DELAWARE COUNTY DISTRICT LIBRARY

IT Disaster Recovery Plan

2012

84 E. Winter St. Delaware, Ohio 43015

I. Overview

This Information Technology Disaster Recovery Plan (DRP) has been developed by DCDL information technology leaders to provide guidance for responding to IT disasters and other security incidents. Disasters and security incidents may threaten the organization's ability to carry out its mission as well as other operational functions. Advance planning and preparation will allow the organization to:

- Continue serving its patrons and community
- Ensure the availability of patron information as well as business information
- Minimize loss and facilitate recovery of core IT and business assets
- Preserve the organizations public image and reputation within the community
- Prevent the disaster or incident from threatening the organizations long-term stability and viability
- Heighten organizational awareness, allow for advanced preparation, and workforce education and training

The DRP is a collection of references, guidelines, policies, procedures, forms, and suggestions designed for responding to security incidents and disasters. Components of this plan include:

- Disaster Recovery and Restoration
- Emergency Mode Operation
- Applications and Servers
- Data Back-Up/Restore
- Vendor Contact Information
- IT Staff Contact Information

Objections of the Disaster Recovery Plan

- To provide DCDL with a viable and maintained IT Disaster Recovery Plan (DRP) which, when executed, will support a timely and effective resumption and recovery of all interrupted business operations.
- To minimize the possible financial and business impact to DCDL as a result of an interruption of normal business operations
- To reduce operational effects of an information technology disaster on DCDL as an organization by providing a set of pre-defined and flexibility guidelines and procedures to be used in directing a resumption and recovery of processes
- To meet the needs of DCDL patrons, workforce members, and other communities reliant on the organizations ability to provide services during and following a disaster situation.
- To protect the public image and credibility of DCDL

Applicability

The DRP has been developed to support the organizations Emergency Preparedness/Disaster Plan, providing

further specificity to address IT needs. The DRP applies to all hardware, software, workstations, applications, systems and networks (LAN, WAN, Internet, Intranet), and other components of the organizations information technology.
The DRP is limited to the recovery of IT services only. The DRP does not address disaster prevention or long-term restoration of information technology. The DRP does not address the recovery of business processes that may be last in the various departmental or business unit operations. Downtime/recovery processes are the responsibility of each department/business unit unless specifically covered in the DRP.

Key Definitions

Disaster (Information Technology): An event that significantly challenges the continuation of normal information system functions impossible; an event which would render the information system unusable or inaccessible for a prolonged period of time (may be departmental or organization-wide).

Disaster Recovery Coordinator: Individual assigned the authority and responsibility for the implementation and coordination of IT disaster recovery operations.

Disaster Recovery Plan: The document that defines the resources, action, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business within the stated disaster recovery goals (DRJ).

Recovery Time Objective: Amount of down time before outage threatens survival of the organization/mission critical processes.

Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices, or an adverse event whereby some aspect of computer security could be threatened. An IT Disaster would be considered a security incident.

Authority

The Disaster Recovery Coordinator (DRC), in conjunction with the organizations administrative leadership, shall have the responsibility and authority to take whatever steps necessary to identify, respond, contain, and eradicate the impact of an IT disaster.

Administrative Oversight

A senior administrative leader shall be assigned to provide support and assistance during the IT disaster recovery process. This individual shall also research the organizations disaster insurance coverage and determine available financial resources.

Organization & Notification

Once an IT disaster has been declared and the IT Disaster Plan activated, the DRC shall communicate such to senior administrative leaders and implement the IT recovery steps outlined in this plan. The DRC shall determine the need to notify external resources including vendors to assist with IT disaster recovery

activities.

Disaster Recovery Coordinator (DRC)

Disaster Recovery Coordinator (DRC) Position Description/ Job Action Sheet	
Position Assigned To:	IT Leader or Designee
Position Reports To:	Library Director or Designee
Authority Level:	To Be Determined
Mission/Responsibility:	Implement, organize and direct information systems disaster recovery options.

Disaster Recovery Coordinator (DRC) Position Description/Job Action Sheet	
Criticality Level	**Job Actions**
Immediate (0-6 Hours)	☐ Review DRC Job Action Sheet and IT DRP ☐ Identify DR command center/ assembly site ☐Notify Disaster Recovery Team Members ☐ Assemble Team at Command Center ☐ Gather and Assemble Resources (see checklist) ☐ Provide Team Briefing ☐ Review Tasks To Be Performed and Assign Personnel ☐ Notify Other Key Leaders as Necessary ☐ Notify Vendors as Necessary ☐ Determine Need For Additional Support/Team Members
Intermediate (6-12 Hours)	☐Assess Continued Staffing Needs/ Staff Relief
Ongoing	☐ Damage Assessment ☐ Assess Recovery Priorities ☐ Communicate IT Disaster Recovery Status with Administration ☐ Approve Expenses Related to Recovery Processes
Extended (> 12 Hours)	☐Assess Need for Staff Relief/ Additional Resources
Follow-Up (Following Disaster)	☐Facilitate “post mortem” evaluation of IT Disaster and Recovery Processes ☐Revise IT DRP as Needed/Necessary

IT Disaster Recovery Team Emergency Contact Information

Members of the IT Disaster Recovery Team shall be contacted immediately once the IT DRP has been activated. The following information should be provided at the time of contact:

- A Brief Description of the problem
- Location of the IT Disaster Recovery Command Center
- Phone Number of the IT Disaster Recovery Command Center
- Identification of immediate Support Required (Services, Equipment, Ect.)
- Information Regarding How the Facility can be Entered (Need for Identification/Badge)

Contact Information is available as an attachment to this plan.

Damage Assessment

Damage assessment shall be carried out to determine disaster recovery requirements. A preliminary damage assessment shall address:

- Cause of the emergency or disruption
- Potential for additional disruptions or damage
- Areas affected by the disruption
- Status of physical infrastructure (where computer equipment is located)
- Inventory and functional status of computer equipment
- Type of damage (e.g., water, fire, electrical surge, ect.)
- Items to be replaced (e.g., hardware, software, other)
- Estimated time to restore to normal operations

IT Disaster Recovery Command Center

The command center will function as the centralized location for IT disaster recovery processes. The DRC will make the determination as to the location of the command center. The location will be determined by the disaster type and available resources. The command center location must be able to accommodate the necessary critical resources and equipment required for disaster recovery:

- Hardware, Software, Other Equipment
- Electrical Support
- Telecommunications Support
- Desks, Chairs, Tables, Lights

Primary Location			
Facility Name:	Delaware County District Library (Main)	Floor Room:	1st Floor/Server Room

Address:	84 E. Winter St. Delaware, OH 43015		
Phone #:	740-362-3861	Fax #:	740-369-0196
Contact Person:	Traci Higgins	Phone #:	740-341-9532
Alternate Contact:	Don Yarman	Phone #:	614.946.8813
Security Considerations: All people entering the facility will need to be identified as staff by either showing an employee badge or photo ID via staff roster.			

Recovery Command Center Alternative Site

The IT leadership shall make the determination as to whether or not recovery activities should be relocated to an alternative site. A pre-determined alternative site should be designated for major disruptions with long term effects. The alternative site should allow the organization to recover and perform system operations for an extended period of time.

Alternative Location			
Facility Name:	Delaware County District Library – Orange Branch	Floor/Room	1st Floor-IT Office
Address:	7171 Gooding Boulevard Delaware, OH 43015		
Phone # :	740-549-2665	Fax #:	740-549-0022
Contact Person:	Traci Higgins	Phone #:	740-341-9532
Alternative Contact:	Don Yarman	Phone #:	614-946-8815
Security Considerations: All people entering the facility will need to be identified as staff by either showing an employee badge or photo ID via staff roster.			

Recovery Resources Supply Checklist

Recovery Resources Supply Checklist

Workspace

- ☐ Desk, Chairs, Tables, Lights
- ☐ Electrical Support
- ☐ Telecommunications Support

Documentation

- ☐ Hardware Inventory List and Serial Numbers
- ☐ Software Inventory List and License Numbers
- ☐ Network Schematic Diagram
- ☐ Contract and Maintenance Agreements

Hardware

- ☐ PC's / Laptops
- ☐ Printers
- ☐ Scanners

Forms

- ☐ Maintenance Forms
- ☐ Message Pads

Software

Back-up Copies of Data Files

Communication

- ☐ Telephones
- ☐ Cell Phones with chargers
- ☐ Fax and back-up fax
- ☐ Dedicated phone line
- ☐ Radios (walkie talkies)
- ☐ Organizational Contact Info
- ☐ Telephone Directories
- ☐ Telephone Log

Other Supplies

- ☐ Office Supplies (pens, paper, folders, paper clips, scissors, staplers, tape, ect.)
- ☐ Office Equipment (shredder, copiers, ect.)
- ☐ Camera / Video Recorder
- ☐ Film / Recording media
- ☐ Duct Tape
- ☐ Back-up Media
- ☐ Flashlight and spare batteries
- ☐ Telephone Log
- ☐ Area Maps

Other: _____

_____

_____

Recovery Team – Roles & Responsibilities

Title	Position	Responsibilities
Disaster Recovery Coordinator	*Director of IT *IS Leader *Security Officer *Administer	See Disaster Recovery Coordinator Position Description/Job Action Sheet
Operations Recovery Coordinator	*IT leader or Technical Support Person	Implement IT disaster recovery processes; facilitate recovery of IT operations as directed by DRC.
Network Recovery Coordinator	*Local or Enterprise Network Administrator	Implement IT disaster recovery processes; facilitate recovery of organization/enterprise network as directed by DRC
Communication Coordinator	*Director of PR	In conjunction with the DRC and Administration, develop and authorize communications with news media or public regarding disaster
Administrative Leader	*Director *Other Leadership Team Member	Support DRC/activities Investigate insurance coverage and resources Facilitate securing critical resources Investigate legal issues
Administrative Assistant		Provide necessary administrative and clerical support to DRC and support teams.

Other IT Disaster Recovery Support Teams

The DRC may determine the need to establish additional support teams based on the circumstances of the IT disaster. Additional teams which may be created include, but are not limited to:

- Administrative Support Team
- Telecommunications Team
- Applications Team
- Recovery Site Operations Teams
- Restorations & Salvage Team

Recovery Priorities

System Criticality Assessment & Priorities

Critically levels are assigned to application systems based upon the relative importance of the applications and systems to the organization's mission and operations. During the disaster recovery process, resources will be allocated based on established critically levels, unless otherwise determined by the DRC and/or administrative leadership. The organization must in advance review all applications, systems, networks, and critical interfaces and assign then to one of the following priority levels:

Critical/Priority 1

Applications and systems designated 'Critical" are mission-critical, impact key operations, and require immediate data recovery resources to ensure prompt restoration, recovery, and operability. Failure of these applications and systems to function for even a short period of time could have a severe impact on the organization's ability to carry out its mission and operations.

Recovery Time Objective (RTO): 0-8 Hours.

Essential/Priority 2

Applications and systems designated as "Essential" and may impact key operations, finance, services, and physical security. Failure of these applications and systems is allowable for a short period of time.

RTO: 9-24 Hours.

Necessary/Priority 3

Applications and systems designated "Necessary" and may tolerate a short period of availability.

RTO: 25-72 Hours.

Desirable/Priority 4

Applications and systems designated "Desirable" are lower priority and may tolerate a significant loss of availability. Recovery will be initiated when normal IT operations are re-established.

RTO: >72 Hours..

Information System Criticality Assessment Sheet:

Local Application/System/Network/ Interface	**Critical Priority 1 RTO: 0-8 Hours**	**Essential Priority 2 RTO: 9-24 Hours**	**Necessary Priority 3 RTO: 25-72**
External		E-Mail	
Communications	Network Access Phone Access		
Financial	Angela		
Human Resources		Time and Attendance	
Enterprise Applications/ System	**Critical Priority 1 RTO: 0-8 Hours**	**Essential Priority 2 RTO: 9-24 Hours**	**Necessary Priority 3 RTO: 25-72**
Millennium	X		
Active Directory	X		
DHCP	X		
File Server		X	
DNS	X		
Symantec (EndPoint)			X
EnvisionWare			X
TeleRenewal			X
DeepFreeze			X
Back-up Exec		X	
Print Server		X	
Hyena Software			X

Recovery Processes and Procedures

1. Upon assessment of damage and activation of disaster recovery processes, the IT leadership will determine the appropriate data recovery strategy
2. The data recovery processes shall reflect the organizations information systems priorities. Data recovery activities shall take place in a pre-planned sequential fashion so that system components can be restored in a logical manner and should take into consideration:
    A. Personnel: The IT leadership and workforce members involved in data recovery processes will be the most valuable resource. These individuals may be asked to work at great personal sacrifice and resources shall be provided to meet their personal and professional needs.
    B. Communications: Notifications of internal and external business partners associated with the organizations information systems.
    C. Salvage of Existing IT Equipment and Systems: Initial data recovery efforts shall be targeted at protecting and preserving the current media, equipment, applications and systems. A priority shall be to identify and obtain storage media. The IT equipment shall be further protected from the elements or removed to a safe location, away from the disaster site if necessary (Alternative Sites).
    D. Designate Recovery Site: It will be necessary to determine if the data recovery efforts can be carried out at the original primary site or moved to another location (see Command Recovery Center Alternative Site section). The choice of using an internal or a remote site will be dependent on the damage and estimated recovery of the computing and networking capabilities.
    E. Backup/New Equipment: The recovery process will rely heavily on the ability of the organizations vendors to quickly provide replacements for the resources which cannot be salvaged. Emergency procurement processes will be implemented to allow the IT leadership to quickly replace equipment, supplies, software and any other items required for data recovery.
    F. Reassembly Process: Salvaged and new data recovery equipment and components shall be reassembled at the recovery site to begin data recovery process.
    G. Restoration of Data from Back-ups: Data recovery will rely on the availability of the backup data from the storage site. Initial data recovery efforts will focus of restoring the operating systems by pre-determined priority (see Amendment A).
    H. Restoration of Application Data: IT leadership will work with the individual departments/application owners to restore each running application. As a period of time may have elapsed between the time that the backups were made and the time of the disaster requiring data recovery, the application owners must address mechanisms to capture and restore the lost interim data.
    I. Move Back to Restored Permanent Site: If the data recovery process has taken place at an alternative site, the equipment and systems that have been assembled at the alternative site will need to be returned to the original site when available.

3. Upon termination of recovery activities and once normal IT operations are back in place, than reconstitution efforts should begin. If the original site is unrecoverable (e.g., burned in fire), then the reconstruction activities may be applied to preparing a new site to support information systems requirements. Reconstitution activities should address:
    A. Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, office equipment and supplies
    B. Installing system hardware and software
    C. Establishing connectivity and interfaces with network components and external systems.
    D. Testing system operations to ensure full functionality
    E. Backing up operational data on the contingency system and uploading to restored system
    F. Shutting down the contingency system
    G. Terminating the contingency operations
    H. Removing and/or locating all sensitive material at the contingency site
    I. Arranging for contingency staff to return to the original/new facility

Data Back-up Procedures

Data backup processes shall be established through existing policy and procedures. The IT Department is responsible for overseeing organizational data backup and recovery processes for those applications, systems, and networks under its control. Users of unique departmental and/or individual applications, systems, and networks will be responsible for data backup and recovery unless arrangements have been made in advance with the IT department.

Review and Testing of Disaster Recovery Plan

The DRP should be reviewed on an annual basis or as often as necessary to ensure that the information contained in the plan is up-to-date and reflects current workforce information (titles, names, and contact information), application/systems, vendors, and other external contacts information. Additionally, after each disaster incident, whether a planned drill or actual disaster, the plan should be reviewed and revised to address practical application issues.

Disaster Recovery/Security Incident Response Team

Position/Department	Name	Extension	After Hours Contact Information
Library Director			
Deputy Director			
IT Manager			
IT Specialist			