District Name

District Address

Information Technology (IT) DISASTER RECOVERY (DR) PLAN

The District Name Disaster Recovery Plan should be strictly controlled. District Name data includes private personnel and student data, proprietary designs, and communication information. The information in this plan is distributed only to District Name and BOCES Name / Regional Information Center (RIC) Name personnel with a “need to know” and with the understanding that they will hold this information confidential and will not disclose any information in this plan to third parties without the prior written consent of the Executive Management Team, or the filing by the third party of a binding non-disclosure statement that has been vetted by legal.

District Name

Updated on:

IT Disaster Recovery Plan

Purpose Statement

This document is to be utilized in the event of a significant disruption to the District' normal daily technical operations. This plan is meant to summarize processes and procedures to execute during and after a technical disruption or disaster; as well as, plans for recovering critical systems and other internal infrastructure back to its normal operational state. In the event of an actual emergency situation, modifications to the IT Disaster Recovery Plan, referred to in this document as the DR Plan, may need to be made in order to ensure physical safety of people, systems and data.

The DR Plan should be used in conjunction with the District's IT Business Continuity Plan to ensure that mitigation and recovery efforts align with the District's defined goals and mission.

The recovery of people, internal and external dependencies, and infrastructure that may not be directly related to technological recovery will be outlined in more depth and detail within the District's Emergency Response Plan.

Sources

IT Business Continuity Plan:

Emergency Response Plan:

Objectives

The primary objective of the DR Plan is to develop, test, and document a well-structured and detailed plan that can be executed and referenced when the District needs to recover quickly and effectively from an unforeseen technological disaster or emergency that may interrupt or completely shut down day-to-day functions.

Additional Objectives:

- The DR Plan shall cover all essential and critical infrastructure elements, systems, and networks in accordance with the IT Business Continuity Plan.
- Communicate and ensure that all employees fully understand their roles and responsibilities as it pertains to the DR Plan.
- Ensure that all operational policies are adhered to pertaining to all DR Planned activities and executed functions.
- A risk assessment shall be conducted periodically to determine if any changes to the existing DR Plan need to be made.
- The DR Plan will be periodically tested in simulated environments to ensure that it can be successfully implemented in emergency situations. This simulation will also ensure that all members of the IT Disaster Recovery Team understand their roles and responsibilities, as well as being able to execute required tasks accurately and timely.
- The DR Plan is to be kept up-to-date as internal and external environments change and evolve.
- Extending disaster recovery capabilities to include staff, vendors, and other stakeholders as necessary.
- The District’s complete DR Plan shall be reviewed yearly.

Scope

The District Name IT Disaster Recovery Plan is focused on recovery of core IT services. Business response, continuity, and crisis management needs to be outlined in separate plans.

This plan is NOT intended to outline all the steps or recovery procedures that the District may need to take in the event of a technological disruption or disaster.

This document is to be used as a tool to guide the IT Disaster Recovery Team, referred to in this document as a DR Team, through the detection, mitigation, recovery and resumption process to return the District back to its normal operational state.

Internal Contacts

Disaster Recovery Leader

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Director of Facilities

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Director of Information Technology

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Technical Contacts

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Communication Specialist

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Legal Counsel

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Additional District Contacts

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

External Contacts

Law Enforcement

Name:

Phone:

Name:

Phone:

Name:

Phone:

Name:

Phone:

Name:

Phone:

EMS & Fire Departments

Name:

Phone:

Name:

Phone:

Name:

Phone:

Name:

Phone:

Name:

Phone:

Power Provider

Name:
Phone:

Water Department

Name:
Phone:

Internet Service Provider (ISP)

Name:
Phone:
Email:

Phone System

Name:
Phone:
Email:

BOCES Name

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Regional Information Center (RIC) Name

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Insurance Information

Overview

Provide a brief explanation of the district’s insurance policies relevant to disaster recovery, including coverage for cyber incidents, natural disasters, and physical damage.

Types of Coverage

Property Insurance – Covers damage to buildings, infrastructure, and physical assets.

Cyber Liability Insurance – Covers data breaches, ransomware attacks, and legal costs related to cybersecurity incidents.

Business Interruption Insurance – Covers loss of income due to operational disruptions.

General Liability Insurance – Covers claims of injury or property damage from third parties.

Policy Details

Provider Name	Policy Number(s)	Coverage Limits	Exclusions

Contact Information for Insurance Representatives

Policy	Insurance agent or broker	Claims department contact	Emergency support numbers

Claims Process

Who is responsible for initiating the claim (e.g., district finance officer, superintendent)
Required documentation (incident reports, financial loss estimates, etc.)
Timelines for filing claims and receiving reimbursements

Annual Review

Updates

Responsible party (parties) for updating insurance details in the Disaster Recovery Plan.

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Name:	
Work Phone:	Primary Email:
Mobile Phone:	Alternative Email:

Disaster Recovery Plan Overview

Disaster Recovery Team

Every person who is identified on the IT Disaster Recovery Team should have a clear understanding of their roles and responsibilities as it pertains to the DR Plan. Within this section, a Disaster Recovery Leader is identified. This person is responsible for ensuring that all team members are fulfilling their roles and responsibilities as it pertains to the plan in an effective and timely manner. Each person should have a clear, defined role within the DR Plan.

Title	Name	Phone Numbers
Disaster Recovery Leader		Mobile:
		Work:
District Access Control		Mobile:
		Work:
District Technology Leader		Mobile:
		Work:
Technology Support Staff		Mobile:
		Work:
Facilities (Buildings & Grounds)		Mobile:
		Work:
Business Office Representative		Mobile:
		Work:
Communication Specialist		Mobile:
		Work:
		Mobile:
		Work:
		Mobile:
		Work:
		Mobile:
		Work:
		Mobile:
		Work:

**Roles and responsibilities for DR team members are outlined on the following page.*

DR Team Roles & Responsibilities

Disaster Recovery Leader: The DR Leader should be the first notified of a detected event. It is their responsibility to determine if and when the DR Plan is to be initiated. Once the DR Plan has been activated, the DR Leader is responsible for notifying all DR Team members. Throughout the identification, mitigation, and recovery process, the DR Leader will be checking in with each team member to ensure that they are adhering to the plan and performing their tasks in an effective, efficient, and timely manner.

District Access Control: The District Access Control representative is responsible for granting or disabling virtual access to any and all systems as needed throughout the DR process.

District Technology Leader: The District Technology Leader will be the main contact for the DR Leader as it pertains to any technology related incidents or disasters. The Technology Leader is also responsible for overseeing the work of the Technology Support Staff as they isolate, mitigate, and recover from any technology disaster. This individual is also responsible for reviewing all of the recovery logs as it pertains to technology changes or modifications.

Technology Support Staff: IT staff are responsible for executing and logging all technology related support that is directed to them by the District Technology Leader. Throughout the isolation, mitigation, and recovery process, these individuals are to report all findings to the District Technology Leader. Any action taken that falls outside of a documented process or procedure must first be discussed and approved with the District Technology Leader prior to execution.

Facilities (Buildings & Grounds): The Facilities representative may be utilized to gain or deny physical access to District buildings as needed throughout the DR process and to liaise with utilities and any third parties necessary to provide any required power, cooling, or other physical infrastructure support.

Business Office Representative: The Business Office Representative will assist in expediting any procurement necessary for recovery, and may need to provide guidance in determining financial values related to physical loss. This individual may need to work with the DR Leader during the recovery process for insurance purposes in order to develop a cohesive list of assets in need of replacement.

Communication Specialist: The Communication Specialist should be the ONLY person (besides the Superintendent) releasing any information pertaining to the event to internal or external stakeholders. This individual(s) will work directly with the DR Leader in order to correlate when and what information will be released to which recipient groups (students, parents/guardians, internal stakeholders, external stakeholders, media, and/or social media).

Alternative Site

The District has an alternative off site location designated and available in the event that the District is displaced due to a disaster. This location is deemed a temporary, secure off site location to be utilized to perform required or needed Districts tasks during the time that our permanent site is inaccessible or unusable.

Alternative Site Location:

Title:

Street
Address:

Phone:

Minimal Equipment Listing

The list below specifies the quantities and types of equipment that will need to be available at the Alternative Site in order for the District to return to minimal / sustainable function.

Equipment Type	Quantity

Plan Updating

This plan should be updated by the responsible parties as needed. Reasons to update this plan should include (but are not limited to) the following scenarios:

- Response to non-major events such as office moves, telephone number changes, personnel changes on the functional teams, job duty changes on the response teams, and additions or deletions of participating applications;
- After each response test to reflect any of the recommendations that result from the post-test debrief;
- Any major system update, upgrade, addition, or removal is performed
- After a yearly review of the plan.

Additionally, the plan will be updated should an actual disaster occur. The plan will be reviewed and updated at a convenient point after the initial responses to the disaster have been completed.

Plan Documentation Storage

Copies of this response plan should be stored at the designated command center, as well as the assigned secondary and tertiary facilities that will be used in the event of the command center being unavailable.

Additional copies of this plan can be found at the following locations:

Location	Address	Contact Person

In the event that copies of this plan are no longer needed at any designated location, the plan should be returned to the following contact person:

Name:
Email:
Phone:
Location:

Prevention

The District has made a good-faith effort to ensure that current safeguards are in place to prevent or mitigate the impact of a disaster as it pertains to the District's most critical systems.

The following steps have been implemented for such purposes:

- All servers are centrally located and secured in locked locations to limit access from District staff. The following individuals have physical access to the server room:

- Each critical system has a short-term battery backup that will sustain operations during a power outage for a minimal period of time.
- All servers require an admin-level username and password to access them; logins are limited to the following individuals:

- A maintenance plan is maintained and executed by Information and Instructional Technology Staff to ensure that software upgrades and regular maintenance is conducted on the servers, systems, and workstations to enhance security.

Risk Management

The District has identified areas of risk within our current network environment through the use of a Risk Register.

Within the table below, the District will identify and rate the potential risk of an environmental disaster or unforeseen event. Each event will be listed and rated on the probability and potential impact it will have on the District's day to day operations. This table will also notate current mitigating controls that are in place to reduce the impact of a disaster or unforeseen event.

Probability Rating: Rare, Unlikely, Possible, Probable or Almost Certain
Impact Rating: Insignificant, Small, Moderate, Large or Severe

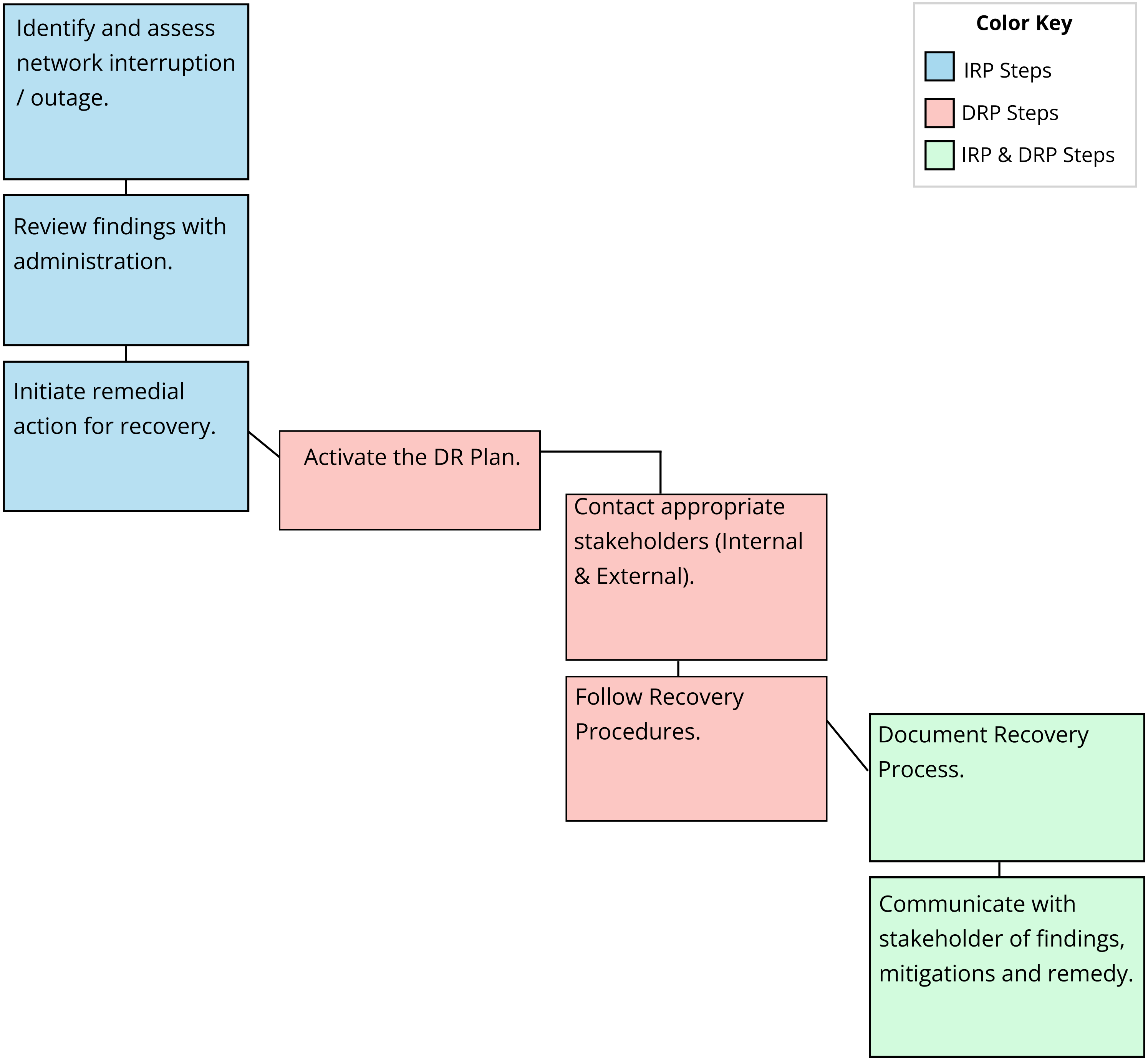
Potential Disaster	Probability Rating	Impact Rating	Current Protection
Flood	Rare	Insignificant	
Fire	Rare	Insignificant	
Electrical Storm	Rare	Insignificant	
Ice Storm	Rare	Insignificant	
Act of Sabotage	Rare	Insignificant	
Electrical / Power Failure	Rare	Insignificant	
Loss of Network Services	Rare	Insignificant	

Potential Disaster	Probability Rating	Impact Rating	Current Protection
Construction	Rare	Insignificant	
Tornado	Rare	Insignificant	
Hurricane	Rare	Insignificant	
	Rare	Insignificant	
	Rare	Insignificant	
	Rare	Insignificant	
	Rare	Insignificant	
	Rare	Insignificant	
	Rare	Insignificant	
	Rare	Insignificant	

Emergency Response

Alert, Escalation and Disaster Recovery Plan Activation

The person discovering the incident or event is responsible for reporting their initial findings to their supervisor. See table on the next page for more detail



Identify and assess network interruption / outage.

Review findings with administration.

Initiate remedial action for recovery.

Activate the DR Plan.

Contact appropriate stakeholders (Internal & External).

Follow Recovery Procedures.

Document Recovery Process.

Communicate with stakeholder of findings, mitigations and remedy.

Color Key

🟦 IRP Steps

🟥 DRP Steps

🟩 IRP & DRP Steps

Identification Phase

Step	Key Personnel	Components
Identify and assess network interruption / outage.		
Review findings with administration.		
Initiate remedial action for recovery.		

Response Phase

Step	Key Personnel	Components
Activate the DR Plan		
Contact appropriate stakeholders (Internal & External)		
Follow Recovery Procedures		

IRP & DRP Steps

Step	Key Personnel	Components
Document Recovery Process		
Communicate with stakeholder of findings, mitigations and remedy.		

Definitions

Application Programming Interface (API): A set of rules and protocols that allow different software applications to communicate with each other. It defines how requests and responses should be structured, enabling developers to integrate services, exchange data, and automate processes. It is frequently used in integrations between the SIS and other applications.

Domain Controller: A server in a Microsoft Windows Active Directory network that manages authentication, authorization, and security policies for users and computers. It stores and enforces directory data, such as user accounts, passwords, and group policies, allowing centralized management of network resources. It handles logins, permissions, and security protocols in order to ensure secure access to the network.

Dynamic Host Configuration Protocol (DHCP): A network protocol used to automate the assignment of IP addresses and other network settings to devices on a network. It eliminates the need for manual configuration by dynamically assigning IP addresses from a predefined pool.

File Server: A specialized server that manages and provides access to files for multiple users within a network. It allows users to store, retrieve, and share files.

Internet Protocol (IP) Address: A unique numerical identifier assigned to a device on a network, allowing it to communicate with other devices over the internet or a local network.

Local Area Network (LAN): A network of interconnected computers and devices within the school district. LANs enable users to share resources like files, printers, and internet connections efficiently. They typically use ethernet cables, Wi-Fi, or both for communication and operate at high speeds. LANs are managed using networking devices like switches, routers, and access points and are fundamental for internal communication in organizations.

Recovery Point Objective (RPO): A statement defining the data loss expectation caused by a disaster based on backup schedules, etc.

Recovery Time Objective (RTO): The period of time within which systems, applications, or functions can be recovered after an outage (e.g. one business day). RTOs are often used as the basis for the development of recovery strategies and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

Structured Query Language (SQL): SQL is a programming language used to manage and manipulate relational databases. It allows users to store, retrieve, update, and delete data efficiently. It supports powerful features like filtering, sorting, joins, and transactions, making it essential for data management and analysis. It is frequently used in integrations between the SIS and other applications.

Student Information System (SIS): A software application designed to manage and store student-related data for educational institutions. It helps schools track enrollment, attendance, grades, schedules, transcripts, and other academic records.

Wide Area Network (WAN): A network that connects computers and devices over a large geographic area, such as cities, countries, or even globally. WANs enable organizations, and individuals to communicate and share data across long distances. They typically use public or private communication links, including fiber optics, satellites, leased lines, and the internet. The internet itself is the largest example of a WAN. WANs are commonly used by educational institutions to connect multiple locations securely.

Backups and Locations

The District backs up critical data and tests recovery on a regular basis to ensure data viability. This section of the DR Plan identifies how often data is backed up and where these backups are located for restoration purposes.

Critical System	Backup Strategy	Dependencies
File Servers		
Domain Controllers		
Email		

Backups and Locations

Critical System	Backup Strategy	Dependencies
Student Information Systems (SIS)		
Cafeteria		
Special Education		

Backups and Locations

Critical System	Backup Strategy	Dependencies
Transportation		
Financial		
Local Area Network (LAN)		

Backups and Locations

Critical System	Backup Strategy	Dependencies

Order of Restoration

Order of Restoration is a prioritized listing of what systems to bring back online in order to return to a normal functioning state. This may be subject to variables such as time of year, etc. Utilize the chart below to create your District's Order of Restoration. Please keep in mind that systems may be dependent on others to function, and priorities will likely need to start with networking, identity, followed by applications.

Rank	Critical System	Notes	Complete
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□
9			□
10			□
11			□
12			□

Appendix

Application & Process Impact Analysis

Use the table below, one for each application or process, in order to evaluate the impact of an outage.

Application or Process Name:		
The loss of this application process would have the following effect on the district		
□ Catastrophic	□ Moderate	□ Minor

Comments:

How long can the School District perform without this application				
Check only one.	□ Up to 3 days	□ Up to 1 week	□ Up to 1 month	□ Other:

Comments:

Does this application or process have peak operational periods?	□ Yes	□ No

If yes, identify peak periods for this application or process:

Days:

Weeks:

Months:

Have you developed/established workaround procedures (manual or otherwise) to continue operations in the event the application or process is unavailable?	□ Yes	□ No

If yes, please explain the workaround procedure in place:

Application or Process Restoration Procedures

Technical Contact - person who handles the technical support / hosting for application

Name	Phone	Email

Application Contact - person who handles the user side of the application

Name	Phone	Email

Recovery Point Objective:

Recovery Time Objective:

Restoration Procedures:

To add next application / process click "Add Application" button
*Note: button will not appear on final printed plan

Add Application