Cyber Tree Systems
A Business IT Solution Company

Contingency Planning

1.0 Purpose

The purpose of this policy is to provide the basis of appropriate response to incidents or disasters that threaten the confidentiality, integrity, and availability of Cyber Tree Systems (CTS) information assets, information systems, and the networks that deliver the information. This policy has been developed to provide guidance for response to and address potential incidents and disasters as they may occur against CTS.

2.0 Scope

This policy applies to all employees at CTS, all systems, and all services that the IS/IT/InfoSec staff is responsible for. This document serves as a guideline for the deployment of trained Security Incident Response Teams (SIRT) in crisis situations dealing with potential incidents and disasters as listed herein, but is not limited to only those events as published.

3.0 Contingency Planning Committee

3.1 Responsibilities

The Contingency Planning Committee (CPC) is a representative collection of individuals with a stake in the successful and uninterrupted operation of CTS. The CPC is charged with the development, testing, and maintenance of the Contingency Planning process, ensuring the clarity of accountability and coordination during incidents and disasters. This will provide clear direction in response efforts, reduce confusion, and ensure quick action.

3.2 Members

The following CTS employees are Members of the Contingency Planning Committee.

- VP, Operations
- VP, Maintenance
- VP, Finance
- Network Systems Manager
- Information Security Manager
- Director of Operations
- Director of Maintenance
- Director of Marketing
- SOC Manager
- IT Risk Manager

4.0 Definition of Critical Incidents

A critical incident is any adverse event, manmade or force of nature (see Table 1), which threatens the confidentiality, integrity, or availability of CTS's information systems and network infrastructure.

Category	Characteristic
Acts of Human Error or Failure	Accidental deletion of user desktop data or files by personnel (accidental user data deletion) Accidental deletion of server data or files by personnel (accidental server data deletion) Accidental release of critical information by personnel, including due to social engineering efforts (accidental leak) Accidental error or failure to follow procedure in creating software or hardware vulnerabilities Accidental modification or deletion of data due to failure to follow policies or procedures Installation of unauthorized software Improper configuration of software or hardware
Compromises to Intellectual Property	Unauthorized installation of software in violation of its licensing (piracy) Release of organizational information performed outside the bounds of policy, sometimes classified as a "leak" Violation of fair use of copyrighted material (plagiarism)
Deliberate Acts of Trespass	Unauthorized logical access to organizational information or systems (hacker probe) Unauthorized physical access to organizational facilities (trespasser)
Deliberate Acts of Information Extortion	Blackmail of organization for information assets (electronic extortionist)
Deliberate Acts of Sabotage or Vandalism	Intentional and unauthorized modification or destruction of organizational information assets (electronic vandal) Physical damage or destruction of organizational assets (physical vandal)
Deliberate Acts of Theft	Illegal "taking" of organizational assets
Deliberate Software Attacks	Email viruses and worms, other viruses and worms Email-based social engineering (phishing) Web-based malicious script

Category	Characteristic
	Denial-of-service attacks on organizational information assets Distributed denial-of-service attacks on organizational information assets
Forces of Nature	Flood Earthquake Lightning Landslide or mudslide Tornado or severe windstorm Hurricane or typhoon Tsunami Electrostatic discharge (ESD) Dust contamination Solar flare Electromagnetic radiation Humidity
Deviations in Quality of Service-by-Service Providers	Network connection outage due to cable severance (phone or ISP) Network connection outage due to service faults (phone or ISP) Power blackout Power brownout Power surge Power spike Power fault Power sag Other issues for example, (water, sewage, garbage, and other utilities)
Technical Hardware Failures or Errors	Equipment failure due to manufacturer or designer faults or defects.
Technical Software Failures or Errors	Software failure due to manufacturer or designer faults or defects (for example, bugs or code problems) Unknown software access bypasses (loopholes and trapdoors)
Technological Obsolescence	Use of antiquated or outdated technologies

Category	Characteristic
	Failure to maintain or update antiquated or outdated equipment-based data storage

Table 1 Threats (potential incidents) adopted from the Whitman ACM Model

5.0 Organization Structure & Delineation of Roles, Responsibilities & Levels of Authority:

5.1 Incident Response Team

The Incident Response Team (IRT) will consist of information technology staff and managers from all departments within CTS. The IRT implements the policies and procedures, according to the Incident Response or Disaster Recovery Plans, in the event of an incident, as defined by either the IRP or DRP.

5.2 Critical Incident Coordinator

The Critical Incident Coordinator is designated by the CTS management team, either the CISO for Information Security incidents or VP of Operations for a natural disaster, to act as the lead in the event a critical incident occurs. This individual is responsible for the management and process of the incident and the incident response or disaster recovery plan.

5.3 Security Incident Response Team (SIRT)

The Security Incident Response Team (SIRT) consists of full-time employees with information technology job functions who have been specially trained in IS incident management; each member has a distinct response role. The SIRT works under the direction of the CISO.

5.3.1 Responsibilities

The SIRT's main focus is to implement the IRP when a critical IS incident occurs. In the event of such a critical incident, normal job functions are considered secondary until the incident is resolved.

- 5.3.2 Members
- SIRT Team Leader
- SOC Analysts
- Threat Intelligence Analysts
- Forensic Analysts
- Network Engineers
- Legal & Compliance Representatives
- HR & Insider Threat Team
- Public Relations & Communications

5.4 Users

Users are CTS employees that are not directly involved in the incident response process, however, play a major role as a notification mechanism. Their responsibility is to inform the information technology staff that a potential incident has occurred.

5.5 Categorization of Incidents

Each incident can be assigned a category rating. See Section 4.2 of the IRP.

5.6 Performance Measures

Performance will be judged on response time and recovery time based on the Categorization of the incident.

5.7 Documentation

For each incident that occurs, a series of documents will be filled out and kept for a period of one year.

5.7.1 Incident Forms

The following is a list of forms required for each incident; see section 5 of IRP for definitions

- Incident declaration
- Incident status update
- Incident closure and end of recovery
- Incident Review
- Incident Response Plan Addendum to Attack Success End Case

5.7.2 Contact List

The following documents are maintained in Appendix A of this document (page 14 of this document)

- Notification List
- First Responders List
- Emergency Contact

6.0 Network Resilience and Remote Access Protocols

6.1 Redundant VPN Gateways

To ensure the continued availability of secure remote access in the event of network failures, redundant VPN gateways will be deployed across geographically dispersed locations. These gateways will be configured in a failover setup, ensuring that if one gateway fails, the backup gateway automatically takes over to maintain uninterrupted service for remote employees and critical access.

6.1.2 Responsibilities for VPN Gateway Failover

The IT infrastructure team is responsible for the maintenance and regular testing of redundant VPN gateways to ensure operational resilience.

The team will perform quarterly tests to verify failover functionality, including switching between primary and backup VPN gateways.

Any issues identified during testing must be resolved within a predefined maintenance window and documented in the incident log.

6.2 Failover Firewalls

In addition to redundant VPN gateways, failover firewalls will be configured to ensure the continuous protection of the organization's network perimeter. This setup will provide redundancy in the event of hardware failure or network disruptions, ensuring that malicious traffic is blocked and that access to the network remains secure.

6.2.1 Responsibilities for Firewall Failover

The IT security team is responsible for configuring and testing failover firewalls to ensure seamless functionality during failover events.

The firewall configurations will be reviewed every six months and after any major network changes to maintain effectiveness.

6.3 VPN Accounts as Emergency Accounts

In the event of a disaster, VPN accounts will be specifically defined as emergency accounts for accessing critical systems remotely. These accounts will be used exclusively for disaster recovery scenarios and will have the highest level of security controls, including multi-factor authentication (MFA) and access logging.

6.3.1 Emergency Account Access Control

VPN emergency accounts will be provisioned only for senior staff, members of the Incident Response Team (IRT), and designated disaster recovery personnel who require immediate access to critical systems in a disaster.

The use of emergency VPN accounts will be tightly controlled through role-based access controls (RBAC), and access permissions will be reviewed annually.

These accounts will be created as part of the Disaster Recovery Planning and will be clearly outlined within the Contingency Response Plan.

6.3.2 Security and Monitoring of Emergency Accounts

Emergency VPN accounts will be closely monitored, with real-time alerts sent to the security operations center (SOC) for any unusual activity, login attempts outside of regular working hours, or attempts to access non-critical systems.

Audit logs for emergency account access will be retained for a minimum of one year and periodically reviewed by the Information Security Manager to ensure compliance with security protocols.

6.4 Testing and Maintenance of Network Resilience and Remote Access

Redundant VPN gateways, failover firewalls, and emergency VPN accounts will be tested during Disaster Recovery Drills to ensure their functionality in various disaster scenarios. These tests will involve simulated failovers of network services and remote access functionality to verify that all recovery procedures can be executed effectively.

The results of these tests will be documented, with any gaps or weaknesses identified and addressed before the next planned drill.

7.0 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