# Provo City School District Technology Security Policy

## Disaster Recovery Plan Procedure

**Last Update Status:** *Updated January 2015*

### 1. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives PCSD an advantage. This procedure requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters include, but are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

### 2. Purpose

This procedure defines the requirement for a baseline disaster recovery plan to be developed and implemented by PCSD that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

### 3. Scope

This procedure is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This procedure is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub plans.

### 4. Procedure

Contingency Plans
The following contingency plans must be created:

- **Computer Emergency Response Plan**: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- **Succession Plan**: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- **Data Study**: Detail the data stored on the systems, its criticality, and its confidentiality.
- **Criticality of Service List**: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- **Data Backup and Restoration Plan**: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- **Equipment Replacement Plan**: Describe what equipment is required to begin providing services, list the order in which it is necessary, and note where to purchase the equipment.
- **Mass Media Management**: Who is in charge of giving information to the mass media?

- **Critical Systems Instructions:** Documentation must include:
  - Location of installation software
  - Backup frequency and storage locations
  - Username and passwords
  - Support phone numbers
  - Steps to restart, reconfigure, and recover the system
  - Power up and power down procedures
  - Equipment age
  - Model and serial numbers
  - Warranty and maintenance contract information
  - Software licensing information and storage location
  - IP and MAC addresses
  - Supplier contacts for sources of expertise to recover systems. These might include vendors that sell/support the products, or the manufacturers themselves
  - Website username and password
  - Server username and password
  - District assigned computer username and password
  - Maps, diagrams, charts, etc.
  - Any username/password for any system where relevant information exists to recover systems (manufacturer website username and password, server passwords, call-in information, etc.)

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Tabletop exercises should be conducted quarterly. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, will be reviewed and updated on an annual basis.