**\_\_\_\_\_\_\_\_\_\_\_\_\_\_ School District**

**Information Technology (IT) Disaster Recovery Plan**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| revision | date | name | description |
| Draft 1.0 |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

Information Technology Statement of Intent………………………………………………………….. 1

Policy Statement…………………………………………………………………………………………. 1

Objectives…………………………………………………………………………………………………. 1

Key Personnel Contact Information……………………………………………………………………. 2

External Contacts………………………………………………………………………………. 3

1. Plan Overview…………………………………………………………………………………... 4

1.1 Plan Updating…………………………………………………………………………. 4

1.2 Plan Documentation Storage………………………………………………………… 4

1.3 Prevention…….……………………………………………………………………….. 4

1.4 Back-up Strategy……………………………………………………………………… 4

1.5 Risk Management……………………………………………………………………. 5

2. Emergency Response…………………………………………………………………………. 5

2.1 Alert, Escalation and Plan Invocation………………………………………………. 5

2.1.1 Plan Triggering Events……………………………………………………… 5

2.1.2 Assembly Points…………………………………………………………….. 5

2.1.3 Plan Invocation………………………………..…………………………….. 5

2.2 IT Disaster Recovery Team………………………………………………………….. 6

2.3 Emergency Alert, Escalation and IT Disaster Recovery Plan Activation………….. 6

2.3.1 Emergency Alert……………………………………………………………. 6

2.3.2 Disaster Recovery Procedures for Management ………………………. 6

2.3.3 Contact with Employees …………………………………………………… 6

2.3.4 Backup Staff………………………………………………………………… 6

2.3.5 Personnel and Family Notification………………………………………… 6

3. Media……………………………………………………………………………………………. 6

3.1 Media Contact………………………………………………………………………… 6

3.2 Media Strategies……………………………………………………………………… 6-7

3.3 Rules for Dealing with Media……………………………………………………….. 7

4. Insurance……………………………………………………………………………………….. 7

5. Financial and Legal Issues……………………………………………………………………. 7

5.1 Financial Assessment………………………………………………………………… 7

5.2 Financial Requirements……………………………………………………………… 7

5.3 Legal Actions………………………………………………………………………….. 7

6. IT Disaster Recovery Plan Exercising……………………………………………………..… 7

7. IT Disaster Recovery Kit & Supplies………………………………………………………….. 8

8. Annual Review…………………………………………………………………………………. 8

Appendix A – Information Technology Disaster Recovery Plan Templates……….…….. 9

IT Disaster Recovery Plan for System One……………………………………….... 9-10

IT Disaster Recovery Plan for System Two………………………………………… 11

IT Disaster Recovery Plan for Wide Area Network (WAN)……………………….. 12

IT Disaster Recovery Plan for Voice Communications…………………………… 12

Appendix B – Suggested Forms……………………………………………………………… 13

Damage Assessment Form…………………………………………………………. 13

Management of IT Disaster Recovery Activities Form…………………………… 13 IT Disaster Recovery Event Recording Form………………..……………………. 13-14

IT Disaster Recovery Activity Report Form………………………………………… 14

Mobilizing the IT Disaster Recovery Team Form………………………………….. 14

Communications Form………………………………………………………………. 14-15 Returning Recovered Operations to Unit Leadership……………..……………… 15

**Information Technology Statement of Intent**

This document delineates the \_\_\_\_\_\_\_\_\_\_\_ School District’s (referred to as the “District”) policies and procedures for an Information Technology Disaster Recovery Plan (referred to as “IT Disaster Recovery Plan”), as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of people, systems, and data.

Our mission is to ensure information system operation, data integrity and availability, and business continuity.

# **Policy Statement**

Management has approved the following policy statement:

* The District’s comprehensive IT Disaster Recovery Plan shall be reviewed annually.
* A risk assessment shall be undertaken periodically to determine the requirements for the IT Disaster Recovery Plan.
* The IT Disaster Recovery Plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key educational activities.
* The IT Disaster Recovery Plan 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.
* Staff must be made aware of the IT Disaster Recovery Plan and their own respective roles.
* The IT Disaster Recovery Plan is to be kept up to date to take into account changing circumstances.

# 

# **Objectives**

The principal objective of the IT Disaster Recovery Plan program is to develop, test and document a well-structured and easily understood plan which will help the District recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and educational operations. Additional objectives include the following:

* The need to ensure that employees 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 cost-effective.
* Disaster recovery capabilities are applicable to staff, vendors and others.

1

**KEY PERSONNEL CONTACT INFORMATION**

| **NAME AND TITLE** | **CONTACT OPTION** | **CONTACT NUMBER** |
| --- | --- | --- |
| **Superintendent of Schools** | Work |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  |  |  |
|  |  |  |
| **Business Administrator** | Work |  |
|  | Alternate (Pager) |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  |  |  |
|  |  |  |
| **Network & Systems Technician** | Work |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  |  |  |
|  |  |  |
| **Supt. of Buildings & Grounds** | Work |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  |  |  |
|  |  |  |
| **Transportation Supervisor** | Work |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  |  |  |
|  |  |  |

2

**EXTERNAL CONTACTS**

| **NAME AND CONTACT** | **CONTACT OPTION** | **CONTACT NUMBER(S)** |
| --- | --- | --- |
| **Power Company** |  |  |
|  | Power Outage |  |
|  | Natural Gas |  |
|  |  |  |
| **Telecom Carrier 1** |  |  |
|  | Work |  |
|  | Fax |  |
|  |  |  |
| **Telecom Carrier 2** |  |  |
|  | Work |  |
|  | Email Address |  |
|  |  |  |
| **Insurance** |  |  |
|  | Work |  |
|  | Email Address |  |
|  |  |  |
| **Fire Security** |  |  |
|  | Work |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  |  |  |
| **HVAC** |  |  |
|  | Work |  |
|  | Mobile |  |
|  | Email Address |  |
|  |  |  |
| **Power Generator** |  |  |
|  | Work |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  |  |  |
| **Other** |  |  |
|  | Work |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |

3

# **1. Plan Overview**

## **1.1 Plan Updating**

It is necessary for the IT Disaster Recovery Plan updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the Technology Department.

## **1.2 Plan Documentation Storage**

Copies of this Plan and hard copies will be stored in secure locations to be defined by the district. Each member of the IT Disaster Recovery Team will be issued a hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

**1.3 Prevention**

All attempts are made to prevent or limit the impact of a disaster on the information systems of our District. Specifically, the following steps have been taken:

* All servers are in a centralized and secured, locked location with access limited to technology staff and selected buildings and grounds staff.
* A separate independent cooling system is installed in the server room.
* All servers are password protected, with only select administrator level user accounts given authorization to log on.
* Uninterrupted power supplies are installed on all servers and key network equipment.
* RAID is used on mission critical servers.

## **1.4 Backup Strategy**

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for a fully mirrored recovery site at the District Office. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site and the backup site.

|  |  |
| --- | --- |
| **KEY BUSINESS PROCESS** | **BACKUP STRATEGY** |
| Technology Operations | Fully mirrored recovery site |
| Facilities Management | Fully mirrored recovery site |
| Email | Fully mirrored recovery site |
| Disaster Recovery | Fully mirrored recovery site |
| Student Management | Off-site data storage facility (NERIC) |
| Finance & Human Resources | Off-site data storage facility (NERIC) |
| Special Education | Off-site data storage facility (NERIC) |
| Testing Fully Mirrored Recovery site | Fully mirrored recovery site |
| Library Automation System | Fully mirrored recovery site |
| School Lunch & Transportation Routing | Fully mirrored recovery site |
|  |  |
|  |  |
| Student Data Files |  |
| Employee Data Files |  |
|  |  |

## 

4

## **1.5 Risk Management**

There are many potential disruptive threats which can occur at any time and affect the normal educational process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of educational disruption which could arise from each type of disaster. Potential disasters have been assessed as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Potential Disaster** | **Probability Rating** | **Impact Rating** | **Brief Description Of Potential Consequences & Remedial Actions** |
| Flood | 3 | 4 |  |
| Fire | 3 | 4 | Fire and smoke detectors on all floors. |
| Tornado | 5 |  |  |
| Electrical storms | 3 |  |  |
| Ice Storm | 3 | 4 |  |
| Act of terrorism | 5 |  |  |
| Act of sabotage | 5 |  |  |
| Electrical power  Failure | 3 | 3 | UPS array tested weekly & remotely monitored 24/7. |
| Loss of communications network services | 4 | 4 |  |

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

# 

# **2. Emergency Response**

## **2.1 Alert, escalation and plan invocation**

### 2.1.1 Plan Triggering Events

Key trigger issues that would lead to activation of the IT Disaster Recovery Plan are:

* Total loss of all communications
* Total loss of power
* Flooding of the premises
* Loss of the building

### 2.1.2 Assembly Points

When the premises need to be evacuated, please refer to the Emergency Evacuation Plan (see attached).

### 2.1.3 Plan Invocation

When an incident occurs, the IT Disaster Recovery Plan may be implemented. All key employees must be issued a digital contact solution to be used in the event of a disaster. Responsibilities are:

* Respond immediately to a potential disaster and call emergency services;
* Assess the extent of the disaster and its impact on the district;
* Decide which elements of the disaster recovery plan should be activated;
* Establish and manage disaster recovery team to maintain vital services and return to normal operation;
* Ensure employees are notified and allocate responsibilities and activities as required.

5

**2.2 IT Disaster Recovery Team**

Team members include:

The team's responsibilities include:

* Establish facilities for an emergency level of service within 1 business day;
* Restore key services within 1 business day of the incident;
* Return to business as usual within 1 business day after the incident (depending upon incident);
* Coordinate activities with disaster recovery team, first responders, etc.

## **2.3 Emergency Alert, Escalation and IT Disaster Recovery Plan Activation**

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The IT Disaster Recovery Plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology.

### 2.3.1 Emergency Alert

### The person discovering the incident calls their immediate supervisor. One of the tasks during the early stages of the emergency is to notify the IT Disaster Recovery Team that an emergency has occurred. The notification will request IT Disaster Recovery Team members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated.

### 2.3.2 IT Disaster Recovery Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the District’s IT Disaster Recovery Plan on file in their homes in the event that the building is inaccessible, unusable, or destroyed.

**2.3.3** **Contact with Employees**

### Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the district’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. Other communication methods: radio, television, email.

### 2.3.4 Backup Staff

### If an administrator, supervisor or staff member designated to contact other staff members is unavailable, the designated backup staff member will perform notification duties.

### 2.3.5 Personnel and Family Notification

### If the incident has resulted in a situation which would cause concern to an employee’s immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

# **3. Media**

## **3.1 Media Contact**

The President of the Board of Education, the Superintendent of Schools, or designee, will coordinate with the media, working according to Board Policy # (see attached).

## **3.2 Media Strategies**

a. Avoiding adverse publicity

b. Take advantage of opportunities for useful publicity

6

c. Have answers to the following basic questions:

* What happened?
* How did it happen?
* What are you going to do about it?

## **3.3 Rules for Dealing with Media**

## Onlythe person(s) listed in Section 3.1 above is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the individual(s) listed.

# 

# **4. Insurance**

# As part of the district’s disaster recovery strategy, a number of insurance policies have been put in place. These include errors and omissions, School District Educators Legal Liability, general liability, and business interruption insurance.

Amount of Coverage Person Responsible Next

Coverage Type: Coverage: Period: For Coverage: Renewal Date:

# **5. Financial and Legal Issues**

## **5.1 Financial Assessment**

## The IT Disaster Recovery Team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

* Loss of financial documents
* Loss of cash

## 

## **5.2 Financial Requirements**

## The immediate financial needs of the District must be addressed. These can include:

## Cash flow position

* Temporary borrowing capability
* Upcoming payments for payroll taxes, Social Security, etc.
* Availability of District credit cards to pay for supplies and services required post-disaster

## **5.3 Legal Actions**

## The District’s attorney and IT Disaster Recovery Team will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event.

# **6. IT Disaster Recovery Plan Exercising**

# IT Disaster Recovery Plan exercises are an essential part of the plan development process. In an IT Disaster Recovery Plan exercise, no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that the emergency team is familiar with the assignment and, more importantly, is confident in their capabilities.

# Successful IT Disaster Recovery Plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

# Upon completion of the exercises, amendments to this document may be determined necessary. Revisions to this document will be noted on the cover sheet of the IT Disaster Recovery Plan.

7

**7. IT Disaster Recovery Kit and Supplies**

An IT Disaster Recovery kit, including the following items, will be located at the District Office and the Senior High vault:

* Copy of the District’s IT Disaster Recovery Plan
* Copy of the telephone numbers and email addresses for all members of the IT Disaster Recovery Team.
* Copy of telephone numbers with extensions and email addresses for all \_\_\_\_\_\_\_ School District staff.

**8. Annual Review**

The District will review and update the IT Disaster Recovery Plan annually.

8

# **Appendix A**

# **IT Disaster Recovery Plan Templates**

## **IT Disaster Recovery Plan for <System One>**

|  |  |
| --- | --- |
| SYSTEM | Primary Site |
| OVERVIEW |  |
| SYSTEM SPECIFICATIONS |  |
| MORE INFO | Visio Diagram Attached |
| SECONDARY SITE |  |

9

|  |  |
| --- | --- |
| BACKUP STRATEGY FOR SYSTEM ONE |  |
| Daily |  |
| Monthly |  |

|  |  |
| --- | --- |
| **SYSTEM ONE** **IT DISASTER RECOVERY PROCEDURE** |  |
| Scenario 1  Total Loss of Data |  |
| Scenario 2  Total Loss of Hardware |  |

**ADDENDUM**

|  |  |
| --- | --- |
| **CONTACTS** |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

10

## **IT Disaster Recovery Plan for <System Two>**

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| OVERVIEW |  |
| PRODUCTION SERVER | Location:  Server Model:  Operating System:  CPUs:  Memory:  Total Disk:  System Handle:  System Serial #:  DNS Entry:  IP Address:  Other: |
| HOT SITE SERVER | Provide details |
| APPLICATIONS  (Use bold for Hot Site) |  |
| ASSOCIATED SERVERS |  |

|  |  |
| --- | --- |
| BACKUP STRATEGY for SYSTEM TWO |  |
| Daily | Provide details |
| Monthly | Provide details |
| Quarterly | Provide details |

|  |  |
| --- | --- |
| **SYSTEM TWO** **IT DISASTER RECOVERY PROCEDURE** |  |
| Scenario 1  Total Loss of Data | Provide details |
| Scenario 2  Total Loss of HW | Provide details |

**ADDENDUM**

|  |  |
| --- | --- |
| **CONTACTS** |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

11**IT Disaster Recovery Plan for Wide Area Network (WAN)**

**ADDENDUM**

|  |  |
| --- | --- |
| **CONTACTS** |  |
|  |  |
|  |  |
|  |  |
|  |  |

## **IT Disaster Recovery Plan for Voice Communications**

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| OVERVIEW |  |
| EQUIPMENT | Location:  Device Type:  Model No.:  Technical Specifications:  Network Interfaces:  Power Requirements;  System Serial #:  DNS Entry:  IP Address:  Other: |
| HOT SITE EQUIPMENT | Provide details |
| SPECIAL APPLICATIONS |  |
| ASSOCIATED DEVICES |  |

|  |  |
| --- | --- |
| BACKUP STRATEGY for SYSTEM TWO |  |
| Daily | Provide details |
| Monthly | Provide details |
| Quarterly | Provide details |

|  |  |
| --- | --- |
| **SYSTEM TWO** **IT DISASTER RECOVERY PROCEDURE** |  |
| Scenario 1  Total Loss of Switch | Provide details |
| Scenario 2  Total Loss of Network | Provide details |

**ADDENDUM**

|  |  |
| --- | --- |
| **CONTACTS** |  |
|  |  |
|  |  |
|  |  |
|  |  |

12

**Appendix B**

**Suggested Forms**

## 

## **Damage Assessment Form**

|  |  |  |
| --- | --- | --- |
| **Key Business**  **Process Affected** | **Description Of Problem** | **Extent Of Damage** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## **Management of IT Disaster Recovery Activities Form**

* During the IT Disaster Recovery Plan process, all activities will be determined using a standard structure;
* Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
* All actions that occur during this phase will need to be recorded.

|  |
| --- |
| **Activity Name:** |
| **Reference Number:** |
| **Brief Description:** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Commencement**  **Date/Time** | **Completion**  **Date/Time** | **Resources Involved** | **In Charge** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## **IT Disaster Recovery Event Recording Form**

* All key events that occur during the IT disaster recovery phase must be recorded.
* An event log shall be maintained by the IT Disaster Recovery Team leader.
* This event log should be started at the commencement of the emergency.
* The following event log should be completed by the IT Disaster Recovery Team leader to record all key events during disaster recovery.

|  |
| --- |
| **Description of Disaster:** |
| **Commencement Date:** |
| **Date/Time IT Disaster Recovery Team Mobilized:** |

13

|  |  |  |  |
| --- | --- | --- | --- |
| **Activities Undertaken by IT Disaster Recovery Team** | **Date and Time** | **Outcome** | **Follow-On Action Required** |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **IT Disaster Recovery Team's Work Completed:** <Date> |

## **IT Disaster Recovery Activity Report Form**

* On completion of the initial IT disaster recovery response, the IT Disaster Recovery Team 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 IT Disaster Recovery Team together with outcomes arising from those actions.
* The report will also contain an assessment of the impact to normal business operations.
* An IT Disaster Recovery Report will be prepared by the IT Disaster Recovery Team leader on completion of the initial IT disaster recovery response.

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 IT Disaster Recovery Team
* Outcomes arising from actions taken
* An assessment of the impact to normal business operations
* Lessons learned

## **Mobilizing the IT Disaster Recovery Team Form**

* Following an emergency requiring recovery of technology infrastructure assets, the IT Disaster Recovery Team should be notified of the situation and placed on standby.
* The format shown below can be used for recording the activation of the IT Disaster Recovery Team once the work of the damage assessment and emergency response teams has been completed.

|  |
| --- |
| **Description of Emergency:** |
| Date Occurred: |
| Date Work of IT Disaster Recovery Team Completed: |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name of Team Member** | **Contact Details** | **Contacted On (Time / Date)** | **By Whom** | **Response** | **Start Date Required** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Relevant Comments (e.g., Specific Instructions Issued) | | | | | |

## **Communications Form**

* It is very important during the IT disaster recovery activities that all affected persons and organizations are kept properly informed.
* The information given to all parties must be accurate and timely.
* In particular, any estimate of the timing to return to normal working operations should be announced with care.
* It is also very important that only authorized personnel deal with media queries.

14

|  |  |  |  |
| --- | --- | --- | --- |
| Groups of Persons or Organizations Affected by Disruption | Persons Selected To Coordinate Communications to Affected  Persons / Organizations | | |
| Name | Position | Contact Details |
| Parents |  |  |  |
| Management & Staff |  |  |  |
| Suppliers |  |  |  |
| Media |  |  |  |
| Board of Education |  |  |  |
| Others |  |  |  |

## **Returning Recovered Operations to Unit Leadership**

* Once normal operations have been restored, it will be necessary to return the responsibility for specific operations to the original department.
* This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to normal operations-as-usual

15