Disaster Recovery Plan

Jan 2020

Introduction

Overview

The Disaster Recovery Plan (DRP) sets out…

Accompanying Documentation

This DRP is accompanied with a group of documents, together forming the ***Disaster Recovery Pack***.

- Business Continuity Plan
- Disaster Recovery Plan (this document)
- Data Backup and Recovery Policy
- Technology Vendor/Provider Contact List
- IT Asset Register (Up-to-date excel export)

Where can I find copies of this plan

Document locations -

- ***Primary File Server***
- ***Secondar Office Domain Controller Server***
- ***Printed copies***, in various locations

Purpose

Importance of the DRP

Assumptions & Other Considerations

Disaster Recovery Review Panel (DRRP)

The Disaster Recovery Review Panel (DRRP), consisting principally of key personnel, with relevant decision-making abilities.

DRRP Member Structure

Disaster Recovery Review Panel (DRRP)		
Name, Title	**DRP Responsibility**	**Contact Option**
John Smith Chief Executive Officer	Final approval	Work Number Mobile Number Work Email Alternate Email
Emilio IT Director	Final approval	Work Number Mobile Number Work Email Alternate Email

1. Disaster Recovery Team (DR Team)

Specialist leads in the event of a disaster. Other roles can be added.

1.1 DR Team Roles

DR Director

overall recovery of an incident and the restoration of business systems and functionality. Additional information to be added specific to the organisation and role.

DR Coordinator

overall direction and response of an incident, coordinating the entire recovery process. Additional information to be added specific to the organisation and role.

DR Management Team

specialists team members and vendors, as well as allocating priorities for the members of the team. Additional information to be added specific to the organisation and role.

DR IT Network Team

assessing, and repairing all IT Network Systems, including Network links, Firewalls, Routers and Switches. Additional information to be added specific to the organisation and role.

DR IT Systems & Applications Team

assessing and repairing all IT Systems and Applications. Additional information to be added specific to the organisation and role.

DR IT Backup & Restore Team

restoration of data from on-premise, cloud and archive backup services. The team will take direction from the DR Management Team and will work closely with the other technical teams as required.

1.2 DR Team Member Structure

Disaster Recovery Team (DR Team)		
Name, Title, Company	**Role**	**Contact Option**
Sue Helen Director, Shared Services *Company Name*	DR Director	Work Number Mobile Number Alternate Number Work Email Alternate Email
Emilio Director of Tech *Company Name*	DR Coordinator (primary) DR Management Team (primary) DR IT Systems & Applications Team DR IT Backup & Restore Team DR IT Network Team	Work Number Mobile Number Alternate Number Work Email Alternate Email

2. Communication Plan

How is the DRP initiated, who is contacted and in what order. This may include informing directors, board and CEO.

3. Alternate Assembly Location **could also be located in BCP

3.1 Staff - Working remotely (local)

3.2 Staff – Office A

3.3 Staff – Office B

3.4 Staff – Shared Space Office Building 233

3.5 Staff – Working remotely (international)

4. Core System Setup

The critical business processes and systems, as well as agreed backup approach and strategies are listed below.

Core Systems reside across five locations.

1) Head Office. Address, and what IT systems are located here
2) Brisbane Office. Address, and what IT systems are located here
3) Singapore Office. Address, and what IT systems are located here
4) Amazon Cloud (AWS). Address, and what IT systems are located here
5) NextGeneration DataCenter. Address, and what IT systems are located here

4.1 Hardware / System Configuration

Critical Business Service / System	Backup/Recovery Strategy	Location
Physical Server Hardware (Lenovo, Dell, HP)	x34 VMware ESXi Hosts setup with HA	Head Office
Network Switching (Cisco, HP)	x38 Cisco Gigabit Switches, x4 HP Gigabit Switches	Singapore Office

5. Recovery Point Objective (RPO) & Recovery Time Objective (RTO)

The critical business processes and systems are listed below.

5.1 Recovery Point Objective (RPO)

Time period allowed for data to be lost, before it is not useful.

Critical Business Service / System	RPO
Email services (Exchange, Microsoft 365)	24 hours
Finance services (Xero)	24 hours
Human Resource services (File Server)	24 hours
VoIP Telephony	2 days

5.2 Recovery Time Objective (RTO)

Time period allowed for service to be unavailable before significant risks and losses are incurred.

What is the maximum length of time allowed between an unexpected failure and recovery of normal operations of service?

Critical Business Service / System	RTO
Single Physical Server Hardware	2 days
Multiple Physical Server Hardware	4 hours
Firewall Hardware	4 hours
Network Hardware – Switches/Firewalls	4 hours
Data/Software/Applications – Email	4 hours

6. Incident Type, Response and Recovery

Identifying the incident type, response and recovery options to invoke DR led by the DR Coordinator. Each incident scenario may require a varied response and resolution.

The below incident types may lead to the activation of the DRP.

6.1 Incident Type

6.1.1 Loss of Head Office;
6.1.2 Loss of Primary Datacenter;
6.1.3 Major Cyber Attack;
6.1.4 Major Network Failure;
6.1.5 Major Power Failure;
6.1.6 Loss of Core Server/System;
6.1.7 Environmental, Pandemic or similar;

6.2 Incident Response and Recovery

Each Team member will be assigned tasks, with each incident requiring varied response as required.

6.2.1 DR Coordinator

Tasks -

- Inform the CEO of incident, seeking confirmation on invoking the DRP

6.2.2 DR Management Team

Tasks -

- Will take direction from and report to the DR Coordinator

6.2.3 DR IT Network Team

Tasks -

- Will take direction from DR Management Team member(s), with overall direction from DR Coordinator

6.2.4 DR IT Systems & Applications Team

Tasks –

- Will take direction from DR Management Team member(s), and DR Coordinator

6.2.5 DR IT Backup & Restore Team

Tasks –

- Will take direction from DR Management Team member(s), and DR Coordinator

7. Incident Review

7.1 Post incident review

A review meeting will be conducted, and all actions and response discussed.

Items for discussion will include -

- What worked well
- What didn’t work well, etc

8. Key Contacts

8.1 Primary internal & external stakeholders

Refer to ***BCP*** (Part of ***Disaster Recovery Pack***)

8.2 Service Providers, Vendors, Suppliers

Refer to ***IT Contact List*** document (Part of ***Disaster Recovery Pack***)

Appendices

Appendix 1 – WAN Diagrams

Appendix 2 – Head Office and Remote Office Rack Diagram

Appendix 3 – Cloud Systems setup