Cyber Tree Systems
A Business IT Solution Company

POLICY NAME	**Contingency Planning**		
DATE OF LAST REVISION:	9/4/2003	**VERSION NO.**	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

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.

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 deployment of trained Security Incident Response Teams in a crisis situation dealing with potential incidents and disasters as listed herein but is not limited to only those events as published.

Contingency Planning Committee

- Responsibilities

  The Incident Response Planning Committee is a representative collection of individuals with a stake in the successful and uninterrupted operation of CTS. The Incident Response Planning Committee is charged with the development, testing, and maintenance the Incident Response Plan.

- 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 Operation
    - Director of Maintenance
    - Director of Marketing

- 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 • Denial-of-service attacks on organizational information assets • Distributed denial-of-service attacks on organizational information assets
Forces of Nature	• Flood • Earthquake • Lighting • Landslide and 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 • Failure to maintain or update antiquated or outdated equipment-based data storage

Based on the nature and severity of the incident or disaster, the following policies will be implemented, and the appropriate teams will be notified:

- Incident Response Plan
- Disaster Recovery Plan

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

- 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.

- Critical Incident Coordinator

  The Critical Incident Coordinator is designated by the CTS management team, either the InfoSec Manager for IS 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.

- 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 InfoSec Manager.

  - Responsibilities

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

  - Members
    - CEO
    - CISO
    - CIO
    - IT Manager
    - Security Manager

        - Operations Manager

- 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.

- Categorization of Incidents

  Each incident can be assigned a category rating. See Section 4.2 of the IRP (page 8-9 of this document).

- Performance Measures

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

- Documentation

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

      The following is a list of forms required for each incident; see section 5 of IRP for definitions (page 9 of this document)
        - Incident declaration
        - Incident status update
        - Incident closure and end of recovery
        - Incident Review
        - Incident Response Plan Addendum to Attack Success End Case
    - 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 List

Revision History

Revisions made 9/4/2023