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

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.

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.

Notification

An Automated Emergency Notification System is required by policy. The system should call employees in order of Chain of Command to notify special teams, officials, and other employees if and where to report.

Recovery Facility

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

The Facility has several 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

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 may be classified as a loss.

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.

Disaster Recovery Team

Employees will be trained and assigned to Disaster Recovery Teams. Examples of such teams are not limited to but include the following:

- Recovery Management Team
- Damage Assessment Team
- Facility Recovery Team
- Network Recovery Team
- Platform Recovery Team
- Applications Recovery Team
- Computer Operations Team
- Administrative Support Team

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.

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.

Equipment & Supplies

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

Planning, Testing, Training, & Exercises

This plan is to be tested bi-annually. Training and exercises for this plan will be conducted quarterly, to include simulated data loss, fire, flood, electrical outage, and tornado/hurricane (depending onsite location).

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 InfoSec Office at CTS will review this plan on an annual basis and make necessary changes. If a change to this policy is made, affected parties will be notified.

Revision History

Revisions made 9/4/2023