* School District Information Technology
Disaster Recovery Plan

sa

* School District
Information Technology Department
May 2022

Definition of an Information Technology Disaster

There are many potential causes for an information technology disaster, requiring a response to the loss of services. The Information Technology Disaster Recovery Plan is designed to be used to guide the recovery process of critical information technology services to the District. Below are examples of potential causes for an information technology disaster:

- *Fire*
- *Flood*
- *Power outage*
- *Theft of equipment*
- *Facility damage*
- *Terrorism*
- *Cyber Attack*

Objectives

- The principal objective of the disaster recovery (DRP) program is to develop, test and document a plan which will help * School District recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:
- To ensure that all disaster team members fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are efficient and cost-effective
- A formal risk assessment shall be undertaken to determine the requirements for the DRP.
- The DRP should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The DRP should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- The DRP is to be reviewed periodically (semi-annually) and kept up to date to take into account changing circumstances.
- A detailed list of all internal/external members to be notified during the disaster recovery process
- A plan to acquire hardware for rebuild of technology infrastructure

Scope

The * School District DRP Identifies the below categories for responding to a disaster to the District's information technology resources. The Business Services team will work with the Information Technology Department within these broad categories to prioritize the services needed to be restored.

- *Network Infrastructure*
- *Server Infrastructure*
- *Voice over IP (VoIP)*
- *Data Storage and Backup Systems*
- *Computing devices*
- *Information Systems and software applications*
- *Information Technology Documentation*

Disaster Assessment

The disaster assessment phase lasts from the inception of the disaster until all services impacted by the disaster have been restored.

Disaster Recovery Activation

Based on the disaster assessment, the IT DR team will work in conjunction with Business Services to determine if the loss of services represents a disaster, based on services lost, recourse needed, and the time constraints to restore services.

Alternate Site Location

Depending on the severity of the loss from a disaster, continuing some operations using an alternate location may be required. The District does not currently have an alternative location to function as a temporary MDF/Data Center. Depending on the types of services to be restored, the District may have to rely on replacement of damaged equipment, network connectivity and restoration of information system data from backup storage. Data and applications that are hosted may potentially remain accessible with minimal interruption of service.

Key Disaster Recovery Steps

The below steps are used to guide a disaster recovery process for the Incident Response Manager

- Notify The Chief of Business Operations and Development of the potential disaster
- Identify if the potential disaster constitutes a problem, event, or disaster. If the Chief of Business operations agrees to initiate disaster recovery, continue with these steps.
    - A disaster is any event involving critical technology or critical technology services that causes significant interruption to school district operations. Factors in determining a disaster include
        - Impact - how many individuals are affected
        - Urgency - the severity of the interruption
        - Duration - how long
- Notify the IT Disaster response team using the IT Disaster Communication Tree to initiate a response to the disaster recovery plan
- Perform an assessment of the loss of services
- Identify as appropriate any additional District departments, staff or outside agencies needed to be included in the disaster recovery process.
- Coordinate all communication with Business Operations for any communication outside of the disaster response team.
- Prioritize services to restore business continuity

- Determine what resources and support are needed to restore services
- Acquire the needed resources
- Restore services to a normal level of operation, based on the priorities to restore business continuity

Key Business Process Strategy for Recovery

The Disaster Recovery Plan Focuses on Key Business Processes essential to business Continuity. The strategy for each business process is based on current available resources for the District. Hosted services are not directly impacted, but access to cloud-based information systems may be impacted by a loss of locally based systems.

KEY BUSINESS PROCESS	RESTORATION STRATEGY
IT Operations and Help Desk Support	On Premise Restoration
Financial/HR Systems	On Premise Restoration
Timeclock	Hosted Application/Data Storage
Student Information System	Hosted Application/Data Storage
Document Storage	On Premise Restoration
Productivity and Communications Platform	No restoration required.
District Website	No restoration required
District Phone System	On Premise Restoration
Application Account Management	On Premise Restoration

DR Procedures for Leadership Team

Members of the Senior Leadership Team will keep a hard copy of the names and contact numbers of each employee in the departments. In addition, Senior Leadership team members will have an electronic/hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the Data Center is inaccessible, unusable, or destroyed.

Contact with Employees

Support Department directors will serve as the point of contact for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

Communication from the IT department outside of their immediate teams will flow through from employees, to their management, to the IT Director, to the Chief of Business Operations. The Chief of Business Operations will handle communication to other business units and maintain communications with the Director of Information Technology.

Recovery Time Objectives (RTO)

The Recovery Time Objectives reflect the estimated recovery times based on current configurations and operations. Here is a general overview of the RTO's.

In the event of a disaster, RTO's must be established, however, RTO's should be considered best-case estimates. In the event of a disaster, network servers that host information systems, data, appliances and virtual servers would have to be identified, purchased, shipped, installed, and configured before any software or data could be restored that resides on the District network infrastructure. The availability of the relevant equipment and shipping times could vary greatly depending on the timing and scope of the disaster. Systems that are hosted may greatly reduce the RTOs.

Recovery Point Objectives (RPO)

The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure. The RPO is expressed backward in time (that is, into the past) from the instant at which the failure occurs, and can be specified in seconds, minutes, hours, or days. It is an important consideration in disaster recovery planning (DRP).The recovery point objectives for hardware, software, access data and applications will vary, based on the circumstances of the disaster.

Version Information & Changes

Updated versions of this document are reviewed, updated and stored electronically, and in hard copy format. stored in multiple locations on and off premise and provided to the lead positions of the disaster recovery team and the office of the assistant superintendent for business services.

Information Technology Disaster Recovery Lead Positions

- IT DR Administrator – Director of Information Services and Technology
- Communication Lead – IT Department Fiscal Services Coordinator
- Data and Application Recovery Lead – Network Administrator
- Technical Support Lead – Help Desk Manager

Key System Categories

These categories have been identified as key areas to support District Business Continuity; depending on the nature of a disaster, specific staff have a lead role identifying the requirements for recovery of the category.

Key System Category	**Lead Staff**
IT Infrastructure – Network WAN, LAN, Internet connectivity	Network Administrator
VoIP (District phone system)	Network Administrator
System Infrastructure – servers, data backup and recovery	Network Administrator
Information Systems, Active Directory, Applications and Data	Network Administrator
Email and Cloud-Based Communication	Network Administrator
Technology support – End user devices, IT Documentation, User Accounts, Print Services	Help Desk Manager

Overview System Network Map

The * School District IT Infrastructure is comprised of the following,
There are 13 sites total, 9 schools and 4 support facilities.

These sites are connected by a private Fiber Optic Metro Ethernet (MOE) infrastructure supplied by Cox Communications.

Cox has a physical presence at each location as a point of termination for the MOE.

Cox has a second physical presence at DO North as a point of termination for the 2 gigabit fiber optic hand off for Internet access.

All sites connect to the District Office North for core server access and Internet access. The core server infrastructure is located in a secure data center with air conditioning.

Disaster Recovery Activity Reporting

On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.

The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.

- The report will also contain an assessment of the impact to normal business operations.
- The report will be given to the business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- The report will be provided to the Chief of Business Operations and Development.

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- All key events that occur during the disaster recovery phase must be recorded.
- An event log shall be maintained by the disaster recovery team leader.
- This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.

Event Log

The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

Description of Disaster:
Commencement Date:
Date/Time DR Team Mobilized:

Activities Undertaken by DR Team	Date and Time	Outcome	Follow-On Action Required

Disaster Recovery Team's Work Completed: <Date>
Event Log Passed to Business Recovery Team: <Date>

Disaster Recovery Plan Maintenance

The DRP will be updated yearly or any time a major system update or upgrade is performed. The Information Technology Disaster Recovery Team Lead will be responsible for updating the Disaster Recovery Plan document and ensure that the designated staff retain the updated version of the document.

Testing The Disaster Recovery Plan

* School District IT is committed to ensuring that this DRP is functional. The DRP is evaluated and revised in order to ensure the viability of the recovery plan. Testing the recovery plan can be done using a number of methodologies:

1) **Walkthroughs**- Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).
2) **Desktop Simulation -** A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing may be evaluated through this process.
3) **Parallel Testing**- A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.
4) **Full-Interruption Testing**- A full-interruption test activates the total DRP. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence with respect to previous DRP phases cannot be overstated.

Results from the different methodologies are documented and used to make changes to the Disaster Recovery Plan when appropriate.

Addendum List

Disaster Recovery Call Tree

Incident Response Manager Backup:		
Executive Leaders Backup:	**Legal Counsel** Backup:	**Information Technology** Backup:
Human Resources Backup:	**Communications** Backup:	**Risk Manager** Backup:
Documentation and Timeline Leader Backup:		**Department Data Officer** Backup:

The Trust Contact Information

- This section contained contact information from The Trust in the event of a cyber attack.

Key Vendor Contact Information

Vendor Company	System Name	Key Contact Name	Contact Phone	Contact Email

* School District Information Technology Disaster Recovery Plan

Key Vendor Contact Information

An up-to-date version of this document is maintained here: (link removed)

This section contained contact information for department leaders.