1 Disaster Recovery Plan Policy

Last Update Status: *April 2020*

1. Overview

Since disasters happen so infrequently, 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 is likely to cause an extended delay of service should be considered.

Note that the Disaster Recovery Plan is often part of the Business Continuity Plan.

2. Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by <Company Name> 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 policy is directed to IT management staff accountable to ensuring the plan is developed, tested and kept up to date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirements around what goes into the plan or sub-plans.

4. Policy

4.1 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 services provided and their order of importance. The order of recovery should also be defined 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 to provide 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?
- *Appropriate Data:* Provide some guidelines on what data is appropriate to be provided.

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 annually. 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, should be reviewed and updated on an annual basis.

5. Policy Compliance

5.1 Compliance Measurement

The <Company Name> security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the <Company Name> security team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2 6. Related Standards, Policies and Processes

3 7. Revision History

4 Date of Change	5 Responsible	6 Summary of Change
7	8	9