Cyber Tree Systems
A Business IT Solution Company

Incident Response

1.0 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.

2.0 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.

3.0 Roles & Responsibilities

Designated security team members, such as SOC personnel or a threat intelligence unit, have responsibilities related to the security of all CTS computing systems and networks. 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, the SIRT will take control of the incident until it is resolved. SOC personnel or the designated security team functions as the initial notification mechanism by detecting the event and then notifying the InfoSec team.

4.0 Procedure:

4.1 Discovery

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.

4.2 Categorization

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.

4.3 Review

Upon receiving the incident ticket, members of the InfoSec department will initiate an investigation to assess the severity and impact of the incident. If the incident is determined to be critical, the Security Incident Response Team (SIRT) will be formed to take control of the situation.

As part of the investigation, the following steps will be undertaken:

4.3.1 Firewall Log Review:

- Review firewall logs for potential indicators of compromise, such as unusual or suspicious traffic patterns.
- Ensure that all traffic from external IPs is logged, with particular attention paid to inbound and outbound communications that may indicate unauthorized access or data exfiltration attempts.
- Analyze both ingress (incoming) and egress (outgoing) firewall logs to determine if any data was exfiltrated or if there were unauthorized connections to internal systems.
- Flag any suspicious traffic for further analysis to assist in identifying the source and scope of the attack.

4.4 Implementation

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

4.5 Isolation

SIRT will isolate the affected systems.

4.5.1 Mission Critical System Breach

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.

4.5.2 Non-Mission Critical System Breach

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.

4.5.3 VPN Breach Procedure

In the event of a VPN compromise, SIRT will follow these steps:

- Immediately disable the compromised VPN access and any related accounts.
- Perform forensic analysis to determine the extent of the breach, including any data exfiltration.
- Identify and remediate any vulnerabilities that allowed the breach to occur.
- Notify affected users and departments, and assess the need for credential resets.
- Review VPN logs for any suspicious activity leading up to and during the breach.
- Apply necessary patches to the VPN infrastructure to prevent recurrence.

4.6 Post Incident Review

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.

5.0 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 course of the investigation.
• Incident closure and end of recovery	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.

Templates can be found in Appendix B (page 15 of this document)

6.0 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.

7.0 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.

8.0 Disaster Recovery Team Roles and Responsibilities

8.1 Team Composition

The Disaster Recovery Team (DRT) will be composed of members from various departments to ensure comprehensive coverage and effective coordination. The DRT should include the following roles:

- DRT Leader: Responsible for overall coordination and decision-making during a disaster recovery process.
- IT Recovery Lead: Oversees the recovery of IT systems and infrastructure.
- Network Specialist: Manages network-related recovery tasks.
- Application Specialist: Focuses on recovery of critical applications.
- Database Administrator: Handles the recovery of databases and data integrity.
- Communications Coordinator: Manages internal and external communications during the recovery process.
- Logistics Coordinator: Coordinates logistical support and resource allocation.
- Legal/Compliance Representative: Ensures recovery efforts comply with legal and regulatory requirements.
- HR Representative: Coordinates with employees and handles staffing and personnel issues during recovery.

8.2 Reporting Structure

The DRT Leader will report directly to the Chief Information Security Officer (CISO) and will provide regular updates on the recovery progress. The DRT Leader will also coordinate with other members of the executive leadership team to ensure alignment with organizational priorities and strategic goals. Each team member will report to their respective leads (e.g., IT Recovery Lead, Network Specialist) who will, in turn, report to the DRT Leader.

8.3 Leadership Roles

8.3.1 DRT Leader:

- Coordinates overall disaster recovery efforts.
- Acts as the primary decision-maker during the recovery process.
- Ensures communication flow between the DRT and executive leadership.

8.3.2 IT Recovery Lead:

- Manages the recovery of IT systems and infrastructure.
- Ensures that recovery tasks are completed according to the recovery plan.
- Coordinates with other technical leads to restore services.

8.3.3 Network Specialist:

- Focuses on restoring network services and connectivity.
- Analyzes network issues and implements solutions.
- Collaborates with the IT Recovery Lead on network-related recovery tasks.

8.3.4 Application Specialist:

- Restores critical applications and ensures their functionality.
- Works with application owners to prioritize recovery tasks.
- Provides technical support for application-related issues.

8.3.5 Database Administrator:

- Recovers databases and ensures data integrity.
- Implements backup and restoration processes.
- Collaborates with the IT Recovery Lead on database recovery tasks.

8.3.6 Communications Coordinator:

- Manages internal and external communications during the recovery process.

- Develops communication plans and ensures timely updates to stakeholders.
- Coordinates with the PR team for external communications.

8.3.7 Logistics Coordinator:

- Coordinates logistical support and resource allocation.
- Manages the procurement of necessary supplies and equipment.
- Ensures that the DRT has the resources needed to execute the recovery plan.

8.3.8 Legal/Compliance Representative:

- Ensures that recovery efforts comply with legal and regulatory requirements.
- Provides legal guidance during the recovery process.
- Coordinates with regulatory bodies and ensures compliance reporting.

8.3.9 HR Representative:

- Coordinates with employees and handles staffing and personnel issues during recovery.
- Ensures that employee needs are addressed and that there is adequate staffing for recovery tasks.
- Communicates with employees regarding recovery efforts and status.

9.0 Revision History

Revision Number	Date	Editor	Reason
2.0	1/16/2025	Aidan Schmeckpeper	Separated into library and prepared for future edits.
2.1	2/19/2025	Aidan Schmeckpeper	Better conform to new organizational chart and firewall/VPN policy