

DEPARTMENT: Information Services	POLICY DESCRIPTION: Security Incident Response Team
PAGE: 1 of 4	REPLACES POLICY DATED:
APPROVED DATE:	RETIRED:
EFFECTIVE DATE:	REFERENCE NUMBER:
NEXT REVIEW DATE:	APPROVALS: Business Unit Leader: Legal: Compliance:
Author: Jo Previte	

SCOPE: This policy applies to all facilities and information assets.
PURPOSE: This policy establishes a <u>Security Incident Response Team</u> (SIRT) to investigate any suspected intrusion (or attempted intrusion) into THE COMPANY'S computer systems, networks, or data resources or breaches of Security Policies. The objective of the SIRT is to investigate apparent or suspected security breaches so that current incidents can be controlled as quickly as possible to avoid damage to assets and so that future incidents can be prevented.
POLICY: THE COMPANY will establish a <u>Security Incident Response Team</u> to respond rapidly to any suspected security incident by identifying and controlling the suspected intrusion, reporting all findings to management and notifying users of proper procedures to preserve evidence. If a security incident does occur, it is Sirt's role to minimize damage to or vulnerability of information resources.
<p>PROCEDURE: Security Incident Response Team</p> <p>Responsibilities of SIRT:</p> <ul style="list-style-type: none"> • Respond to all security incidents or suspected incidents • Convene within 1 hour of notification of a potential incident • Identify affected critical systems • Assess damage and scope of the incident • Control and contain the breach/intrusion • Collect and document all evidence relating to the incident according to established procedures • Contact additional support members as necessary for investigation of a given incident • Provide liaisons to proper criminal and legal authorities <p>Availability of SIRT:</p>

DEPARTMENT:	POLICY DESCRIPTION:
Page 2 of 4	REFERENCE NUMBER:
EFFECTIVE DATE:	

Security incidents can arise at any time of the day and on any day of the week. Often attacks happen during non-business hours in the hope that it will go undiscovered until the damage is done. In order to react swiftly to minimize damage, the SIRT must be available 24 hours a day, 7 days a week.

Each core SIRT member must be on call to respond to an incident page immediately.

SIRT Team Composition:

Core Members:

IS Security Officer (team lead)
Data Network rep
Web/Internet Team rep
IS Security Supervisor
IS Security On call staff members

Support Members (called as incident dictates):

Internal Audit
IS Operations Mgr
System Engineering (for affected platforms)
Physical/Building Security
Human Resources
Legal
Helpdesk
Dept Mgrs/Supv for affected areas

SIRT Notification Process:

All security incidents will be reported to the Security Team member on call. The security team member on call will make a quick evaluation of the information available and determine whether or not SIRT activation is warranted. If so, the SIRT activation page (66) will be issued to all core members.

SIRT core team members are to report to the Data Center as soon as possible after the page is received, but required to do so within 60 minutes. If you can not physically join us in the Data Center, please call into the main helpdesk number and leave a number where you can be conferenced-in to the initial problem assessment meeting.

Core member responsibilities:

- Determine if the incident warrants further investigation/action
- Categorize the security incident

DEPARTMENT:	POLICY DESCRIPTION:
Page 3 of 4	REFERENCE NUMBER:
EFFECTIVE DATE:	

- Determine what, if any, support members should be called
- Ensure that proper procedures are followed for investigation
- Ensure the auditability of the investigation process
- Document the investigative steps taken and evidence gathered
- Provide a detailed analysis of the incident to upper management
- Recommend further actions/sanctions
- Provide liaison with appropriate law enforcement agencies
- Make recommendations to block further intrusions

Responsibilities of support SIRT members:

- Participate with SIRT core members in investigation and Evidence gathering related to a reported incident
- Make recommendations to block further intrusions

Security Incident Classifications:

- There will be 2 classes of security incidents:
 - Class 1 incidents require immediate SIRT activation.
 - Attacks against a firewall
 - Virus attacks
 - Internet abuse
 - Attacks against a server or mainframe
 - Attacks against any system containing patient Identifiable information
 - Class 2 incidents are those referred to SIRT after investigation Within a specific department or by the helpdesk or other Support group. Though these require SIRT review They may not be emergency situations and may be able To await review by SIRT during normal business hours
 - Suspected password misuse
 - Theft of property containing information assets
 - Request from management to review activity of a Specified employee

Escalation Process:

A class 2 incident can be raised to a class 1 in the following ways:

- The SIRT team leader (ISO) determines based on the initial Investigation of a class 2 incident that it is more widespread Or severe than previously suspected

DEPARTMENT:	POLICY DESCRIPTION:
Page 4 of 4	REFERENCE NUMBER:
EFFECTIVE DATE:	

- At the request of the CIO or other director level staff member or above

REFERENCES:

Information Technology Acceptable Use Policy

Information Security Policy