IT Disaster Recovery Plan
Procedure (IT-P032)

The online version of this procedure is official. Therefore, all printed versions of this document are unofficial copies.

1.0 SCOPE:

1.1 The Washoe County School District's Information Technology Department recognizes the need for a comprehensive disaster recovery plan in the event that an unexpected disaster should occur within our area. Our plan, with the following assumptions and components, will be quickly and efficiently implemented in order to prevent a severe disruption in services to our students and employees.

2.0 RESPONSIBILITY:

2.1 Chief Technology Officer

2.2 Assistant Chief Technology Officer

2.3 Technical Service Manager

2.4 Technical Service Supervisor

2.5 IT Security Officer

2.6 IT Application Supervisors

3.0 APPROVAL AUTHORITY:

(Approval signature on file)

_____ _____

Signature Date

3.1 Chief Technology Officer

4.0 DEFINITIONS:

4.1 **Data Duplication** - Sharing information between databases (or any other type of server) to ensure that the content is consistent between systems.

4.2 **Email Security** – The act of protecting email users from threats such as spam and phishing schemes.

4.3 **Web Security** - The act of protecting internet users from threats such as malicious websites, phishing attacks, key logging, spyware and viruses.

4.4 **Wide Area Network -** is a computer network that covers a broad area.

5.0 ASSUMPTIONS:

5.1 The disaster recovery plan only affects the Information Technology computer operations and does not consider systems outside of the department unless explicitly identified.

5.2 The Corporate Way facility will be the backup site should computer operations no longer be viable at the District Office.

5.3 The disaster recovery plan will be implemented in phases:

5.3.1 Phase One: Corporate Way's facility will provide partial data duplication capabilities with data that will be 12 to 24 hours old.

5.3.2 Phase Two (not funded): Provide near real-time data backup to duplicate processing capabilities.

5.3.3 Phase Three (not funded): Provide internet connectivity and email/web security to phase one and two capabilities.

5.3.4 Note that internet capabilities are critical for those applications that are hosted outside the District e.g. Aesop, Follett, Edline, Edusoft, VPN.

5.4 Recovery operations would break into two tiers; connectivity and infrastructure:

5.4.1 The first tier would be to ensure District sites have Wide Area Network connectivity to the Corporate Way site.

5.4.2 If the Wide Area Network fails due to problems outside the control of the District, the vendor will be responsible for reestablishing connectivity.

5.4.3 If the Wide Area Network fails due to problems within the District's control, IT has responsibility for reestablishing connectivity.

5.4.3.1 Once the necessary connectivity is reestablished then the focus will be on ensuring the infrastructure, hardware/software of the backup site, is operational.

5.4.4 In the event that of a disaster, a classroom at Corporate Way will be set aside for key personnel to use to connect to their application(s).

6.0 DUPLICATION AND STORAGE PROCEDURES

6.1 The following data records are needed in the event of a disaster:

6.1.1 BiTech (Business, HR, Risk Management, Purchasing)

6.1.2 SASI student Information

6.1.3 WinSnap

6.1.4 GIS Maps

6.1.4.1 The above critical applications will be running at the District's backup site in parallel to the District's main computer room.

6.1.5 The following applications are on the second tier to be brought up in the event of a disaster:

6.1.5.1 GroupWise

6.1.5.2 Document Management System

6.1.5.3 Internet

6.1.5.4 Emergency Management System

7.0 DATA RECOVERY STRATEGIES

7.1 If a disaster occurs, the Recovery Team will convene as quickly as possible and follow the outlines steps, as appropriate:

7.1.1 Contact the Emergency Management Team.

7.1.2 Verify that IT personnel are safe.

7.1.3 A command center will be chosen, according to the availability of pre-determined sites. .

7.1.4 Data retrieval needs will be determined.

7.1.5 As needed, appropriate data will be retrieved from the offsite location.

7.1.6 The platform (which includes hardware, operating environment and application to access data) will be recreated or copied.

7.1.7 Needed data will be uploaded into the newly copied or created platform.

7.1.8 A workspace environment for appropriate system end users will be set up so that needed data can be utilized and there will be as little disruption as possible in administrative services to the system's schools.

8.0 PLAN MAINTENANCE

8.1 The Disaster Recovery Team will convene annually to review and/or revise the above procedure. In addition, a test environment for data recovery verification will be created bi-annually, or more often if necessary, to insure that the backup procedures of the school system are functioning properly.

8.2 The Disaster Recovery Team will have the emergency generator tested for the data center on an annual basis during the summer months to not impact the District as much as testing during the school year.

9.0 ASSOCIATED DOCUMENTS:

9.1 Washoe County School District (WCSD) School Board Acceptable Use Policy, 6163.2

9.2 Washoe County School District IT Acceptable Use Procedure (IT-P002)

9.3 Remote Access Procedure (IT-P004)

9.4 Virtual Private Network (VPN) Procedure (IT-P005)

10.0 RECORD RETENTION TABLE:

Identification	Storage	Retention	Disposition	Protection

11.0 REVISION HISTORY:

Date:	Rev.	Description of Revision:
11/12/09	A	Initial Release

*** End of procedure ***