DISASTER RECOVERY POLICY

The disaster recovery policy must be reviewed at least annually to assure its relevance. Just as in the development of such a policy, a planning team that consists of upper management, and personnel from information security, information technology, human resources, or other operations should be assembled to review the disaster policy. Roles and responsibilities of the planning team should be as follows:

- Perform an initial risk assessment to determine current information systems vulnerabilities.
- Perform an initial business impact analysis to document and understand the interdependencies among business processes and determine how the business would be affected by an information systems outage.
- Take an inventory of information systems assets such as computer hardware, software, applications, and data.
- Identify single points of failure within the information systems infrastructure.
- Identify critical applications, systems, and data.
- Prioritize key business functions.

Company personnel will carry out the following procedures in the implementation of a disaster recovery policy

- Setup and maintain offsite facilities for data backup storage and electronic vaulting as well as redundant and reliable standby systems if necessary.
- Ensure that critical applications, systems, and data are distributed among facilities that are reasonably easy to get to but not so close that they could be affected by the same disaster.
- Establish written policies, contracts, and service level agreements with third party hosting, collocation, telecommunications, and Internet service providers that facilitate prompt recovery and continuity.
- Create an incident response team that consists of information security, IT, marketing, HR, legal, and other relevant personnel.
- Define the roles and responsibilities of the incident response team.
- Obtain each incident response team member's contact information.
- Determine which methods the incident response team members will use to communicate in the event of a disaster.
- Create a public relations plan to assist with the effective handling of an incident.
- Assign a manager (such as an IT or Information Security Manager) that has the responsibility and authority to make critical IT decisions.
- Develop testing standards.
- Document and distribute the disaster recovery plan.
- Distribute copies of the written plans to everyone involved and also store extra copies in an offsite, fireproof vault.
- The following are ongoing procedures that must be followed:
- Continuously perform data backups, store at least weekly backups offsite, and test those backups regularly for data integrity and reliability.
- Test plans at least annually, document and review the results, and update the plans as needed.
- Analyze plans on an ongoing basis to ensure alignment with current business objectives and requirements.
- Provide security awareness and disaster recovery education for all team members involved.
- Continuously update information security policies and network diagrams.

- Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
- Perform continuous computer vulnerability assessments and audits.

Acknowledging Receipt of Disaster Recovery Policy

I have received my copy of the [COMPANY] Disaster Recovery Policy and I have read and I understand the information contained here in.

I further acknowledge my understanding that my employment with [COMPANY] may be terminated at any time with or without cause.

Note: The preceding sentence should be included only in states where termination at will is permitted and where the employer desires this status.

_____

Date

_____

Employee's Signature

_____

_____

Name [Please Print]