{Company Logo]

Business continuity and disaster recovery plan

[Company] BCP/DR Plan

Author: Joe Bloggs

Date: 6 September 2016

Version: 0.9

distribution audience

|  |  |  |
| --- | --- | --- |
| Name and Position | Date | Signature Required |
| [Name] [Position] |  | YES |
|  |  |  |
| [Name] [Position] |  | YES |
|  |  |  |
| [name] [Position] |  | YES |
|  |  |  |
| [Name]  [Position] |  | YES |
|  |  |  |
| [Name] [Position] |  | YES |

By signing approval of this document you understand its contents and your role and that of your team(s) in a BCP/DR scenario.

document version history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author(s) | Summary of Changes |
| 0.1 |  |  | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

contributors

|  |  |  |
| --- | --- | --- |
| Name | Position | Department |
|  |  |  |
|  |  |  |
|  |  |  |

Table of Contents

[1. general information 9](#_Toc460920607)

[1.1. Purpose 9](#_Toc460920608)

[1.2. Ownership 9](#_Toc460920609)

[1.3. Audience 9](#_Toc460920610)

[1.4. Process Involved 9](#_Toc460920611)

[1.5. When To Invoke The [Company] CMT 9](#_Toc460920612)

[1.6. Where To Meet 10](#_Toc460920613)

[1.7. What To Do With This Plan 10](#_Toc460920614)

[2. scope 11](#_Toc460920615)

[2.1. Structure And Format 11](#_Toc460920616)

[3. the strategy 12](#_Toc460920617)

[3.1. Background 12](#_Toc460920618)

[3.2. Business Impact Analysis (BIA) 12](#_Toc460920619)

[3.3. Property 12](#_Toc460920620)

[3.4. Network 12](#_Toc460920621)

[3.5. Framework/Strategy 12](#_Toc460920622)

[3.6. [Company] CMT 13](#_Toc460920623)

[3.7. [Company] IMT 15](#_Toc460920624)

[3.8. Other IT Team Contacts 15](#_Toc460920625)

[3.9. Development Contacts 15](#_Toc460920626)

[3.10. Key Business Contacts 16](#_Toc460920627)

[3.11. Disaster Recovery Functions 16](#_Toc460920628)

[3.12. Remote Support/Access Capability 17](#_Toc460920629)

[3.12.1. IT Group 17](#_Toc460920630)

[3.12.2. Leadership Team 17](#_Toc460920631)

[3.12.3. Development Team 18](#_Toc460920632)

[3.12.4. Project Team 18](#_Toc460920633)

[3.12.5. Business Analyst Team 18](#_Toc460920634)

[3.12.6. Test Team 18](#_Toc460920635)

[3.12.7. Finance Team 19](#_Toc460920636)

[3.12.8. Product Team 19](#_Toc460920637)

[3.12.9. Other Team 19](#_Toc460920638)

[4. The priority it services/system/business group 20](#_Toc460920639)

[4.1. Overview 20](#_Toc460920640)

[4.2. Pre-Prioritised Services/System 20](#_Toc460920641)

[4.3. Pre-Prioritised Business Group/Functions 21](#_Toc460920642)

[5. restoration priorities and timeframes 22](#_Toc460920643)

[5.1. Fault Tolerance 22](#_Toc460920644)

[5.2. Scenario Planning 22](#_Toc460920645)

[5.3. Scenario.1 22](#_Toc460920646)

[5.4. Scenario.2 24](#_Toc460920647)

[5.5. Scenario.3 24](#_Toc460920648)

[5.6. Scenario.4 25](#_Toc460920649)

[5.7. Scenario.5 25](#_Toc460920650)

[5.8. Scenario.6 27](#_Toc460920651)

[5.8.1. Service Desk 27](#_Toc460920652)

[5.9. Scenario.7 28](#_Toc460920653)

[6. the initial response guidelines & processes 30](#_Toc460920654)

[6.1. Alert Levels 30](#_Toc460920655)

[6.2. Initial Response & Activation Procedures 30](#_Toc460920656)

[6.3. Mobilisation 31](#_Toc460920657)

[6.4. IS Damage Assessment Procedures 31](#_Toc460920658)

[6.5. Action Plan Development 32](#_Toc460920659)

[6.6. Resumption Procedures 32](#_Toc460920660)

[6.7. Recovery Procedures 32](#_Toc460920661)

[6.8. Restoration Procedures 33](#_Toc460920662)

[6.9. Communications 33](#_Toc460920663)

[6.9.1. Internal Communications 33](#_Toc460920664)

[6.9.2. Customer Communications 34](#_Toc460920665)

[6.9.3. Media communications 34](#_Toc460920666)

[6.9.4. Emergency Services Communications 34](#_Toc460920667)

[7. pandemic response activities 35](#_Toc460920668)

[7.1. Assumptions 35](#_Toc460920669)

[7.2. Actions 35](#_Toc460920670)

[8. ongoing operational management responsibilities 37](#_Toc460920671)

[8.1. Effective Service Continuity Management And ITIL 37](#_Toc460920672)

[8.2. Education And Awareness 37](#_Toc460920673)

[8.3. Training 37](#_Toc460920674)

[8.4. Reviewing & Auditing 37](#_Toc460920675)

[8.5. Change Management 37](#_Toc460920676)

[8.6. Testing 38](#_Toc460920677)

[9. Appendices 40](#_Toc460920678)

[9.1. Appendix 1: Network Diagram 40](#_Toc460920679)

[9.2. Appendix 2: Useful Contact Numbers 41](#_Toc460920680)

[9.3. Appendix 3: list of [Company] buildings with generator capabilities 42](#_Toc460920681)

[9.4. Appendix 4: On Call Process 43](#_Toc460920682)

[9.5. Appendix 5: Bcp Change Control 44](#_Toc460920683)

[9.6. Appendix 6: Conference Number 45](#_Toc460920684)

[9.7. Appendix 7: Crisis Event Log 46](#_Toc460920685)

[9.8. Appendix 8: BCP Planning Checklist 47](#_Toc460920686)

[9.9. Appendix 9: BCP Roles & Responsibilities 49](#_Toc460920687)

[9.10. Appendix 10: Communcations 51](#_Toc460920688)

[9.11. Appendix 11: Major Incident Process 52](#_Toc460920689)

[9.12. Appendix 12: Contact List 53](#_Toc460920690)

[9.13. Appendix 13: Phone System Information 54](#_Toc460920691)

[9.14. Appendix 14: Remote Access 55](#_Toc460920692)

[9.15. Appendix 15: Off Site Storage 56](#_Toc460920693)

[9.16. Appendix 16: Data Centres 57](#_Toc460920694)

List of Figures

No table of figures entries found.

List of Tables

Table 1: Related Documents 6

Table 2: Governing Policy and Procedure Documentation 7

Glossary

|  |  |
| --- | --- |
| Term | Description |
| BAU | Business as usual |
| RTO | Return to Operation (usually after an outage) |
| IMT | Incident Management Team – usually technical resources required to restore services (in this case they can come from any team as required, based on the outage type) |
| CMT | Crisis Management Team which is made up from senior members of [Company] to determine how best to respond to a crisis situation and lead/coordinate restoration efforts |
| Recovery Team | Part of the [Company] IMT, these resources actually do the work to restore services/system and may be made up of multiple team depending on the nature of the crisis. |
|  |  |
| Team member | A contractor, permanent, temporary person employed by [Company] |
| SAN | Storage Area Network |
|  |  |

related documents

The following table lists other documents reference by this document

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ref | Document Name | Description | Location | Version | Author |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 1: Related Documents

The following table lists documents that describe policy, standards and procedures that apply to the continuing operational support of the deliverables of DR/BCP planning and execution:

|  |  |  |  |
| --- | --- | --- | --- |
| Ref | Document Name | Description | Location |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 2: Governing Policy and Procedure Documentation

# general information

## Purpose

The purpose of this plan is to:

* Outline the **strategy** used for the formation of this Business Continuity Plan
* Identify how [Company] will respond to a Crisis/Incident and how the Support/Operations Teams will continue to function in a crisis scenario
* Assist Support/Operations Teams in the restoration of key IT Services and business processes to **agreed levels within the agreed timeframes** following a major disruption
* Publish a “**Baseline**” of the **priority IT services**, their **restoration priorities** and **restoration time frames** as seen by IS following a major disruption
* Provide **guidelines** to Support/Operations Teams and other critical teams for the initial response to a failure or disruption that prevents [Company] from operating ‘Business As Usual’ (BAU)
* Enable the sustained **execution of identified processes** in the event of a major disruption
* Identify **functions, roles** and **responsibilities** of the Crisis Management Team, Support/Operations Teams and recovery teams
* Assist Support/Operations Teams in the **management of risk** following an IT Service failure or disruption.

## Ownership

* Ownership of the [Company] DR/BCP rests with Chief Executive the but is under the management of the Operations Manager
* The [Company] DR Co-coordinator is responsible for maintenance and change control of the plan and ensuring consistency with other [Company] business groups BCP documents.

## Audience

* IT Support/Operations Teams
* [Company] Leadership Team
* Other [Company] Business Groups (especially those who may be involved with the IMT or CMT)
* Customers as required

## Process Involved

Major Incident Process

The first respondent must notify one the [Company] Leadership along with all known information, who will then determine the crisis/impact level and invoke the Major Incident process in [Appendix 11](#_Appendix_11:_Major) if required.

## When To Invoke The [Company] CMT

The [Company] CMT (list of members is in [Section 3.6](#_[Company]_CMT)) can be invoked by the [Company] IMT (list of member in [Section 3.7](#_[Company]_IMT)) if they feel that wider [Company] involvement is required (e.g. to assist with communications or that the incident may be unable to be resolve within 2 days or as required by [Company] Customer Service Agreements/Contracts/SLAs. The [Company] CMT will be contacted through the CFO or Chief Executive (contact numbers are in [Section 3.6](#_[Company]_CMT)) who will make the decision to invoke the [Company] CMT or not.

## Where To Meet

The [Company] Incident Management Team (IMT) and [Company] CMT Team (if required) should meet in the following location(s): [Location] (Incident Management Hub) if either of these locations are unavailable then use: [Location]

## What To Do With This Plan

**Leader’s/Managers responsibility:** Print two copies and keep a copy at home and another in the office. Also keep a copy on a USB stick at home and also make sure you can access it via your Email as another way of keeping a copy to be easily accessible. Also ensure all team members have a copy accessible should they be called to partake in a BCP/DR exercise or event

# scope

This BCP/DR Plan focuses only on those critical IT Services/Systems required to support the vital business processes of [Company] and it customers and centres on core Applications/infrastructure and systems to support those customers and [Company] itself. The impact of the “loss” has been measured through the business impact analysis (BIA) carried out by the Operations Manager.

During the process of BIA a large number of scenarios were identified which caused considerable debate and litigation. To ensure consistency and clarity this plan covers seven selected scenarios:

1. Single Service or System failure
2. Multiple Services or Systems failure (concurrently)
3. Total loss of the Data Centre Services (and its facilities)
4. Total devastation of the [your region] Isthmus (e.g. volcanic eruption, tsunami, earthquake, significant loss of life)
5. Pandemic Management: OPERATIONS’s proposed service offering during a pandemic
6. Building evacuation: Relocating critical [Company] staff or supporting the relocation of critical business staff should a [Company] building be inaccessible or due to be evacuated or unusable because of power issues on site
7. Loss of Power to an [Company] Data Centre(s)

## Structure And Format

The IS BCP is divided into six sections:

1. The strategy
2. The priority IT services and systems
3. The restoration priorities and time frames matrix
4. The initial response to a failure, guidelines and processes to be used following a disruption
5. IS’ Pandemic Crisis activities
6. Ongoing operational management responsibilities

**Section 1** – Outlines the strategy used to define the plan, the purpose of the strategy and the expected outcomes

**Section 2** – Outlines the critical IT services identified during the business impact analysis

**Section 3** – Outline the restoration priorities for the IT Services and the expected periods for their restoration

**Section 4** – The OPERATIONS guidelines and processes to be followed during the initial response and subsequent restoration activities following a disruption

**Section 5** – Based on the proposal put forward by OPERATIONS, this outlines the process and activities that would occur in OPERATIONS to support the organization during a Pandemic Crisis

**Section 6** – Outlines the on-going operational management responsibilities to ensure this plan succeeds.

# the strategy

## Background

[Company] has adopted the internationally recognised Information Technology Infrastructure Library (ITIL) as its IT Service management (ITSM) framework. Developed in the 1980’s, the IT infrastructure library has become the worldwide “de facto” best practice standard in IT Service Management. Starting as guide in the UK government, the framework has proved to be useful to organisations through its adoption by many companies as the basis for IT Service management. .

[Company] has based its BCP/DR strategies around the ITIL Service Continuity Management processes within the ITIL framework.

## Business Impact Analysis (BIA)

A business impact analysis (BIA’s) was carried out on the [Company] vital IT systems and services to identify the key deliverables for this plan. This plan represents OPERATIONS’s current capabilities in terms of its abilities to restore IT Systems/Services/Business Groups/Functions.

## Property

The [Company] offices (listed below) have a number of facilities in place to deal with BCP/DR scenarios

|  |  |  |  |
| --- | --- | --- | --- |
| ITEMS | Location 1 | Location 2 | Location 3 |
| Spec & Quantity |  |  |  |
| Contractor |  |  |  |
| Service Power  Supplied |  |  |  |
| Running time |  |  |  |
| Fuel Tank Size |  |  |  |
| Refuel Contractor |  |  |  |
| Service Frequency |  |  |  |
| Annual Service Date and load test data |  |  |  |

## Network

{Describe network set up} (see [Appendix 1](#_Appendix_1:_), for a network diagram).

## Framework/Strategy

The ITIL strategy is broken down into four stages, which IT have followed during the formation of this plan. Note that this framework is best practice and IT have chosen to use it as a guide only.

The ITIL approach uses a “4 stage” methodology

Stage 1: Initiate Business Continuity Management (BCM)

This involves policy setting, specifying the terms of reference and the allocation of resources.

Stage 2: Requirement analysis and strategy definition

This involves business impact analysis (BIA), Risk assessment and the formation of Disaster Recovery (DR) and Business Continuity Planning (BCP) strategies.

Stage 3: Implementation

This involves planning and development of recovery plans, implementing of risk reduction measures and standby arrangements and initial testing.

The recovery plans are constantly under review by the accountable [Company] Leaders as part of the on-going management of Services they provide.

Stage 4: Operational Management

This involves education and awareness, review and auditing, testing (regularly), change management and on-going training and assurance

The responsibility for the on-going management of the DR/BCP rests with the Department managers responsible for the individual areas. Each manager is to ensure that the DR services they provide are at the standards outlined in this plan. This includes the management of change as the infrastructure/services evolve.

Whilst recoveries are constantly being tested as part of the regular business as usual (BAU) activities, the on-going strategy is to test the core applications/services recovery on an annual basis. It is also essential to test the restore and recovery processes all current backup systems monthly.

## [Company] CMT

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Team Members | Function | Phone contact |
| Escalation and inform Board if required, liaise with customer(s)/media as needed |  | Chief Executive |  |
|  | CFO |  |
| Lead & coordinate with IT/Operations. Also the DR Coordinator |  | CTO |  |
| Coordinate with Applications team |  | Development Manager |  |
| People & Performance liaison (if required) |  | HR Manager |  |
| Liaise with Customer (if required) |  | Service Delivery/Client Managers |  |

[Company] crisis management structure

## [Company] IMT

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Team Members | Function | Phone contact |
| Recovery Manager |  |  |  |
|  |  |  |
|  |  |  |
| Supervisor & Recovery Team |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

\*Also the disaster Recovery Coordinator (with {name} as a backup)

**Note:** The Recovery team can be made up on any resources from [Company] or its suppliers to restore services; the above list is just an indication

## Other IT Team Contacts

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Team Members | Function | Phone contact |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |

## Development Contacts

| Role | Team Members | Function | Phone contact |
| --- | --- | --- | --- |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |
| Team Members |  |  |  |

## Key Business Contacts

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Location | Phone contact |
| Landlords |  |  |  |
| Recovery Manager |  |  |  |
| Supervisor |  |  |  |

## Disaster Recovery Functions

The functions of each team listed below are to be used as a guide only.

[Company] CMT

1. Direct and authorise the recovery effort
2. Set policy
3. Manage IS DR/BCP
4. Accept IS DR/BCP deliverables,
5. Communicate and maintain IS DR/BCP awareness with team members.

[Company] IMT

* Liaison between the [Company] CMT and Recovery Teams
* Ensure procedures necessary to facilitate a successful Disaster Recovery are integrated into day-to-day operations
* Assist the DR Coordinator in maintaining the plan and authorising regular drills, training and testing.
* Negotiate and manage contracts, consultants and external service providers where necessary during a crisis
* Work with Recovery Team members to identify the most appropriate recovery method for the crisis.

Recovery Managers

* Define and ensure IS DR/BCP deliverables
* Manage test review and assurance exercises
* Contract for services (as required)
* Undertake IS DR/BCP analysis
* Ensure BCP and DR actions are undertaken as requested by the IS Incident Management Team
* Maintain plan
* Ensure annual testing, awareness and education is undertaken
* Be the contact point for matters relating to DR and DR planning pertaining to their area of expertise

Supervisors and Team members

* Develop IT DR/BCP deliverables
* Develop operate and perform procedures
* Perform test reviews and assurance
* Coordination of resources to carry out actions requested by the [Company] Incident Management Team
* Form part of the [Company] Recovery Team

## Remote Support/Access Capability

### IT Group

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Position | Remote access capability |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Leadership Team

|  |  |  |
| --- | --- | --- |
| Name | Position | Remote access capability |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Development Team

|  |  |  |
| --- | --- | --- |
| Name | Position | Remote access capability |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Project Team

|  |  |  |
| --- | --- | --- |
| Name | Position | Remote access capability |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Business Analyst Team

|  |  |  |
| --- | --- | --- |
| Name | Position | Remote access capability |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Test Team

|  |  |  |
| --- | --- | --- |
| Name | Position | Remote access capability |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Finance Team

|  |  |  |
| --- | --- | --- |
| Name | Position | Remote access capability |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Product Team

|  |  |  |
| --- | --- | --- |
| Name | Position | Remote access capability |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Other Team

|  |  |  |
| --- | --- | --- |
| Name | Position | Remote access capability |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# The priority it services/system/business group

## Overview

This section outlines the priority and order in which services/systems are to be recovered; it also outlines the priority for each business group.

## Pre-Prioritised Services/System

|  |  |  |
| --- | --- | --- |
| Service/system | Priority | Comments |
| Network and Active Directory Services | 1 | Prerequisites to get other services working (incl. DCs, DHCP servers, internet) |
| Core Infrastructure | 2 | SAN, core switches, VM environment, backup & Db servers i.e. underlying infrastructure for all services |
| Internet Access | 3 |  |
| Computers | 4 | Allows [Company] users to log in to the [Company] network and tools to carry out their jobs |
| JIRA\* | 5 | Used by internal teams and customers to detail development work for applications/SDLC/bug fixes |
| Maven\* | 6 | Development tool used by [Company] to store code releases |
| GIT\* | 7 | Code repository, holds [Company]’s IP |
| Service Desk Tool | 8 | Allows all customers to log incidents/changes/problems. In the event of a failure then Service Desk will have to revert to pen and paper or making notes in word and calling back customers when Service Desk Tool is recovered |
| E-mail | 10 | MS 365 |
| Remote Access | 11 | Remote access is dependent on the above services (internet access, directory services) being available |
| VoIP Phones | 12 | Critical business function to allow [Company] to be contacted, in the event of a PaBX failure the [Company] answering services kicks in, so no calls will be lost. |
| Monitoring Tool | 1 |  |
| [Company] web site | 2 |  |
| Other websites | 3 |  |
| Production Environments | 4 |  |
| Project environments | 5 | Stand up any environments used by project teams, that do not just recover as a result of standing up the core infrastructure (above) |
| Payroll | 1 | Finance package |
| Dropbox/Google Docs | 1 |  |
| Yammer | 2 |  |
| Skype | 3 |  |

**Note:** the number (in each column) denotes the order in which the business group/function will be recovered for each priority (e.g. Jira will be the fifth system to be recovered of the priority 1 group)

\* Denotes critical [Company] Applications

## Pre-Prioritised Business Group/Functions

|  |  |  |
| --- | --- | --- |
| Department | Priority - BAU | Priority – Crisis/Emergency |
| Service Desk | 1 | 1 |
| Leadership Team | 4 | 1 |
| IT Group | 2 | 2 |
| Development Team - BAU | 3 | 3 |
| Development Team - Projects | 1 | 1 |
| Finance | 2 | 2 |
| HR | 3 | 4 |
| Project Managers | 1 | 2 |
| Business Analysts | 3 | 3 |

|  |  |
| --- | --- |
| Legend | Max. tolerable disruption |
| Priority 1 | 1-2 days |
| Priority 2 | 3-7 days |
| Priority 3 | 1-2 weeks |
| Priority 4 | Cloud provided |

Please be aware of any customer priorities, these will be detailed in their own BCP/DR plans, the above priorities are for [Company] Managed systems only.

# restoration priorities and timeframes

## Fault Tolerance

All the critical IT Systems/Services are designed with a degree of fault tolerance/redundancy in mind, utilising the appropriate technology such as database clustering, application load balancing, and built in hardware redundancies (RAID, disk mirroring, etc.).

The resultant is that should we experience an initial component failure the service will continue to operate. An alarm will be triggered in the [monitoring tools](http://acnagios1/nagios.php) and the initial fault is responded to and resolved accordingly without the service being impacted or an outage being experienced.

For the purposes of this document, when we state “System failure”, we mean a total failure following those initial counter measures. Therefore the total restoration time refers to a situation where all initial “built in” redundancies have been compromised and / or the fault is serious enough to totally disable the service, requiring a complete rebuild from the ground up.

## Scenario Planning

For each scenario (detailed below), there will be high level analysis of what is affected, likely restoration times and activities as well assumptions:

**Scenario.1** - Single Service or System failure

**Scenario.2** - Multiple Services or Systems failure (concurrently)

**Scenario.3** - Total loss of the Data Centre Services (and its facilities)

**Scenario.4** - Total devastation of the [your region] region (e.g. volcanic eruption, tsunami, earthquake, significant loss of life)

**Scenario.5** - Pandemic Management: IT’s proposed service offering during a pandemic

**Scenario.6** - Building evacuation: Relocating critical [Company] staff or supporting the relocation of critical business staff should a [Company] building be inaccessible or due to be evacuated or unusable e.g. because of power issues on site

**Scenario.7** - Loss of Power to a [Company] Data Centre

## Scenario.1

This section outlines the capabilities of [Company] to restore the key IT Services/systems that support the organisations vital business processes for itself and its customers in **respect to a single service failure**.

This Plan assumes that in the case of a single system failure, the data storage component of each system will be provided by a new storage system, separate to the existing SAN storage system - which will continue to be used by the other systems in operation.

The first respondent must notify the relevant manager(s) along with all known information; they will then determine the incident level and invoke the Major Incident process, (in [Appendix.11](#_Appendix_11:_)) and if the incident can be handled by the IT Group.

If the outage/incident is not able be recovered within 1-2 days then the [Company] CMT maybe be invoked by members of the [Company] IMT

**Estimated time of recovery (by system - see chart)**

The table below contains the estimated time to recovery for each of the systems included in this plan.

**Procurement:**

The procurement process available to [Company] for the purposes of this plan is estimated at “nil” as hardware will be made available (utilising/leveraging development and test services or borrowing from suppliers) as required. However if new hardware is required sourcing that may take some time depending on availability.

**Recovery Activities (basically rebuilding system(s) from the bottom up):**

The recovery activities including, troubleshooting/analysis, server building, operating system build, application install, patch application, data restore (from tape or disk), configuration and interface/application testing. Note these estimates are durations, not effort.

**System Restoration Timeframes**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| System Name | Procure | Install or Implement | Restore | Test | Total time to restore Service |
| Network & AD |  |  |  |  |  |
| Core Infrastructure |  |  |  |  |  |
| Email |  |  |  |  | On Microsoft 365 – cloud based solution |
| Internet Access |  |  |  |  |  |
| AWS |  |  |  |  |  |
| Remote Access |  |  |  |  |  |
| Monitoring |  |  |  |  |  |
| Phones |  |  |  |  |  |
| Service Desk Tool |  |  |  |  |  |
| [Company] Website |  |  |  |  |  |
| Confluence/Intranet |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

ND = next day

\* = some file restoration may occur before these times, but will be on a priority basis

$ = will be less if parts are in country, time taken will be for vendor (such as IBM or HP) to arrive with parts on site.

The remote access solution is based on Outlook Web Access (OWA), VPN or RDP access.

Outlook web access is a good way to access your e-mail from a PC with an internet connection <https://login.microsoftonline.com> for Microsoft 365

## Scenario.2

This section outlines the capabilities of [Company] to restore the key IT Services/systems that support the organisations vital business processes for itself and its customers in **respect to multiple service failures**.

Same as “single service restoration” timeframes however this would be carried out concurrently.

The first respondent must notify the relevant manager(s) along with all known information; they will then determine the incident level and invoke the Major Incident process, (in [Appendix 11](#_Appendix_11:_)) and if the incident can be handled by the Technology Services Group.

If the outage/incident is not able be recovered within 1-2 days then the [Company] CMT will be invoked by members of the [Company] IMT.

## Scenario.3

In the event of a **total loss of one of [Company]’s Data Centre** by an event or series of events (e.g. a technical catastrophe, overheating, contamination of the environment, flooding etc.)

The first respondent must notify the relevant manager(s) along with all known information; they will then determine the incident level and invoke the Major Incident process, (in [6.1](#_Appendix_11:_Major)) and if the incident can be handled by the IT Team.

If the outage/incident is not able be recovered within 1-2 days then the [Company] CMT will be invoked by members of the [Company] IMT

Assumptions:

1. All projects will stop (or have minimal support so resources can focus of restoration tasks)
2. All Professional Services resources sent home and are not to use the network resources
3. All non-essential staff to go home, where they can assist they will be seconded to the Recovery Teams
4. The [Company] CMT will decide where to relocate critical staff
5. Critical [Company] staff is available at all times – from the IT and Development teams as well as the Leadership Team.

IT would have to request off site tapes (list of offsite tape locations and providers can be found in [Appendix 15](#_Appendix_15:_)) to be returned to [Company] premises and they will be used to recover data to any available infrastructure either at another [Company] Data Centres or secondary site (yet to be determined). [Company] will have to borrow, lease or get on loan replacement equipment in which to restore services, which may take several days or weeks and then will have to restore from tape which will take several days to weeks.

**Cloud Infrastructure**

[A description of each service/technology, any dependencies]

**Recommendation:** [Ways of ensuring functionality during a BCP scenario]

**The Voice Connectivity**

[A description of each service/technology, any dependencies]

**Recommendation:** [Ways of ensuring functionality during a BCP scenario]

**Network Connectivity**

[A description of each service/technology, any dependencies]

**Recommendation:** [Ways of ensuring functionality during a BCP scenario]

**Active Directory and Email**

[A description of each service/technology, any dependencies]

**Recommendation:** [Ways of ensuring functionality during a BCP scenario]

**Remote Access**

[E.g. the infrastructure to support remote access is physically located in the Data Centre 1, this requires the internet link at this location to be functioning in order for users to utilise the remote access solution.] **Recommendation:** [Create redundant remote access/service in at least two locations]

**Internet Access**

[A description of each service/technology, any dependencies]

**Recommendation:** [Ways of ensuring functionality during a BCP scenario]

## Scenario.4

A scenario involving the **total devastation of the [key] region** is a scenario we really do not want to plan for, that said in the event of this occurring we must ensure we cater for the wellbeing and safety of our staff. This scenario is also relevant for any location where we have [Company] staff located (remote workers or those in other offices).

## Scenario.5

IT service delivery during a **Pandemic** ([see section.7 for more details](#_Pandemic_response_Activities))will be dependent on the organisations ability to deploy mobile solutions (e.g. laptops and remote access, etc.) to its staff for either; use at home (via the internet) or to a suitable location connected to the [Company] network.

Our strategy to date has been to encourage critical business users to have remote access capability and supply remote access as requested. IT has ensured that most of the key business users have remote working capability already thus reducing the need to provide it during a pandemic.

IT also assumes that all business critical staff has remote access capability, such as laptops, mobile phones and remote access enabled.

The other dependency is IT’s ability to obtain additional bandwidth from its communication provider so it can provide the service to a higher volume of users (e.g. more network bandwidth quickly). This is simply a negotiation process with our communication provider which would enable more users to connect remotely.

## Scenario.6

Relocating critical [Company] staff or supporting the relocation of critical business staff. This scenario is to cover a **building evacuation** that lasts long enough (over 2 hours) to adversely impact the business (e.g. bomb threat, flooding, power outage).

IT service delivery during a building evacuation will be dependent on [Company] ability to decide which business critical functions and staff will be relocated to an alternative [Company] location or sent home or to an alternative location [Detail here of other locations]

Critical business staff/functions should already have mobile solutions (e.g. laptops using remote access, etc.) allocated for either; use at home (via the internet) or to a suitable location connected to the [Company] network or with internet access.

The IT strategy to date has been to encourage critical business users to have remote access capability and supply VPN access as requested. IT has ensured that most of the key business users have remote working capability already thus reducing the need to provide it during a pandemic.

If the building evacuation is the result of a power failure, please see [Appendix.3](#_Appendix_3:_)  for a list of [Company] buildings with generator capabilities.

Assumption:

1. The [Company] CMT will decide where to relocate critical business staff
2. All projects will stop if project resources are affected by the building evacuation or to make way for critical [Company] staff.
3. All projects will stop (or have minimal support so resources can focus of restoration tasks)
4. All Professional Services resources sent home and are not to use the network resources
5. All non-essential staff to go home, where they can assist they will be seconded to the Recovery Teams
6. The [Company] CMT will decide where to relocate critical staff
7. All business critical staff have remote access capability, such as laptops, mobile phones and remote access (and they know how to use them).
8. A building cannot be re-entered until the all clear has been given by the appropriate authorities (e.g. the Fire or Police Services or Structural Engineers or Electrical Engineers).
9. HR will ensure that processes for re-location meet staff safety requirements and support Business Managers in managing staff issues relating to re-location.

### Service Desk

If the building evacuation is likely to be more than one hour then provision of the [Company] Service Desk will have to catered for in an alternative location, the mostly likely secondary location would be: [List locations]

## Scenario.7

In the event of total loss of power to one of **[Company]’s Data Centres,** [Company] Leadership Team has outlined a plan (based on the BIA) that would allow critical services to be restored to the business with minimal disruption.

The first respondent must notify the relevant leader(s) along with all known information, they will then determine the incident level and invoke the Major Incident process, if the incident can be handled by the IT department.

If the outage/incident is not able be recovered within 1-2 days then the [Company] CMT will be invoked by members of the [Company] IMT.

All vendors (e.g. EMC, Datacom, Spark) should be contacted to be put on notice should [Company] infrastructure fail to be powered on or be faulty as new equipment will need to be supplied.

Assumptions:

1. All projects will stop (or have minimal support so resources can focus of restoration tasks)
2. All Professional Services resources sent home and are not to use the network resources
3. All non-essential staff to go home, where they can assist they will be seconded to the Recovery Teams
4. The [Company] CMT will decide where to relocate critical staff
5. Critical [Company] staff is available at all times – from the IT and Development teams as well as the Leadership Team.

[Company] will require the property landlords/Data Centre providers to restore power in to the affected Data Centre and once a stable power feed has been confirmed, the [Company] IMT will begin powering up infrastructure in a planned manner as stated in the Action Plan below. If mains or generators power is unable to be restored, temporary units will have to be provided by the landlords/Data Centre providers. [Company] IMT may have to invoke Scenario.3 as work to restore power continues to be completed in parallel.

Action Plan:

1. Networks: Monitoring and Management
2. Non SAN attached Domain Controllers
3. Infrastructure Servers (note: P Class blades chassis’ must be powered up as they are a SAN Fibre switch)
4. Storage
5. ESX clusters (VMware Farm)
6. Restoration of services based on priority (as per BIA in [section.4](#_the_priority_it)) - Once the underlying infrastructure has been restored, the services and applications affected in this scenario will be recovered in line with system/services priorities. The restoration of [Company] Core Applications will be provided in the same manner as outlined in scenario one and two and involves functionally testing each of the applications (by the Test Team).

**Services Affected by an outage to the Data Centre 1**:

{List services}

**Services Affected by an outage to the Data Centre 2**:

{List Services}

**Production Applications:**

{List}

**[Company] Internal Tools:**

{List}

# the initial response guidelines & processes

## Alert Levels

An incident is an unexpected event that could have significant impact on how the [Company] functions, or causes disruption of critical [Company] functions for more than half a day. [Company] has identified 4 different impact levels:

|  |  |  |
| --- | --- | --- |
| Alert  Level | Definition | Criteria |
| 1 | Single service outage where BAU recovery plans need to be activated or a threat may exist or be imminent.  (e.g. [Scenario.1](#_Scenario_1:)) | * Minor impact * Manageable situation * Low probability of escalation * No staff safety issues |
| 2 | An event has occurred or a previous alert has been escalated where the [Company] Data Centre and services are intact but with no or reduced personnel onsite. Multiple services have been affected. (e.g. [Scenario.2](#_Scenario_2:)) | * Possible escalation * Possible impact to [Company]’s reputation, services, resources and assets * Manageable situation * Possible impact to ‘normal business operations’ * Unavailability of staff or redeployment of staff may occur * Invoke [Company] IMT * Use Major Incident Management process to assist with communications to customers/organisation |
| 3 | Multiple service outage/loss of data where DR/BC plans need to be invoked but Data Centre remains intact. (e.g. [Scenario.7](#_Scenario_7:)) | * Criminal act may have occurred * Situation is difficult to manage * Major disruption to ‘normal business operations’ * [Company] CMT may be invoked * Unable to restore services within 1-2 days |
| 4 | Multiple service outages/loss of data where DR/BC plans need to be invoked through damage or destruction/loss of a Data Centre or occurrence of a major regional/ national disaster  (e.g.[Scenario.3](#_Scenario_3:), [Scenario.4](#_Scenario_4:) and [Scenario.5](#_Scenario_5:)) | * Serious injury or loss of life may have occurred. * Situation very difficult to manage and may be on-going. * Prolonged and serious disruption to normal business operations. * [Company] CMT will be invoked * Unable to restore services within 1-2 days |

Alert level 1 and 2 would be an Incident.

Alert level 3 and 4 would be a Crisis.

## Initial Response & Activation Procedures

In an emergency, [Company]’s priority is to preserve team safety and wellbeing before executing the Initial Response and Activation procedures.

Based on the initial assessment of the crisis, the [Company] IMT and/or [Company] CMT may be activated.

* Initial contact is to be made verbally where possible on either DDI’s or cell phones during business hours, or cell phones or home numbers outside of business hours. If the primary contact is unavailable, the alternate should be contacted immediately.
* The first respondent must notify the relevant department leaders along with all known information, who will determine the crisis level and notify the leadership team as per the Major Incident process, in [Appendix 11](#_Appendix_11:_)
* If crisis extends beyond IT, the Head of IT (or designate) will notify the [Company] CMT (if necessary).
* If the [Company] BCP is invoked, a member of the [Company] CMT will be notified.
* The Head of IT and [Company] IMT/CMT will obtain facts, determine the nature of the problem, and identify appropriate damage assessment and recovery team members, and their responsibilities.

## Mobilisation

* Head of IT (or designate) and [Company] IMT will meet in the CEOs office (Incident Management Hub) on [Location] and use the conference number (in [Appendix 6](#_Appendix_6:_)) and/or Skype/Conf call should there be a requirement to conference in other [Company] Recovery Team members.
* A communications plan will be developed which will include team communication, liaison with the CMT, any staff, family, client, supplier, and Business groups where required and appropriate.
* All communications, tasks and actions will be recorded on the Crisis Event Log. A template is in [Appendix 7](#_Appendix_7:_Crisis).
* [Company] Incident Management response must include staff wellbeing issues such as rolling shift work, managing the number of hours the team works, taking into account any personal loss and identifying any team members who may be suffering from crisis-induced stress.
* An initial action plan will be developed which outlines the damage assessment activities and the timeframe within which the [Company] Recovery Teams must report back to the [Company] IMT/CMT. This will set clear priorities and responsibilities for team members.

## IS Damage Assessment Procedures

A damage assessment carried out by member of the [Company] IMT will assess the nature and extent of any damage and to determine how the Action Plan should be implemented.

**Damage Assessment will be completed as quickly as possible with staff safety a top priority.**

The following areas will be addressed:

* Cause of crisis;
* The potential for additional damage or disruptions;
* Area affected by crisis;
* Containment of crisis;
* Status of physical infrastructure (i.e. data centre status, power availability, air conditioning, voice and data communications)
* Functional status of infrastructure (i.e. what is working, what is not)
* Type of damage to hardware or data (i.e. water damage, fire damage, physical destruction etc.)
* What needs to be replaced
* Estimated time to restore normal services
* Upon completion of the Damage Assessment, the [Company] IMT will meet back at the pre-determined location to discuss impact and determine an appropriate action plan.
* Technology Services GM (or designate) to communicate with the [Company] CMT (if required) as required
* Once the damage or disruption has been characterised, the [Company] IMT and Recovery teams will together determine the appropriate recovery strategy (action plan).

## Action Plan Development

* Develop Recovery objectives
* Identify recovery teams/members as per the Roles & responsibilities in [Appendix 9](#_Appendix_9:_BCP)
* If the crisis is expected to only cause short-term disruption and physical damage is limited to few devices, then it may be preferable to recover on site using a different device.
* If long-term or structural damage, it may be necessary to restore to our temporary, alternate location (other [Company] or home locations) for an extended period.
* [Company] Recovery Team to notify offsite tape storage that backup tapes are required (if necessary)
* [Company] IMT to notify external suppliers of execution of [Company] BCP as appropriate?
* Plan to recover pre-identified critical business services first
* Liaise with [Company] CMT if required

## Resumption Procedures

[Company] has previously determined the priority in which systems should be restored based on a BIA ([see section 4](#_The_priority_it)), and therefore these should be considered in order of restoration priority where appropriate

* Define recovery objective.
* Determine the recovery team composition if it differs per system.
* Ensure responsibilities are clearly defined.
* Plan the recovery procedures/tasks.
* Refer to individual Recovery Folders for Recovery documentation.
* [Company] Recovery team to ensure [Company] IMT/CMT are informed of recovery plans and priorities.

## Recovery Procedures

When all critical systems have been restored, non-critical business systems should then be restored.

* Execute the recovery procedures/tasks
* [Company] recovery team to ensure IS Incident Management Team are informed of recovery progress and priorities.
* [Company] Recovery team to ensure [Company] IMT/CMT are informed of recovery progress and priorities.
* Head of IT (or delegate) to ensure the [Company] CMT remains informed of recovery progress and priorities as required.
* [Company] Recovery team to audit system and ensure integrity and security are in place before advising users of availability.
* [Company] Recovery team to advise Service Desk when system are available or of any systems changes, reduction in functionality etc. so support and information can be provided to end users.

## Restoration Procedures

If resumption and recovery occurred offsite, then restoration and return to normal operations is migrating back to the old site.

* Preparation of procedures to restore or replace the original site so that normal operations can be transitioned
* Procedures that include testing the original or new system to ensure that it is functioning properly before shutting down the contingency system
* Plans should include returning any hired equipment, closing down any voice/data links and returning any other equipment to the appropriate location.
* Determining if the crisis could have been averted with the proper mechanisms in place, and implementing these if appropriate using standard change management processes.
* Updating of documentation with lessons learned and any changes to the DR plan.
* Ensure any changes to the DR plan are documented on the Document Change control sheet and approved by the Head of IT (or delegate) – see [Appendix 5](#_Appendix_5:_)
* Formal debriefing of staff and others involved.
* Filing of documentation and official closing of crisis and dismantling of the CMT and recovery teams.
* Assessment of impact on the team’s wellbeing and planned rest and recovery time.
* Assessment of the financial impact of the incident

## Communications

During a DR or BCP scenario communications to the organisation as well as customers will be critical:

### Internal Communications

Internal communications can be carried out in a number of ways and will be the responsibility of the [Company] IMT usually the designated Coordinator:

1. Communications via E-mail Is the preferred method, if E-mail is unavailable then;
2. The [Company] IMT will communicate through Yammer (assume all [Company] employees are on Yammer), if unavailable then;
3. The [Company] IMT will communicate through Skype (assume all [Company] employees are on Skype), if unavailable then;
4. [Company] subscribes to a text service, where mass texts can be sent with basic information on the outage; see [Appendix 10](#_Appendix_10:_Communcations) for details of the Communications systems.
5. The [Company] IMT Informs each member of the [Company] Leadership team who pass on messages to their respective team through calling trees, if the mobile network is unavailable then;
6. Carrier pigeons or smoke signals {to see if people read this document}

The [Company] IMT and Recovery Teams will communicate through Skype to coordinate the restoration effort.

A list of [Company] contacts is in [Appendix 12](#_Appendix_12:_) and if Active Directory is still operational then contact numbers can also be found there.

### Customer Communications

Internal communications can be carried out in a number of ways and will be the responsibility of the [Company] IMT usually the designated Coordinator, if the Crisis has been escalated this communications may be directly from the [Company] CMT (via the Chief Executive). Customer communications will be in line with contracted arrangements and will be sent at agreed intervals depending on severity and/or time of the incident :

1. The preferred communications will be via the phone/either directly with individuals or on a conference call, If this is unavailable then;
2. Communications via E-mail, if E-mail is unavailable then;
3. The [Company] IMT will communicate to the customer through Skype (will have to ensure customer Skype details are known) if unavailable then;
4. [Company] subscribes to a text service from Vodafone, where mass texts can be sent with basic information on the outage; see [Appendix 10](#_Appendix_10:_Communcations) for details on the communications service

[Company] subscribes to a text service from Vodafone, where mass texts can be sent with basic information on the progress/status of the outage; see [Appendix 10](#_Appendix_10:_Communcations) for details on the Web2txt service.

### Media communications

All media communications will be through the Chief Executive or designate. No member of [Company] may speak to the media without the permission of the Chief Executive.

### Emergency Services Communications

Communications to the emergency services will be through the designated Fire Warden (if fire is the source of the crisis). Otherwise all communications should be through [Company] CMT or IMT.

Space left for response process flow

# pandemic response activities

## Assumptions

1. It is assumed that the warning of an approaching Pandemic will be communicated over days rather than hours.
2. Non-required staff would be sent home and IT would be providing the organisation with a skeleton on site/remote support staff.
3. All projects will stop if project resources are affected by the building evacuation or to make way for critical [Company] staff.
4. All Project resources sent home and are not to use the network resources.
5. All Professional Services resources sent home and are not to use the network resources.
6. All non-essential staff to go home, where they can assist they will be seconded to IT/Support Teams.
7. The [Company] CMT will decide where to relocate critical staff.
8. All business critical staff have remote access capability, such as laptops, mobile phones and remote access (and they know how to use them).

## Actions

During the notice period leading up the announcement of a Pandemic key [Company] Operational staff (both Operations, Development and Testers) will be identified and scheduled to provide 1st, 2nd and 3rd level support remotely (for both [Company] customers and internal staff). This group will include members from:

1. Operations Teams
2. Service Desk
3. Testers
4. Applications Support
5. Some project resources

Whilst most key staff has remote working capability already ([see section.1 for a list of [Company] employees with remote access capability](#_Remote_support/access_capability)), those who do not may be issued with the VPN configuration files to enable them to work from home. However all users will be able access e-mail remotely via OWA.

The [Company] network infrastructure has been designed with a degree of high availability and enables continued support remotely (excluding the requirement to change backup tapes)

The remote support roles will be scheduled between team members of each support area ensuring 24x7 coverage.

As the number of [Company] staff will be minimal 1st level support will be provided by the Service Desk/IT Teams or 3rd party from alternate locations using support tool available via remote access.

During the lead up to the pandemic, the Service Desk will have the ability to commission/commandeer spare desktops/laptops (depending on availability) to give to critical [Company] employees as identified by the organisation should they not have remote access already. These devices can be provided to those staff at a designated point (or by whatever method the organisation decides upon at the time e.g. taken home provided they have internet access/connectivity) for remote connectivity and use during the period of the pandemic.

# ongoing operational management responsibilities

## Effective Service Continuity Management And ITIL

Using the ITIL framework there are five topics fundamental to providing effective IT Service Continuity Management. They are:

* Education and awareness
* Training
* Change Management
* Review and auditing
* Testing

This section will outline [Company]’s approach to each topic.

## Education And Awareness

Firstly, this DR Plan is to be socialised with all members of the [Company] Leadership Team and likely members of the Incident Management Team ([as defined in 3.7](#_Foster_moore_IMT)) signed off understood”.

A “**Disaster Recovery Coordinator**” is to be appointed to ensure the relevant activities occur as planned.

The relevant [Company] leader(s), supported by the Disaster Recover Coordinator will ensure that their areas of responsibility are fully understood and achievable as indicated within this Plan. This includes ensuring that regular exercises are held to ensure each team can meet the restorations requirements/timeframes as outlined in this plan.

Whilst the restoration of service is occurring regularly as part of the standard BAU operational activities, there is an expectation that service restoration would be tested at least twice a year to ensure each team is compliant to the timeframes indicated in this DR Plan. This will become part of each Leaders KPIs to ensure it occurs.

The DR Coordinator has assumed that each Business Group has its own DR/BCP awareness campaign. However, every endeavour will be made to work in with each group to aid and support their process.

## Training

The **Disaster Recovery Coordinator** will work with the relevant managers and training team to ensure annual awareness campaigns are run to educate and identify training needs of [Company] employees.

This BC plan will be part of the [Company] induction and should be read and understood by all new team members.

## Reviewing & Auditing

The Disaster Recovery Co-coordinator will be responsible for ensuring that the annual testing takes place and that any areas of risk are identified to the [Company] Chief Executive

## Change Management

It is envisaged that the all changes being made to the IT Services and their associated environments will consider the Disaster Recovery (DR) requirements at all times.

It will be the responsibility of the relevant Leader(s) to ensure that this occurs. The proposed bi-annual testing will be used to identify any areas where IT services are at risk. Again, it will be the relevant [Company] Leader’s responsibility to ensure any DR risks are mitigated. The Technology Services GM has overall responsibility for ensuring that the IS DR requirements are met for the Chief Executive.

## Testing

The purpose of testing the plan is to:

* Ensure the plan is feasible, and any deficiencies identified and addressed.
* Evaluate the ability of the [Company] recovery team members to execute the plan quickly and effectively which will also help determine specific training requirements by team members.

It is the responsibility of the [Company] DR Coordinator to:

* Prepare drills; and
* Assess reactions and prepare debriefing documentation that highlights training requirements and any shortcomings in the plan itself.

The drills will either be announced or unannounced tabletop or functional simulations.

* Tabletop – Walk through procedures without any actual recovery occurring
* Functional – Simulates a disaster scenario in a non-production environment
* Announced drill - team members are told when the drill will occur, and what the objectives and scenario are.
* Unannounced drills occur without prior notification and are helpful in preparing the team for disaster because it focuses on the adequacy of in-place procedures and readiness of the team.

Drills will address:

* System recovery on alternate platform from backups.
* Co-ordination among recovery teams.
* Internal and external connectivity.
* Restoration of normal operations.
* Notification procedures.
* Team abilities and performance in a DR/BCP scenario

The plan will be considered valid and effective if:

* Backups can be successfully restored.
* Response is within the allowed timeframe.
* Team members are aware of the specifics of the plan.
* Team members are able to perform their allocated tasks.
* The plan is up-to-date.

[Company] will perform 1 table top drill and 1 functional simulation each year.

[Appendix 8](#_Appendix_8:_BCP) contains the DR Test Plan template to be used when planning drills

# Appendices

## Appendix 1: Network Diagram

{For network Diagram}

## Appendix 2: Useful Contact Numbers

{List}

## Appendix 3: list of [Company] buildings with generator capabilities

## Appendix 4: On Call Process

{List}

## Appendix 5: Bcp Change Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Page # | Name | Date of Change | Distributed | Comments |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Appendix 6: Conference Number

To conference a number of the team you can use one of the following numbers:

## Appendix 7: Crisis Event Log

|  |  |  |  |
| --- | --- | --- | --- |
| Event or Crisis: |  | | |
| Maintained by: |  | | Sheet …… of. …… |
| Date: | Time: |  | Summary of Events or Actions Taken |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |
|  |  |  | |

## Appendix 8: BCP Planning Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Item | Action | Checked | Exists | Commentary | Date | |
| A. Administration | | | | | | |
| 1. | Agree the DR Coordinator. |  |  |  | |  |
| 2. | Agree the Backup DR Coordinator |  |  |  | |  |
| 3. | Agree members of the DR Management team |  |  |  | |  |
| 4. | Ensure [Company] CMT Team Leader is aware of key IT members |  |  |  | |  |
| 5. | Distribute copies of this plan to all relevant staff  IT  CMT members  Business Group BCP Co-ordinators |  |  |  | |  |
| 6 | Distribution List Updated |  |  |  | |  |
| B. Documentation | | | | | | |
| 7. | BCP hardcopy and electronic copies are distributed |  |  |  | |  |
| 8. | Electronic and location hardcopy Recovery documentation is known |  |  |  | |  |
| 9. | Recovery Documentation maintained and checked |  |  |  | |  |
| 10. | Supplier details maintained and checked |  |  |  | |  |
| 11. | Service contract details maintained and checked |  |  |  | |  |
| 12. | Complete hardware listing |  |  |  | |  |
| 13. | Hardware warranty details maintained and checked |  |  |  | |  |
| 14. | Software Licensing Information maintained and checked |  |  |  | |  |
| 15. | Applications maintained and checked |  |  |  | |  |
| 16. | Internal Security audits available |  |  |  | |  |
| 17. | Detailed IS Infrastructure schematics |  |  |  | |  |
| 18. | System Configurations |  |  |  | |  |
| 19. | Password Management |  |  |  | |  |
| 20. | Backup Configuration and Restoration procedures |  |  |  | |  |
| 21. | Development documentation maintained and checked |  |  |  | |  |
| Training/Schedule | | | | | | |
| 22. | IS BCP Coordinator to establish and monitor the training schedule. |  |  |  | |  |
| 23. | IS BCP Coordinator to establish and monitor the review and audit schedule. |  |  |  | |  |
| Maintenance/Audit | | | | | | |
| 24. | IS BCP Coordinator to ensure the plan is regularly updated, reviewed and distributed. (6 monthly) |  |  |  | |  |
| 25. | Review the BCP bi-annually. |  |  |  | |  |
| 26 | Test BCP scenarios regularly |  |  |  | |  |

## Appendix 9: BCP Roles & Responsibilities

|  |  |  |
| --- | --- | --- |
|  | Before a crisis | During and After a Crisis |
| DR Coordinator | Promote awareness of the BCP/DR plan within IT and [Company] Departments through training and awareness. | Meet with the DR management team on invocation of the IS BCP and act in an advisory role to ensure the plan is enacted appropriately. |
| Co-ordinate, schedule and manage regular drills and recovery planning workshops. | Maintain an events register during the crisis. |
| Audit and review day-to-day practice to ensure objectives of the BCP and recovery plans are continually met. | Act as the central coordinator and ensures communications are produced |
| Maintain a distribution record of copies of the BCP |  |
| Maintain an events register that details past events, their impact, lessons learned and recommendations to be implemented to reduce either the risk or the impact of reoccurrence. |  |
| Authority to make approved changes to the BCP and promote these changes. |  |
| Act as the central coordinator for DR/BC Plans and ensures communications are available |  |
| [Company] IMT | Appoint DR Coordinator and alternate | Determine the composition of Recovery Teams and notify them of the invocation of the DR Plan. |
| Authorise budget to ensure the BCP remains up to date. | Work with Recovery Team members to identify the most appropriate recovery method for the crisis. |
| Assist the DR Coordinator in maintaining the plan and authorising regular drills, training and testing. | Negotiate and manage contracts, consultants and external service providers where necessary during a crisis |
| Participate in drills. | Develop a communications plan and co-ordinate this with the CMT, Recovery Teams and customers as required |
| Promote awareness of the BCP/DR plan within IT and other [Company] Departments. | Manage, co-ordinate and monitor the recovery process; |
| Ensure procedures necessary to facilitate a successful Disaster Recovery are integrated into day-to-day operations | Act as a liaison between Recovery Team members and [Company] CMT, other recovery teams and users. |
| Authorisation of expenditure (up to DFA) necessary for the recovery of IT systems. | Communicate recovery efforts to users and management.  Manage stress and provide support to recovery Team members. |
| [Company] Recovery Terms | Understand the Recovery teams function | Determine the extent of damage and provide best effort estimates on recovery time to the [Company] CMT and customers; |
| Participate in scheduled and unscheduled drills and training | Provide basic Service Desk services (if the Service Desk is not available) to communicate system statuses to users. |
| Ensure backups are scheduled and completed; and recovery documentation is updated and maintained. | Recovery/Rebuilding of systems. |
|  | Ensure retrieval of data backup tapes. |
|  | Review/Audit integrity of systems and data before end users access them. |
| [Company] CMT | Direct and authorise the recovery effort | Sign off on significant expenses as a result of the crisis |
| Set policy | Ensure policies are be adhered to |
| Manage IS DR/BCP | Coordinate BCP and DR response if required |
| Accept IS DR/BCP deliverables, | Sign off on a communications plan and co-ordinate this with the IMT, Recovery Teams, media and customers as required |
| Communicate and maintain IS DR/BCP awareness with team members. | If invoked, CMT will be the central coordination point for IMT and recovery teams |

## Appendix 10: Communcations

{If required}

## Appendix 11: Major Incident Process

{Major Incident Process}

## Appendix 12: Contact List

## Appendix 13: Phone System Information



## Appendix 14: Remote Access

## Appendix 15: Off Site Storage

One risk response method is to ensure all vital data is backed up and stored off-site. Once the recovery strategy has been defined, an appropriate backup strategy should be adopted and implemented to support it. The backup strategy must include regular (probably daily) removal of data (including the CMS to ease recovery) from the main data centres to a suitable off-site storage location. This will ensure retrieval of data following relatively minor operational failure as well as total and complete disasters. As well as the electronic data, all other important information and documents should be stored off-site, with the main example being the DR and Business Continuity plans.

## Appendix 16: Data Centres

Currently [Company] has 3 Data Centre locations:

Data Centre 1

Data Centre 2

AWS Data Centre 1