Business Continuity

Purpose

The primary objective of this recovery policy is to provide guidance, tools, and procedures allowing a company to survive a disaster and re-establish normal business operations. For this, the organization must assure that critical operations can resume within a reasonable time frame. The goals of this policy are to enable the organization to identify weaknesses and implement a disaster prevention program, minimize the duration of disruption to business operations, facilitate effective coordination of recovery tasks, and reduce the complexity of the recovery effort.

Scope

This policy outlines a baseline disaster recovery plan to be developed and implemented by your company. It describes the process to ensure safety and recover IT Systems, applications, and data from any type of disaster affecting company assets.

Definitions

DRP stands for Disaster Recovery Plan. A plan to endure business continuity in the event of a disaster that destroys part or all of a business's resources, including IT equipment, data records, and the in some cases even the physical space of an organization.

1. Assessment and Inventory

Critical business processes are defined as processes that have an immediate impact on business activities when they are down. To safeguard critical business processes and related assets, the company must assess them, define their requirements for data integrity, and determine how the different areas of the company will be affected in the event that the data becomes unavailable.

1.1 Map and document critical processes and related assets.

1.2 Following the mapping of critical processes and related assets, map up critical data.

2. Data Backup

A company should create processes to back up critical data and store the data in a separate dedicated network to ensure data continuity.

2.1 Store backups in a separate dedicated network, that is connected to the main company network only when backing up data.

2.2 Create a process to back up critical data from employee workstations.

2.3 Back up critical application data both On-Premises and in the cloud, Software as a service

(SaaS).

2.4 Back up critical data from company network storage.

2.5 Make sure to include in the regular backup routine critical data stored in company external storage devices, such as hard drives.

2.6 Back up the server data and configuration.

3. Recovery Requirements

The basis of a recovery plan is to define the desired Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

3.1 Define with management the RTO and RPO for each critical business process.

3.2 It is important to verify the reliability of meeting the targets for Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

3.3 Develop and implement an ICT Business Continuity policy

4. Recovery Testing

The recovery plan should be tested, maintained, and updated regularly. The backup process requires that personnel be trained to handle contingencies.

4.1 Test recovery processes for different scenarios.

4.2 Train employees for disaster recovery and emergency response.

5. Backup Protection

Using encryption, backing up to a separate site, and backing up through a dedicated admin account are ways of safeguarding the backup process.

5.1 Create a dedicated admin account for backup and restoring daily tasks.

5.2 Encrypt backups to prevent data theft or loss.

5.3 Prepare a separate site for deploying contingency plans for data centers and employee workplaces.

6. Continuity

Hardware components, software infrastructure, and physical workspaces require alternate physical solutions to ensure the continuity of company performance.

6.1 Implement information processing facilities with redundancy sufficient to meet availability requirements.

7. Incident Recovery

The goal of recovery after a cybersecurity incident is to restore normal operations, strengthen defenses, and rebuild trust with stakeholders. This process involves implementing a comprehensive recovery plan, managing public relations effectively, and incorporating lessons

learned to avoid future incidents and mitigate potential reputation damage.

7.1 Execute recovery plans for cybersecurity incidents.

7.2 Integrate lessons learned from incidents into your recovery processes

7.3 Manage post-incident public relations and repair company reputation.

8. Continuous Improvement

In order for policies, processes, and procedures to stay current, they need to be reviewed and updated regularly.

8.1 The policy, processes, and procedures are reviewed and updated annually.