Information Security Management System
Procedure for conducting DR drills

Document no. JMBGRP/ISMS/PR-DRD

Version no. v1.2

Document details

Classification	Internal	
Released date	05.12.2017	
Description	Procedure for conducting disaster drills in controlled environment	
Custodian	Corp IT Dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT dept.	

Distribution list

Name
To all locations of JMB group.

Version History

Version no.	**Version date**	**Approved by**	**Comments**	**Signature**
v1.0	28.08.2018	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	10.01.2019	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	08.02.2020	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	11.02.2021	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.1	25.03.2022	Manish Jaiswal (Group CTO)	Logo changes done in this policy	
v1.2	18.08.2023	Manish Jaiswal (Group CTO)	Report attached in this policy	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Document reviewed. Modifications done in Section: “General Procedure, User Drill”	

Contents

Purpose

The purpose of this document is to have a standard operating procedure for conducting systematic disaster recovery drills. It assures the disaster drills are conducted in controlled environment with appropriate steps taken and avoid erroneous.

Objective

The disaster drill is the proactive measure to ensure the preparedness towards the location specific disasters and to minimize or to eliminate the impact over business.

The primary objective is, to ensure that the business shall not suffer due to natural or manmade catastrophes that result to non-availability of business-critical applications.

Secondly, the existing application specific disaster recovery plan to be verified for its appropriateness. It ensures that the business will not suffered in real disastrous situations and IT dept. will not face any last-minute surprises or lack of readiness while dealing with any disaster.

Thirdly, valuable business time can be saved on recovery procedure and systems shall made available with less time and perform efficiently.

Scope

The procedure is applicable to all business-critical applications of JMB group of companies.

Exception

The disaster recovery scenarios exclude situations like national disasters i.e. war (both conventional and nuclear). No drills will be conducted on this scenario.

Procedure

General

All business specific applications are covered in respective disaster recovery plans and ensure the systematic approach to deal with disastrous situations.

– Corporate IT dept. creates the yearly schedule for conducting application DR drills which are broadly categorized as administrative drills and Full (User) drills.

– The administrative drills are conducted on half yearly basis, wherein full drills are conducted on yearly basis. Drill frequency may be revised based upon requirement or criticality of the application.

– The application owners from IT dept. in consultation with respective business owner, Corporate IT, DR site owners & application vendors (If any) combinedly decide the suitable date for conducting drill.

– Application owner documents plan of action (POA) for DR drill, it consists the identification of pre-requisites i.e. all required details for performing the drill which is discussed amongst all stakeholders as well as prepare RACI matrix for conforming the roles of each DR activity partner.

– POA constitutes the following;

a. Pre-requisites
    i. Software availability and requirements
    ii. Hardware availability and requirements
    iii. IT HW & SW support
    iv. Procurement, if any
    v. Expertise to perform some of the activities and their availability
    vi. Responsibility
    vii. Timeline
b. Activities Phase – I (Switchover)

i. Stoppage of primary site
    ii. Activities to Switch application to DR site
    iii. Handover for verification of successful switchover
    iv. Application verification with necessary screenshots as evidence
    v. Confirmation to switchback
c. Activities Phase – II (Switchback)
    i. Stoppage of the DR site
    ii. Activities to switch application to production site.
    iii. Handover for verification of successful switchback
    iv. Application verification with necessary screenshots as evidence
    v. Confirmation for end of activities
d. Post drill
    i. Preparation of IT Drill Report
        1. RCA in case of drill failure

2. Reporting recommendations & actions, assigning responsibilities and define target dates for closure.
3. Summarizing the DR and take away from the drill (learnings)
4. Annexing all evidence to report

– The downtime announcement with its specification sent to impacted business at least 7 days prior to respective application users, DR site owner and application vendors (if any) to enable DR participants to plan their activities well in advance (notification format is annexed).

Administrative drills

The notion of this drill is to ensure the disaster recovery plan is efficient, effective and verified by application owner.

Who is involved in the administrative drill?

- IT dept. (Application Owner)
- Application vendor (if any)
- DR site owner/vendor
- DB owners/vendors
- Business (in case any special approval required)

How to conduct administrative drills?

1. Application owners plans the administrative drill based on the schedule.
2. Application owner and DR site owner (e.g. Sify, ESDS, AWS etc.) confirms the success of data availability as per RPO (Recovery Point Objective) before doing switchover activity.
3. Only if the data is available as specified in RPO at DR site, IT dept. proceeds for further activities, in case of any deviation from intended result, the DR process will be aborted and system will be switched back to production site and initiated for use.
    a. Details of failures to be reported in the IT Drill Report format and initiate root cause analysis with respective stakeholders.
4. On the successful backup, the DR will be performed as stated in POA.
5. IT dept. follows the steps to confirms appropriateness and records the following;
    - Ping response - Verification of reachability and network establishment success
    - Application access and screenshots

- DR server event log
- DR application event log

6. On the success, IT dept. activates primary site and initiate switchback from DR site to Primary site.
7. IT dept. (application owner) records each step performed in the drill with time in IT Drill format.
8. Importantly Application owner assesses the RTO (Recovery Time Objective) success of actual time of recovery vs business expected recovery time.

User Drill (As per Business Requirement/ Approval)

The notion of this drill is to ensure the disaster recovery plan is efficient, effective and verified by user.

Who are involved in the Full (User) drill?

- IT dept. (Application Owner)
- Application vendor (if any)
- DR site owner/vendor
- DB owners/vendors
- Business (in case any special approval required)
- Actual users of the application

How to conduct full (user) drills?

1. Full drill carries the same attributes as administrative drill and stated general procedure, with the following additions/changes;
   - Actual application users key in data in the application after switching to DR site.
   - Application will be operational through DR site for at least 2-3days. Where User will actually perform day to day activities on application.
   - On the completion of drill, Application Owner (IT dept) initiates the data restoration to primary site.
   - DR site owner confirms the completion of data restoration on primary site and stops the DR site.
   - Primary site will be restored and user will confirm if the data is available as obligatory.
   - Based on the confirmation received from users, application owner stops the drill.

- Application owner assesses the RTO (Recovery Time Objective) success of actual time of recovery vs business expected recovery time.

Evidence

- Screenshots of all key activities
- POA (Plan of action)
- Screenshots of failure
- Backup & restorations logs

Performance indicators

- Effectiveness of POA
- RTO vs actual time of performing drill
- RPO vs actual data backed up

Annexure

Annexure I - IT announcements notification

JMBAXI , IT Department

NOTIFICATION		
Notification Type	Affected Business	Impacted Location
Planned/unplanned/Restoration	*Multiple*	*Multiple*
Start Time	End Time	Duration
Date, Time	*Date, Time*	*…….Hrs*

Technology Domain	*Network/Infrastructure/Telecommunication etc.*
Affected Service	*List of services*
Impact	*Single/Multiple users*
Description	*E.g. During the outage period, users may face **intermittent** disconnection of internet & network.*
Reason	*Define reason for outage*
CR No	*Reference change no.*
Additional Information	*If any*

We apologize for the inconvenience caused to you and look forward to your support on the same.

Please note:

In case of **Unplanned** outage notification strip will be of 'red' coloured.

In case of **Planned** outage 'notification' strip will be of 'yellow' colored. (as currently shown in above notification.

On **completion/restoration** of outage, notification strip will be of 'green' colored.

Annexure II – Plan of action (POA) template

_POA (Server Migration) .xlsx

POATemplate_v1.0.xlsx

Annexure III – IT drill report template

ITDrillReport (Portall_Migration).d

ITDrillReport.docx