<Company Name>
Computer Disaster Recovery Plan Policy

1.0 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 <Company Name> a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered.

2.0 Purpose

This policy defines the need for management to support ongoing disaster planning for <Company Name>.

3.0 Scope

This policy applies to the management and technical staff of <Company Name>.

4.0 Policy

4.1 Contingency Plans

The following contingency plans must be created:

1. **Computer Emergency Response Plan:** Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
2. **Succession Plan:** Describe the flow of responsibility when normal staff is unavailable to perform their duties.
3. **Data Study:** Detail the data stored on the systems, its criticality, and its confidentiality.
4. **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.
5. **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.
6. **Equipment Replacement Plan:** Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
7. **Mass Media Management:** Who is in charge of giving information to the mass media? Also provide some guidelines on what data is appropriate to be provided.

4.2 Plans must be Placed into Action

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 plan. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

4.3 Plans must be Updated

Review all plans annually so changes in the <Company>'s situation can be incorporated.

5.0 Enforcement

Any employee that violates this policy may be subject to disciplinary action up to and including termination of employment.

6.0 Definitions

Terms	**Definitions**
Disaster:	Any event that could likely cause serious disruption of the IT systems, including without limitation, weather events, power events, or acts of terrorism.

7.0 Revision History

Original 7/6/09 Robert Comella