Disaster Recovery Plan

Version # 1.0

22 September 2015

Contents

**Document Information**

Purpose:

* To provide a concise summary of DRP
* To identify systems, resources and operational activities & procedures required to maintain and restore Blueprint application
* Identifying tasks required to successfully ‘fail over’ Blueprint application in the event of a disaster

This document is intended for:

* Support Analysts
* Technology Managers

1. Document Purpose 4

1.1. Primary Systems 4

1.2. Secondary Systems 4

1.3. Document Structure 4

2. Plan Documentation Management 6

2.1. Plan Storage 6

2.2. Off-Site Plan Copies 6

3. Plan Accountability & Maintenance 7

3.1. Accountability 7

3.2. Responsibility & Accountability Matrix 7

4. High Level Architecture 9

4.1. Primary Site 9

4.2. Redundant Site 9

5. Recovery Time Objectives 10

5.1. Key Production Systems & Devices 10

6. BCP Scenarios 11

7. Testing The Plan 12

8. Appendices 13

8.1. Acronyms and Abbreviations 13

# Document Purpose

The goal of this Disaster Recovery Plan *(“DRP”)* is to re-establish the Blueprint application environment in the event of a significant system failure.

Key areas of consideration include:

* Network components
* Database servers
* Web servers
* Data preservation

The DRP is an IT owned plan and is not to be mistaken with the corporate business contingency plan (“BCP”).

## *Primary* Systems

A primary system is one that is deemed business critical in making the **Blueprint Application** available for access.

## *Secondary* Systems

A secondary (non-critical) system is one that is deemed unessential during a period of disaster recovery.

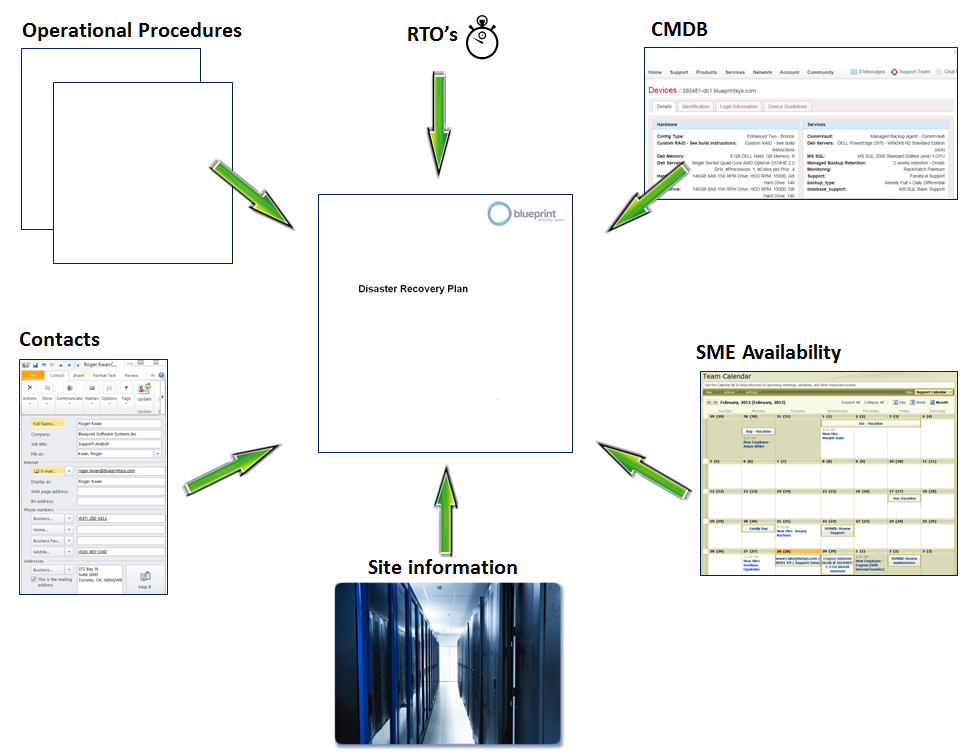
## Document Structure

This document will serve as DRP for Blueprint Application. This document should be linked to the following resources;

* Recovery Time Objectives (RTO’s)
* Configuration Management Database (CMDB)
* Software License Information
* Vendor Contacts
* Operational Procedures
* Subject Matter Expert (SME’s) contact information
* SME availability
* Redundant deployment information

### Document Structure

The diagram below depicts the DRP document being the aggregation point for different data sources and documentation sets.



# Plan Documentation Management

This DRP contains links to the resources that should reside in disaster recovery site.

## Plan Storage

The plan resides in PDF & MS Word format. The plan document will be reviewed and updated periodically.

## Off-Site Plan Copies

The DRP along with other required resources and documentation should be encrypted and distributed to by the plan owner to those responsible for recovery activities. The plan owner is also responsible for the retrieval, updating & reissuing of the encryption keys.

### Encryption & Password Control

The plan owner is responsible for encrypting the documents on the USB keys, prior to distribution. The password will be known to IT Managers & Team Leaders only and will be provided to resources holding keys on an ‘as needed’ basis.

# Plan Accountability & Maintenance

## Accountability

An individual designated as Disaster Recovery Officeris deemed accountable for the plan.

The DRP plan consists of this document and all references made to other documents or resources deemed essential to reestablish application operation.

The plan may reference, via ‘HTTP’ links, *‘living’* documents and resources that are maintained by those accountable.

Living documents / resources are essential to support service restoration but are managed outside the DRP.

These documents or resources are assigned to ‘owners’ (managers, administrators, vendors) to ensure they remain current. Their personal objectives reflect this responsibility.

## Responsibility & Accountability Matrix

Those responsible for key documents or resources required in supporting DRP are detailed in the following sample RACI chart.

Abbreviations used in the chart are as follows:

**R = Responsible**

**A = Accountable**

**C = Consulted**

**I = Informed**

**DRO** – Disaster Recovery Officer

**ITM** – Information Technology Manager

**SSA** – Systems Administrator

**DBA** – Database Administrator

### Sample RACI Chart

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **DRP Component** | **Elements Included** | **CTO** | **ITM** | **SSA** | **DBA** |
|  |  |  |  |  |  |
| Plan Document | Nucleus doc / references all other resources | A | R | C | C |
| Operational Proc's | Required for each service recovery activity |  | A | R | R |
| CMDB | Details all items referenced by the operational procedures |  | R | R | I |
| SME Contacts | Register of resources & skill sets required to recover services |  | A | C | C |
| Site Information | Details of facilities |  | C | A | C |
| RTO's | Recovery Time Objectives to support Blueprint Customer Service Level Objectives | A | R | C | C |

The purpose of RACI chart is to aid IT Management in appropriately assigning document or resource ownership.

# High Level Architecture

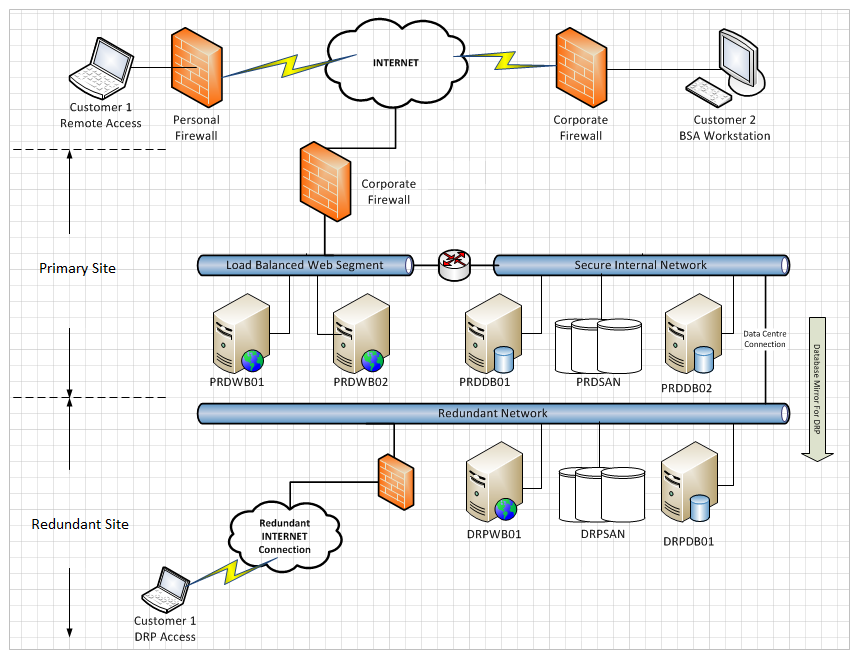
The diagram below illustrates the example of high level Blueprint application configuration.

## Primary Site

Under normal operations, customers connect to the Blueprint application via a unique URL. Inbound connections are load balanced using a BIG-IP unit from F5 Networks. Connections are routed to a web server (for example: PRDWB01) running IIS and an instance of Blueprint. Once authenticated, users update their ‘projects’ via a clustered MS-SQL database server (for example: PRDDB01). Data is then stored on the Storage Area Network (for example: PRDSAN).

## Redundant Site

In the event of significant failure at the Primary site, customers will be re-routed to the Redundant site network. At close to real time, production data in primary site is mirrored to redundant site.



# Recovery Time Objectives

This section provides the reader with an indication of the importance of key systems and devices, essential for supporting normal operations.

## Key Production Systems & Devices

The table below details devices that form the sample infrastructure.

**System / Device** = assigned system or device common name

**Function** = the function of the device within the architecture

**Impact** = impact value 0 through 3 should the device not be available for some reason

0 = No impact

1 = Minor impact

2 = Major impact – failover decision required

**RTO** = Recovery Time Objective in minutes

### Sample System Impact Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Function** | **Impact** | **RTO (mins)** | **Notes** |
|
|  |  |  |  |  |
| **PRDWB01** | Web Server | 0 | Instant | PRDLB01 will handle traffic routing in the absence of a PROD web server |
| **PRDWB02** | Web Server | 0 | Instant | As PRDWB01 - we anticipate additional web servers (WB03, 04, etc..) will be added to the infrastructure as the number of subscribers to the service increases |
| **PRDDB01** | Database | 1 | 1 (Auto) | Cluster will handle failover to DB02 |
| **PRDDB02** | Database | 2 | 240 (Manual) | While PRDDB02 is master - PRDDB01 is being restored If PRDDB02 fails while PRDDB01 , failover to DRP site is required |
| **PRDAD01** | Active Directory | 1 | 1 (Auto) | Could be up to 1 min re-connection as AD02 is called No new primary accounts can be created |
| **PRDAD02** | Active Directory | 2 | 120 (Manual) | If either AD1 or AD2 is off-line unplanned, the creation of AD3 should be initiated |
| **PRDSAN** | SAN | 2 | 120 (Manual) | If SAN fails, Failover to DRP site is required |
| **DRPSAN** | SAN | 0 | N/A | Risk is very low that both PRDSAN & DRPSAN would be off-line simultaneously |
| **PRDLB01** | Load Balancer | 2 | 240 | If LB1 fails, customers are instructed to use DRP URL or directed to specific web server |

# BCP Scenarios

This DRP considers only the following scenarios. Standard Operation Procedures (SOP’s) exist to recovery systems primarily to support the disaster scenarios described below:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Scenario Number** | **Disaster Description** | **Customer Impact** | **Decision Required** | **Decision Team** | **Notes** |
|
|  |  |  |  |  |  |
| **DRP01** | Primary location fails / web access to service is lost | Access to Blueprint application and customer data impacted for a period > 4 hours | Failover to Redundant location? | CTO  SSA DBA | Customers will be instructed to use alternate URL |
| **DRP02** | SAN fails in Primary location | Client data off-line for a period > 4 hours | Failover to Redundant location? | CTO  SSA DBA | Impact as per DRP01 however forecasted recovery time would be less which may alter decision |
| **DRP03** | Active Directory (PRDAD01/02) fails in Primary location | Client data off-line for a period > 4 hours | Failover to Redundant location? | CTO  SSA DBA | As per DRP02 |
| **DRP04** | Redundant location off-line | Primary location is providing service but the DRP site has been lost | Establish alternate DRP site? | CTO  CFO  CEO | For the duration that Redundant location is off-line, any impact to the primary site would jeopardise access to the application, Risk = Low |
| **DRP05** | PRDLB01 fails in Primary location | Client data off-line for a period > 2 hours | Bypass LB01 / provide IP Addr? | CTO  SSA DBA | Customers may remain impacted until any required firewall rule changes are completed to permit the new IP |

# Testing The Plan

The DRP should be tested regularly. However, in the event of a material change to the plan, a test of the plan should be scheduled at the earliest convenient date.

A material change may include but is not limited to the following;

* A change to the location of primary components of the architecture;
* A change of key vendors as providers of key services;
* A change of resources that hold key roles identified in this document, e.g. DBA.

# Appendices

## Acronyms and Abbreviations

|  |  |
| --- | --- |
| Acronym / Abbreviation | Description |
| BCP | Business Continuity Plan |
| BPM | Business Process Management |
| DRP | Disaster Recovery Plan |
| RACI | Responsibility & Accountability Matrix |
| SOP | Standard Operating Procedures |

**Privacy Information**

This document contains information of a sensitive nature. This information should not be given to persons other than those who are involved in the disaster recovery planning or plan execution.

End of Document