BUSINESS CONTINUITY MANAGEMENT POLICY

Table Of Contents

1 Purpose - Business Continuity Management....2

2 Policy Statement....2

2.1 BUSINESS IMPACT ANALYSIS....2
2.2 RISK MITIGATION....2
2.3 BUSINESS CONTINUITY STRATEGY....2
2.4 BUSINESS CONTINUITY PLAN....3
2.5 DISASTER RECOVERY PLAN....3
2.6 DR DOCUMENT....3
2.7 TESTING....5
2.8 Updating your BCP and DRP....5

1 Purpose - Business Continuity Management

In accordance with industry 'best practices' and to comply with numerous compliance regulations, The company has implemented various Information Security policies and procedures in order to protect the confidentiality, integrity and availability (CIA) of their critical client data, their computing resources, and their business interests. This document provides describes the Business Continuity Management procedures to be performed by the IT staff at The company.

2 Policy Statement

2.1 Business Impact Analysis

Before a Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP) is created, a Business Impact Analysis (BIA) must be performed on each business unit's systems and processes.
Guidelines for this can be found in the, "The company's Risk Assessment Planning Guide for Information Technology Systems".
Things to consider:

- A determination the maximum time of not having the service(s) provided by the system that can be tolerated.

An identification of all of the threats to the system such as:

- Program or Data Failure.
- Hardware Failure.
- Electrical Power Failure.
- Fire.
- Natural disasters

2.2 Risk mitigation

Following the BIA, appropriate controls should be considered for implementation in order to decrease the risk to an acceptable level.

The business process owner should discuss all risk mitigation options with Management before the strategy is developed.

2.3 Business continuity strategy

Business process owner and Management should then develop a business continuity strategy consistent with business objectives. Emphasis should be on restoring services within the acceptable time.

- BCP recovery strategies should include input from all relevant business units. This ensures that there is ownership of the BCP strategy by the business units.
- Assess all the risks associated with the strategy you have adopted.
- Business owners must weigh their tolerance for downtime when selecting a recovery strategy.
- Once the strategy is determined, develop the BCP.

2.4 Business Continuity Plan

All COMPANY locations must create high-level BCP's (often non-IT system specific, business recovery). BCP's should include manual processes where possible, and should be developed in conjunction with Business Process Owners, not IT personnel. Individuals must be assigned to execute each component of the plan.

2.5 Disaster Recovery Plan

DRP can be included with the BCP and will often involve IT specific recovery. Business Process owners and IT personnel must work together to create the DRP. All IT systems should be considered during the development of the plan. Individuals must be assigned to execute each component of the plan.

For example, the following areas should be included in the plan :

- Data backup – media/content must be sent offsite.
- Documentation backup – all hard copies and soft copies
- Archived data – may include removable and internal media
- Facilities backup – for example: backup generator, UPS.
- Business resumption team training – during disaster
- Critical applications
- Alternate processing procedures – for example manual procedures.

2.6 DR Document

Your DR Plan must include a DR document. This is what you will use during an actual disaster and auditors will require it.

This is how the document should be structured:

Mitigation

- *Identify Recovery Components (the scope of the plan)*
- *Perform an Operational Analysis – to ensure current operational flaws are not replicated in emergency mode so you must review the current strategy*
- *Perform a Disaster Risk Analysis*

Examples to look for are:

- *Electronic security*
- *Viruses*
- *Hardware failure*
- *Fire*
- *Power outages*
- *Physical security*
  - *Flood*
  - *Storms*
  - *Civil unrest*
  - *Sabotage*
  - *Labor disputes*

Preparation Mode

Focus on documenting existing systems, network configurations, hardware, applications and assigned personnel.
This answers the question of WHAT needs to be recovered, WHEN (prioritized), HOW and by WHOM.

- *Document Systems and Applications*
- *Perform a (Risk) Tolerance Analysis*
- *Prioritize Recovery*
- *Create Organizational Chart*
- *Create a Contact List (print and distribute)*
- *Put in place a DR Team*
- *Assign Roles and Responsibilities*
- *Review the Plan*
- *Make necessary policy changes to align with the plan*
- *Test the Plan*
- *Implement the Plan*
- *Perform routine Plan Maintenance*

Response Mode

- *Conduct the appropriate actions in the Event of an Emergency – evaluate the problem before engaging Recovery Mode.*

Recovery Mode

- *Execute the plan*

2.7 Testing

Must be tested at least annually where possible.

2.8 Updating your BCP and DRP

Must review annually and updated if.