in containment, including, but not limited to, providing forensic images (memory and disk) and baseline information as deemed necessary by the Information Security Office.

4. Eradication and Recovery

4.1. After providing requested information to the Information Security Office, personnel should attempt to remove the threat from (clean) the affected system or re-image the affected system and restore the system to service.

4.2. If eradication is unsuccessful, or the incident recurs after re-imaging, personnel should notify the Information Security Office and await further instructions.

5. Resolution

5.1. The Information Security Office will communicate resolution and lessons learned to management, personnel, and/or end users, as appropriate.

Effective Date: January 23, 2015

Standard History:
August 16, 2005
January 18, 2010
November 11, 2013