Disaster Recovery Policy Statement

This is the statement of general policy and arrangements for:

Grillatech Limited

Overall and final responsibility for disaster recovery:

Rick Dye

Grillatech is totally committed to the principles and practice of a business continuity and disaster recovery plan. Since they are aligned in the principle of keeping the business running in the event of an incident, this disaster recovery plan is referenced in the business continuity plan and vice-versa.

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realise that having a contingency plan to ensure recovery in the event of a disaster gives Grillatech a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts.

Incidents are not limited to adverse weather conditions or natural acts. Any event that could likely cause an extended delay of service should be considered.

1. Purpose

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

2. Scope

This policy is directed to the Management Staff who are accountable to ensure the plan is developed, tested and kept up to date. This policy is to state the requirement to have a disaster recovery plan and highlight the main contingencies within the plan, it does not provide requirement around what goes into the sub-plans.

3. Policy

Contingency Plans
The following contingency plans are contained in the planning presentation to staff:

- 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: the flow of responsibility when normal staff are unavailable to perform their duties.
- Data Study: details of 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 to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Communication Management: Who is in charge of giving information to the outside the business including some guidelines on what data is appropriate to be provided.

The plan is to be practiced to the extent possible. Management will set aside time to test implementation of the disaster recovery plan. During these tests, issues that may cause the plan to fail should be corrected.

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

4. Exceptions

Any exception to the policy must be approved by the Management Team in advance.

5. Non-Compliance

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

6. Related Standards, Policies and Processes

Business Continuity Plan.

Disaster recovery/Business continuity plan overview slide: