

Rogers State University
Information Technology Policies
Subject: Incident Response
Approved:
Effective Date: 1/19/12
Revised:

I. Purpose

The purpose of this policy is to provide the basis of appropriate reporting of incidents that threaten the confidentiality, integrity, and availability of university information assets, information systems, and the networks that deliver the information. This policy underlies the establishment and ongoing deployment of a trained computer security incident response team, formed with the purpose of managing IT Security incidents at Rogers State University. This effort is being taken to improve the response time for resolving incidents, provide consistent responses, and improve incident reporting.

The office of Academic Computing Services supports and protects open access to pursue all academic endeavors and to share information. Access to information systems and the network supports the academic community by providing an interchange of information using a variety of media. Rogers State University's network has become a mission critical resource and should be used properly. In order to better protect campus users, critical resources, and sensitive data, all incidents should be reported and investigated.

Identification of, and response and recovery from computer security incidents will be conducted within the framework of the Incident Response Plan. The plan is designed to provide effective coordination between university officials for protecting information assets and responding to computer security incidents.

II. Scope

This policy applies to use of any Rogers State University technology resource.

III. Policy

Users of computer devices that are connected to RSU's network must report all security incidents promptly to the Academic Computing Services office. Reported incidents will be classified and handled according to the procedures set forth in the Incident Response Plan.

In order to properly classify and investigate an incident, any records or data that are related to an incident and are under the authority of, or coming in the custody, control or possession of the university, must be made available to the Director of IT or designee upon request.

To ensure the integrity of the network during an incident, it may be necessary to disconnect a host, a group of hosts, or a network that is disrupting services to others. This includes hosts that are used by unauthorized parties to attack other systems on the RSU network.

IV. Responsibilities

Any user may report an incident to the Helpdesk in the office of Academic Computing Services. RSU faculty and staff members have a greater responsibility to do so, since they have a higher awareness of what may constitute an incident. Once an incident is reported to the office of Academic Computing services, the leader of the Incident Response team will be responsible for classifying the incident and engaging personnel from the Incident Response team as required. The Director of IT or designee will be in charge of securing any records, data, or equipment pursuant to the incident investigation.

V. Definitions

Computer Security Incident

An incident is an adverse event which results in a loss of confidentiality, disruption of data or system integrity, or disruption or denial of availability of a computer device or network. An incident implies harm or the threat of the occurrence of harm, and can include violation or imminent threat of violation of IT Security policies or standard security practices.

Examples include:

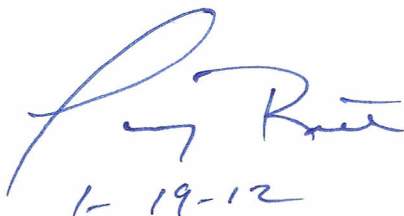
- Mishandling of Sensitive Data
- Denial of Service attacks
- Malicious Code
- Unauthorized Access
- Inappropriate Usage

RSU Network

Any equipment, owned or controlled by Rogers State University, involved in the processing or forwarding of electronic information. These systems include network devices such as routers, switches, and firewalls.

Computer Device

Any device involved in the processing, storage, or forwarding of electronic information. These devices include, but are not limited to, laptop computers, desktop computers, personal digital assistants, and servers.



A handwritten signature in blue ink, appearing to read 'P. R. R.', is written above the date '1-19-12'.