Cyber Tree Systems
A Business IT Solution Company

POLICY NAME	Incident Response		
DATE OF LAST REVISION:	9/4/2003	VERSION NO.	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

Purpose

The purpose of this incident response plan is to provide general guidance to both the technical and managerial staff of the Information Security department at Cyber Tree Systems (CTS). This plan will enable quick and efficient response to and recovery from incidents and enable qualified staff to carry out all necessary steps to correctly handle an incident, prevent or minimize disruption of critical computing services, and minimize impact on information systems owned by or in the control of CTS.

This document also serves as a guide for sharing information with other organizations both internally and externally, including other information security and law enforcement agencies, as well as a guide for pursuing appropriate legal action.

Scope

The guidance contained in this document is applicable to the Information Security staff at CTS, but emphasis is placed on the Security Incident Response Team (SIRT). This plan is to be implemented in the event an incident occurs, closed when the incident is declared to be resolved by an appropriate CTS official.

Roles & Responsibilities

Each Employee member has responsibilities related to the security of all CTS computing systems and networks. Due to this stipulation, non-critical incidents will be handled by CTS system administrators in the department in which the incident occurs. In the event that an incident is identified as critical and a SIRT assembly is mandated, then the SIRT will take control of the incident until it is resolved. Employees play a major role in this process as they function as the initial notification mechanism by detecting the event and then notifying the IS team.

Procedure

- If an employee discovers an incident, they will immediately notify the CTS Help Desk by phone, and a trouble ticket will be opened and escalated to the InfoSec department. Information collected by the help desk will consist of:
    - What was found
    - The time of the discovery
    - A description of the incident
    - Names of all employees involved.

- A senior technician will review the ticket and place the incident into a category. Any incident rated two, three, or four is escalated immediately to the InfoSec team by phone and email. The categories are as follows:
    - Category one – A disruption in service. Small attacks.

    - Category two – Possible or actual downtime to customer servers or low priority servers.
    - Category three – Possible or actual downtime to any core servers or network equipment.
    - Category four – Complete loss of service.

- Members in the InfoSec department will review the ticket and investigate the incident, forming the SIRT if necessary.

- After the incident has been properly identified, members will follow the appropriate procedure given for the situation. Members can create procedures other than the following at any time to improve the quality of this document. Current procedures include:
    - Power spike or brown-out procedure
    - DDOS attacks procedure
    - Active attack procedure

- SIRT will isolate the affected systems.
    - If the system is mission critical SIRT will make every effort to minimize system downtime. The system will be bit-copied and returned to service as soon as the incident is contained, and the system is deemed safe by SIRT.
    - If the system is determined to be non-mission critical, it will be taken out of service and bit copied for forensic investigation, returning to service only after the investigation is concluded.
- SIRT will investigate to determine how the incident was caused. Once determined, system/network vulnerabilities will be resolved, operational change recommendations will be submitted to managers and the network administrator for approval. Upon approval, they will be implemented, and the IRP will be modified as necessary. A file will be created with documentation for each incident. The following documents will be required:

- Forms

    - There are several forms to be utilized throughout the IR process they are:

Form	Use
Incident declaration	Used to specify the details of the incident once determined critical by IS staff.
Incident status update	Used to notify C-level and managerial staff disposition of incident during the investigation.
Incident closure and end of recover	Used at the end of an investigation to officially disposition the case as “closed” and determine if the affected systems can be returned to service.
Incident Review	Used at the end of the investigation to determine what process flows could be modified for efficiency and determine if legal recourse is necessary.
Incident Response Plan Addendum to Attack Success End Case	Used to modify the IR plan according to investigation findings to prevent future occurrences.

Planning, Testing, Training, & Exercises

This plan is to be tested bi-annually. Training and exercises for this plan will be conducted quarterly.

Appropriate testing, training, and exercises are to be decided by CTS officials and are non-negotiable. Testing, training, and exercises should be achievable and should not interfere with everyday business, or at least should conflict at a minimum.

Review Schedule

The Information Security department at CTS, along with the SIRT, will review this plan on an annual basis and at case closing of an incident and made changes accordingly if they are required. If a change to this plan is made, affected parties will be notified.

Revision History

Revisions made 9/4/2023