Cyber Tree Systems
A Business IT Solution Company

Disaster Recovery

1.0 Purpose

The purpose of this policy is to provide a plan to respond to a disaster that destroys or severely cripples the facility's central computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

2.0 Objectives

This disaster recovery plan has the following primary objectives:

- Present an orderly course of action for restoring critical computing capability to the CTS facility within 14 days of initiation of the plan.
- Set criteria for making the decision to recover at a cold site or repair the affected site.
- Describe an organizational structure for carrying out the plan.
- Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
- Identify the equipment, floor plan, procedures, and other items necessary for the recovery.
- Ensure clear accountability and coordination during disaster recovery by defining dedicated leadership roles for all recovery teams.
- Incorporate industry standard performance metrics and incident closure rates to continuously improve recovery processes.

3.0 Notification

Responsibility for notification will fall to the Incident Response Team and/or SOC analysts initiating the notification system in the event that automated notifications from SIEM do not apply.

4.0 Recovery Facility

If the CTS facility is destroyed in a disaster, repair or rebuilding of that Facility may take an extended period of time. In the interim, it will be necessary to restore computer and network services at an alternate site.

The Facility has a number of options for alternate sites. The use of cloud services should be included in the recovery facility set up as a backup measure for vital business information assets.

The options are not limited to but include:

- Hot Site
- Cold Site
- Relocation to other municipal facilities outside of the affected area.
- Cloud Services

Decisions regarding recovery sites should be made in coordination with the CPC to ensure appropriate oversight and rapid decision making.

5.0 Safety Issues

All disaster recovery procedures should be performed in conjunction with local authorities to ensure safety in all areas. In cases where officials deem it unsafe to continue or perform an action, that asset maybe classified as a loss.

6.0 Data Protection Strategies

In preparation for a disaster, the InfoSec Manager will continue standard data backup strategies from the onsite RAID array. Specifically: Monday through Thursday onsite differential backups. Friday full backups are stored off-site at a location to be determined by the InfoSec Manager.

The use of cloud services should be included in the data protection strategies as a backup measure for vital business information assets. CTS will also implement remote backup via cloud services, such as AerOne Cloud Services, for critical data. A backup cloud service provider should also be included.

In the event of a disaster, only authorized personnel will be allowed on site for security and safety reasons. Data recovery should be considered a sensitive matter and will be handled exclusively by a data recovery team.

Firewalls and VPNs will be configured and maintained to ensure that the organization's network remains secure during a disaster.

- VPN Configuration: The VPN should be designed for secure remote access during a disaster. It will allow personnel to work remotely if the primary site is affected. The VPN infrastructure must be tested and reviewed as part of the disaster recovery exercises.
- Firewall Security: Firewalls will be configured to ensure that only authorized personnel can access recovery systems during a disaster. They will be adjusted as needed to allow specific traffic related to disaster recovery activities while blocking any malicious attempts to infiltrate the network.

These cybersecurity measures should be regularly reviewed as part of the disaster recovery testing and exercises.

7.0 Disaster Recovery Teams

To enhance the effectiveness and coordination of disaster recovery efforts, the composition of the Disaster Recovery Teams (DRT) and their leadership roles must be clearly defined. The following changes are recommended to ensure the proper management of recovery operations and improve overall team accountability:

7.1 Contingency Planning Committee (CPC)

The Contingency Planning Committee (CPC) shall be formally introduced as a key oversight body for disaster recovery efforts. The CPC will ensure the integration of disaster recovery processes with broader organizational goals and will have the responsibility for overall coordination during recovery operations.

The CPC will be composed of dedicated cybersecurity professionals to provide specialized knowledge and ensure all technical, legal, and communication needs are addressed during recovery efforts. The key roles and responsibilities of the CPC are outlined below:

- SOC Analysts: Provide real-time monitoring and incident response during recovery to ensure the security of all IT systems.
- IT Risk Managers: Assess and mitigate any emerging risks during recovery operations to ensure continuity and security.
- Legal and Compliance Representatives: Ensure recovery actions comply with regulatory requirements and legal obligations.
- Public Relations and Communications: Manage external and internal communications related to recovery efforts, ensuring consistent messaging and reputation management.

The CPC will also play a crucial role in overseeing the leadership and effectiveness of the Disaster Recovery Teams by ensuring that all operations are aligned with the organization's recovery objectives.

7.2 Disaster Recovery Team Leadership Structure

Each of the Disaster Recovery Teams will be led by a designated leader responsible for managing the recovery of their specific functional area. These leaders will be empowered with clear decision-making authority and will report directly to the Contingency Planning Committee. The team structure should be as follows:

7.2.1 Recovery Management Team Leader

Responsibilities: Oversee the entire recovery process, ensuring that all teams are coordinated and that recovery operations are progressing according to plan. This leader will be responsible for making critical decisions, such as activating specific recovery procedures, determining the allocation of resources, and managing recovery priorities.

Key Functions:

- Coordinate communication between all recovery teams.
- Monitor recovery progress and make necessary adjustments.
- Report recovery status and any issues to the CPC.

7.2.2 Network Recovery Team Leader

Responsibilities: Ensure the restoration and availability of the organization's network infrastructure during recovery operations. This leader will coordinate the efforts of network engineers and ensure that critical network services are restored as quickly as possible.

Key Functions:

- Prioritize network recovery to ensure connectivity for critical business operations.
- Troubleshoot and resolve network issues that arise during the recovery process.
- Report network recovery status to the Recovery Management Team Leader and CPC.

7.2.3 Application and Data Recovery Team Leader

Responsibilities: Lead efforts to restore key business applications and ensure the integrity and security of recovered data.

Key Functions:

- Ensure that application recovery meets defined service level agreements (SLAs).
- Validate and test the integrity of recovered data.

- Work with IT risk managers to address any data or application security concerns.

7.2.4 Infrastructure Recovery Team Leader

Responsibilities: Manage the recovery of physical and virtual infrastructure, including hardware, storage systems, and data centers.

Key Functions:

- Ensure that critical infrastructure components are restored and functioning correctly.
- Oversee the setup of alternate recovery sites if needed.
- Coordinate with vendors for the provision of replacement hardware if required.

7.2.5 Communication and Documentation Team Leader

Responsibilities: Ensure effective communication within the disaster recovery teams and with stakeholders, including employees, clients, and regulatory bodies.

Key Functions:

- Maintain up-to-date documentation of recovery actions and decisions.
- Ensure consistent messaging across all communication channels.
- Report to the CPC regarding the status of communication efforts and stakeholder concerns.

8.0 Equipment Protection & Salvage

Below is information on procedures to be used immediately following a disaster to preserve and protect resources in the affected area.

It is imperative that any equipment, magnetic media, paper stocks, and other items at the damaged primary site be protected from the elements to avoid any further damage so an attempt can be made to recover data.

- Gather all magnetic tape cartridges into a central area and quickly secure them in antistatic, nonmetal containers to avoid water damage.
- Cover all computer equipment to avoid water damage.
- Cover all undamaged paper stock to avoid water damage.
- Ask local authorities to post security guards at the primary site to prevent property theft or vandalism.
- After securing the media and equipment, a line-item inventory should be conducted and all assets cataloged.

Once completed, a secure recovery site should be established, equipment should be transported, and data recovery should begin as soon as possible to avoid further loss.

9.0 Damage Assessment

The initial damage assessment is performed to determine the extent of damage to company assets and housing facilities. Once the extent of damage is assessed, a priority is assigned to “lost” equipment and management is notified. The team responsible for Damage Assessment should be lead by someone from the CPC to ensure oversight and proper prioritization of recovery efforts.

10.0 Equipment & Supplies

Each department head must submit a list of equipment and supplies needed to continue normal business operations to the DR team leaders. These lists, as well as vendor contact information, should be reviewed by the CPC and stored with the DRP manual.

11.0 Planning, Testing, Training & Exercises

The organization’s disaster recovery and incident response plans will undergo regular testing, training, and exercises to ensure readiness in the event of a disaster. These activities are critical for maintaining an effective response and for ensuring that all teams can coordinate efficiently during recovery operations.

11.1 Testing Schedule

The disaster recovery plan is to be tested bi-annually to assess its effectiveness and readiness. These tests will simulate a variety of disaster scenarios, including data loss, fire, flood, electrical outages, and extreme weather events such as tornadoes or hurricanes, based on the organization's location and specific risks.

The testing schedule will explicitly include coordination with the Contingency Planning Committee (CPC) to ensure that incident response procedures are tested with dedicated cybersecurity staff. This will ensure that all relevant teams, including cybersecurity professionals, are actively engaged in the testing process.

It is recommended to implement CPC-led tabletop exercises as part of the bi-annual tests. These exercises will allow the CPC to simulate real-world disaster scenarios and test coordinated response strategies across all teams, ensuring that leadership can effectively manage disaster recovery operations and maintain communication throughout the process.

11.2 Training and Exercises

Regular training will be conducted quarterly for all relevant personnel, with specific focus on:

- Simulated disaster scenarios, including but not limited to data loss, fire, flood, electrical outage, and tornado/hurricane (depending on the location).
- Incident response procedures to ensure team members are prepared for rapid and efficient action during actual events.

CPC and Incident Response Team members will be required to undergo specialized training to ensure they are prepared for their roles in coordination and leadership during a disaster. This includes training on how to manage and lead recovery efforts, as well as how to effectively communicate with other teams and external stakeholders.

The frequency and nature of testing, training, and exercises will be determined by CTS officials, ensuring that the scenarios chosen are relevant to the organization's specific needs and risks. These activities should be non-negotiable and designed to be achievable without disrupting everyday business operations. Where possible, efforts will be made to minimize conflict with daily activities to maintain normal business functions.

12.0 Review Schedule

To ensure the disaster recovery and contingency planning processes remain effective, relevant, and aligned with industry best practices, the Contingency Planning Committee (CPC) will meet annually to review and assess the current disaster recovery policy, contingency planning procedures, and organizational structure.

12.1 Annual Review Requirements

The Contingency Planning Committee (CPC) is responsible for conducting an annual review of the entire disaster recovery and contingency planning process. This review will encompass all aspects of the plan, including response strategies, team roles, and responsibilities, as well as the readiness and effectiveness of all disaster recovery procedures.

The CPC will assess the effectiveness of the current disaster recovery teams and ensure they are appropriately structured to meet the organization's evolving needs. Any necessary adjustments to the roles, responsibilities, and composition of the Disaster Recovery Teams will be made based on lessons learned from previous tests and exercises, as well as any changes in the organization's operations or risk profile.

12.2 Review of Organizational Structure

The annual review will also include an assessment of the organizational structure related to disaster recovery and contingency planning, particularly with regard to team leadership. This will include an examination of:

- Any changes to the CPC membership, ensuring that it remains composed of the necessary cybersecurity professionals, such as SOC analysts, IT risk managers, legal/compliance representatives, and public relations staff related to cybersecurity.
- Adjustments to the Disaster Recovery Teams and any changes in leadership roles within those teams. This may include the addition of new recovery team leaders or shifts in responsibilities to ensure continued effective coordination and decision-making during a disaster recovery scenario.
- Any adjustments or changes to the organizational structure will be reflected in an updated version of the policy and communicated to all relevant stakeholders to ensure that the disaster recovery plan remains aligned with the company's operational needs and security posture.

12.3 Documentation and Implementation of Changes

Following the annual review, all agreed-upon changes to the disaster recovery and contingency planning process will be documented. Any updates to the policy, including structural or procedural changes, will be reflected in the official disaster recovery documentation and communicated to all involved parties.

The updated policy will also be shared with the appropriate departments and leadership to ensure that all stakeholders are aware of changes and have the necessary information to implement the revised procedures

13.0 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