“Your Company Name”
Disaster Recovery Plan/Policy

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 “Your 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. The Disaster Recovery Plan is 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 “Your 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 the IT Management Staff who is accountable to ensure the plan is developed, tested quarterly, and kept up to date. This policy 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. Policy

Contingency Plans
Computer Emergency Response Plan:

First points of contact if an emergency presents.

Name	Title	Mailing Address	Email Address	Phone Number	Cell Number

In the event of a system failure, hack or imminent threat to our data security, accessibility and continuity, contact the above immediately.

“Describe you backup plan here.”

Succession Plan: If “choice #1” is not available at the time of a significant emergency event. “second choice” may direct staff to create the necessary recovery states to restore full services.

Data Study: See definitions below in section 6.

Criticality of Service List: “your services here” Time to restore service access, 2 hours. Time to restore data 24 hours. (can be altered to fit your companies standards.)

Data Backup and Restoration Plan: “Describe your plan here.”

Media Management: “Senior Manager.” will notify relevant authorities, customers, vendors and media.

Frequency: The disaster recover plan must be tested and practiced once every quarter as close as possible to the beginning of that quarter. Jan-1, April-1, July-1, Oct-1. (can be modified to fit your company.)
.

5. Policy Compliance

Compliance Measurement

The Security Team or Data Governance committee will verify compliance to this policy through various methods, including but not limited to, periodic testing, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Data Governance Committee in advance.

Non-Compliance

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

6. Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text – Unencrypted data.

Hacker –a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s). The intent of learning these languages is to find and exploit vulnerabilities in computer systems.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

Protected data - See PII

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data - Data that is encrypted or in plain text and contains PII data.

5 Related Standards, Policies and Processes

(list your related policies here)

6 Revision History

Date of Change	Responsible	Summary of Change
July 1 2022		First Draft