Catholic Charities Disabilities Services

Agency Standard and Procedure

Standard Category	Administration
Standard Title	Information Technology Disaster Recovery Plan
Regulations	
Original Issue Date	July 15, 2014
Latest Revision Date	
Number of Pages	5
Attachments	
Approved by: **Anne M. Ogden, Executive Director**	Anne M. Ogden

The Information Technology Department provides services that, in some manner, virtually every other department at Catholic Charities Disabilities Services (CCDS) are dependent upon. Without telephones, networks, or any one of several critical servers, some aspect of the business would come to a standstill if a failure occurred. In recognition of these dependencies, it is of utmost importance that the IT Department be prepared to respond to a disaster in an orderly, timely, and efficient fashion. This document describes the Disaster Recovery Plan that the IT Department will use in the event that a disaster affects department operations and services. It includes a summary of the current services, identification of the services most critical to company operations, and how these services will be reconstituted following a disaster.

Scope of This Plan

This plan provides the IT department with the ability to address two areas:

1. It enables the department to restore CCDS's core information systems in the event of a disaster.
2. It identifies areas of substantial risk and exposure to disaster, and helps us reduce these risks.

This plan is not intended to be a detailed, step by step series of instructions to follow. It is intended to be a roadmap to lead the recovery team from the incident through a decision making process to implementation of restored services. Although it is targeted at the most likely types of disasters that could be encountered, it may be adapted as necessary for recovery from other situations.

Disaster Scenarios

This plan focuses on recovering from a disaster that involves fire or partial flooding of one or more sites at CCDS's corporate office in Albany, NY. The building deemed most critical is 1 Park Place, where IT houses its core systems. Secondary facilities for network services are located at 98 Slingerlands St., Albany, NY.

Current Practices and Procedures

An understanding of the fundamental business practices currently followed by the department is essential to recovering department operations.

The key activities include:

- Data backup and restoration
- Server and systems administration
- System shutdown and startup
- Identification of critical systems

Data Backup and Restoration

Backups are performed 7 days a week on our Unitrends backup server and are stored on the server for a minimum of 30 days. At the end of each month an archive backup is completed and sent to a fireproof safe at a CCDS residence for offsite storage. Long term archives are set aside monthly (retained for one year). Key servers across the network are included in the backup schedule.

Server and System Administration

Current practice for managing servers and desktop systems across the agency include:

- Ensuring high availability of servers during business hours
- User support and desktop system support during normal business hours
- Monthly scheduled updates for critical servers
- Other major server maintenance is scheduled outside of normal business hours

Critical Systems

The systems, services, and functions identified as necessary to current business operations are as follows:

Microsoft Exchange Email System (CCDS-EXCH)
Fund-EZ Accounting System (CCD-FUNDEZ)
HR Database (CCDS-FS1)
File Server (CCDS-FS1)
Terminal Server (EBS-SQL)
Domain Controller (CCDS-DC2)
VOIP (Tech Valley Communications)
Data Service (Tech Valley Communications)

Recovery Operations

Re-establishing operations after a disaster requires:

- Identification of the most critical services provided by the department
- Setting priorities for re-establishing those services
- The staff required for a recovery
- System configuration information

Recovery Process

The recovery process consists of two basic phases:

- An initial reaction phase where notifications are made, the staff is assembled, information gathered, and an action plan developed
- The recovery phase, where resources are acquired, data recalled, and services are restored as much as possible.

The steps to be followed are:

1. The discoverer of a disaster will notify the people below. Each of these people will notify others as appropriate. For situations during normal business hours, personal contact will be made.
    - Local authorities (911) in the event outside assistance is necessary
    - Picotte Co, Facilities Manager
    - IT Manager, Christopher Delaney
    - Executive Director, Anne Ogden

2. Initial organization and preparation for the recovery:
    - Notify and assemble the recovery staff
    - Review this recovery plan with the staff
    - Organize for damage assessment
    - Establish communications systems for the staff
    - Assign duties and responsibilities to the staff

3. Perform a damage assessment
    - Conduct a site survey of the affected area
    - Inventory any salvageable or usable equipment

4. Plan for recovery
    - Compile a master inventory of salvageable equipment
    - Review the overall damage with the recovery staff
    - Develop a detailed action plan
    - Notify the appropriate vendors and service providers
    - Communicate status to executive staff

5. Salvageable Operations
    - Recover all salvageable hardware
    - Service or refurbish equipment as necessary

Critical Services and Recovery Priorities

Recovery Options are prioritized based on agency needs.

These priorities are:

Priority 1:

Power
Establish phone services VOIP
Voicemail
Phone service to recovery staff
Phone service to executive staff
Install the server LAN Hubs, routers, and switches local to the room
Cabling within the room
Windows primary domain control, print, DHCP
File servers
Mail server
Terminal Server
Directory server
Install or connect to the building LAN
Network routers, switches, etc.
Cabling
Install the Internet service connections to service provider

Priority 2:

Re-establishment of business systems
Accounting
Payroll
HR Systems

Priority 3:

All remaining services

Equipment List

The following equipment is required to re-establish the Priority 1 services listed above to a basic, nominal level of service. It is not intended to duplicate the original performance, but rather to provide a minimally acceptable level of service. This equipment may be obtained from CCDS's normal vendors, or it may be deployed from the salvaged equipment pool.

- Mitel VOIP
- First Light Fiber Connection for Internet Service
- Server Farm located on HYPER-V Replication Server
- Firewall router

Recovery Team

The initial response team will consist of all on-call staff, managers, and directors. The remaining department staff will be called in as required. Should additional staff be required as initial response, managers will contact the appropriate people.

System Configuration Information

The hardware listed above will require configuration to restore reasonable levels of service. The information, data, applications, and instructions that are required for this are:

- Administrative passwords for servers, applications, and network hardware. This information is currently located in the fire safe off site.
- Media containing operating systems, applications, and installed software and licenses, which are maintained by IT manager.

Testing Disaster Recovery

The Disaster Recovery plan will be tested at a minimum of every 6 months, and more if major infrastructure changes occur.