MINISTRY OF SECURITY

BUSINESS CONTINUITY PLAN

TEMPLATE

DOCUMENT MANAGEMENT INFORMATION

Document Title:	Business Continuity Disaster Recovery Plan
Document Number:	ORGANISATION-BCDR-PLAN
Document Classification:	Internal Use Only
Document Status:	Approved

Issue Details

Release Date	
Approved By	

Revision Details

Version No.	Revision Date	Particulars	Approved by
NA	NA	NA	NA

Document Contact Details

Role	Name	Designation
Author		
Reviewer/ Custodian		
Owner		

1 INTRODUCTION

This Business Continuity Planning (BCP) document outlines the procedures required of ORGANISATION. (Hereinafter referred as "ORGANISATION") to ensure the continued operation of the processes setup as part of its Business needs.

These procedures are intended to reduce or eliminate negative business impact by:

- Identifying the triggers that will pinpoint the need to activate continuity efforts;
- Prescribing actions to respond to the incident, expedite recovery, and restore services;
- Providing for continuity of ORGANISATION's processes at recovery facilities, if any;
- Identifying key persons involved in the business process,
- Mitigating the chances of downtime of cloud services by having distributed instances across other locations.

This BCP is owned by the ORGANISATION BCM and will be reviewed annually for needed changes and ensuring the accuracy of the data and this BCP will be updated with any changes in personnel, equipment, facilities and business processes.

2 SCOPE OF PLAN

The scope of this BCP is limited to the business continuity and disaster recovery procedures for ORGANISATION processes identified within this document.

This BCP covers:

- Full or partial destruction of the ORGANISATION site.
- External threats to the primary location, impeding staff's ability to enter the building.
- Technical disasters, such as equipment/network failure, or data corruption.

3 AVAILABILITY OF THE BUSINESS CONTINUITY PLAN

Business Continuity Management Committee approved copies of this document will be available with the Executive management, process owners and all the critical human resources identified to be working in the business continuity scenario as ready reference and with intended Business Continuity Management.

4 RECOVERY OBJECTIVES

In order to ensure the Business continuity, ORGANISATION will ensure that the critical staff will resume work from *<mention the location>*

ORGANISATION Physical Primary facility: *<To Be Filled>*

ORGANISATION Physical Secondary facility: *<To Be Filled>*

At ORGANISATION, the business continuity team will be composed of operations leaders who will be instructed by the ORGANISATION BCM to organize and assist the critical resources including the staff in resuming the critical services at the secondary site.

5 Non BCP/DR Situations Or Normal Situations:

In order to meet Business Continuity Management Objectives, the following will be in order before an incident:

- ORGANISATION facility is equipped with standby power supplies using UPS, backup diesel generators with 48 hours of fuel for uninterrupted power supply. The ORGANISATION team operates on cloud based servers and third party providers are responsible for ensuring fast recovery of IT infrastructure and data. Critical staff/resources will be identified for the recovery team and their contact details will be shared with client managers.

- Evacuation drills will be conducted by an external agency periodically and results will be shared with ORGANISATION and any needed clients.

6 During An Incident (BCP/DR Situations):

Once the BCM declares and invokes the BCP/DR plan, the following activities are performed by the IT support team for facilitating the infrastructure for ORGANISATION operations:

- All critical resources will be trained and made to follow proper online security measures. The critical resources will be asked to report from secondary location or to the nearest safe location in case of any crisis.

- Incase critical resources moved to their home location, VPN will be configured to allow connectivity to the authorized personnel, through internet

- The code SVN /CVS that is automatically backed up on the cloud will be available for restoration on a real time basis.

- The production environment is instantly available to the designated users as it is on the Cloud, emails and intranet would be available to users as it is a cloud based location.

- ORGANISATION IT support will provide the necessary IT support wherever additionally needed.

- Any changes to or deviation from standard processes/procedures will be immediately communicated by the ORGANISATION BCM

- In the event that the BCP is invoked, and work is transitioned between Primary and secondary locations, the coordination for restoration of operations will be prioritized based on the criticality of each activity /process.

7 After An Incident (BCP/DR Revoked):

- The work area and workstations at the ORGANISATION primary location will be restored back to normal state as defined in the NORMAL SITUATIONS section.

- Upon revocation of BCP, and resumption of normal operations from the primary location, a formal communication will be sent to clients by the BCM or alternate regarding the restoration of services, revocation of BCP and resumption of the work at the primary facility. This communication will bring closure to all BCP activities.
- Firewall configurations will be restored to normal.

8 Plan Assumptions

This BCP makes the following assumptions:

- All issues of immediate staff safety and well-being will be addressed.
- Staff will be available from secondary location at time of crisis.
- Important telephone numbers mentioned in this document would be reachable throughout the outage time and would act as the points of contact for their respective functions as part of the BCP.
- All departments and branches outside the affected location are fully functional and able to support recovery/continuation efforts.
- The personnel and management structure required to execute the plan are available.
- Services are available from all the third party service providers as and when required and remain unaffected.

9 Plan Activation

The Business Continuity Plan will be activated by the ORGANISATION Business Continuity Manager (BCM) or alternate in conjunction with the ORGANISATION management team and affected ORGANISATION business contacts.

10 Building Evacuation Procedures

In the event of the need to evacuate the ORGANISATION site, employees will be moved to the safe area. This area is designed to keep employees away from potential danger and to establish a single location for determining if all the employees have been safely evacuated.

Safe Assembly Location: *Next to Main security gate (at the building entrance)*

The ORGANISATION Business Continuity Team plays a key role in evacuation of the site by performing the below duties:

- Directing all personnel at the site to the emergency exits.
- Keeping all personnel calm during the crisis.
- Keeping personnel moving toward the exits at a steady pace.
- Directing personnel to an alternate exit when an evacuation route is blocked.
- Checking all areas to ensure that all personnel have been evacuated.
- Assembling personnel in the designated safe area for a head count.

- Informing the Business Continuity Manager of any personnel that might be missing.
- Ensuring that no one re-enters the building.
- Allowing personnel to re-enter the building only after the Business Continuity Leader (BCM) has given the authorization to do so.

The following activities are performed as part of the Tasks and Responsibilities document:

- Account for all personnel that were on the site at the time of the incident.
- Report on injuries and missing personnel.
- Secure transportation to hospitals.
- Advice next of kin if there are any casualties.

11 THREATS AND MITIGATION ACTIVITIES

Threat	Response Planning	Mitigation Activities
Fire	• Identify the Fire and save/remove the nearby flammable things/objects • Inform to your Supervisor/Manager immediately/Facility & Admin • Evacuate Employees to safe place • Try to extinguish it with the nearest fire extinguisher, only if you have trained to do or if you are a ERT member • Inform to Authorities of the incident • Assemble at the safe assembly zone	• Identification of processes and materials which could cause or fuel a fire or contaminate the environment in a fire in the facility • Facility being inspected for fire hazards on a regular basis • Fire prevention and protection measures. • Distribution of fire safety information to all the employees • Conduct Evacuation drills periodically • Post maps of evacuation routes in prominent places • Provide safe disposal of smoking materials • Fire extinguishers at all the prominent places • Fire alarm, smoke detectors and sprinkler systems in all the floors • Training of key personnel on fire safety systems • Preventive maintenance schedule for ensuring all equipment's operating safely
Flood	• Evacuate the employee with proper safety measures • Domestic support Plumbing & Building verification to be conducted periodically from the Landlord	Precautions are to be taken with the help of the Building management system to mitigate any eventualities that may second the cause. • Warning and evacuation procedures for the employees

		• Backup systems: portable pumps (to remove excess water), battery powered emergency lighting, power sources (in case of power outage) • Check valves to prevent water coming from utility and sewer lines • Regular inspection of building for any structural deterioration • Plumbing system with backflow valves • Backup water supply
Bomb Threat	• Report any suspicious things/person in the Organisation Facility to your Manager/HR/Facility & Admin department • Evacuate the building and Guide other employees to safe zone • Don't re-enter the building • Report to the incident to Law Enforcement Department immediately	• Policy on handling bomb threats • Employee communication on company's plan of action in the event of a bomb threat • Training employees on how to handle Bomb Threat scenarios • Internal security measures • Bomb threat checklist
Riots	• Intimate about the Riots to HR & Operations team • Possible avoid employee coming to office, ensure proper evacuation arranged for the employees in office • Report to the incident to Law Enforcement Department • Get the confirmation of employee reached safely to their place	• Internal emergency communication procedures in place • Formal building access procedures in place • Internal security measures • Establish business contingencies with suppliers • Personnel safety and evacuation plan
Public Infrastructure – Electrical Power	• Security person to ensure DG is in Auto mode always • Minimum 30% Fuel should be maintained	• UPS power backup in case of power outage • Backup power generators with 72 hours of fuel stored locally. • Agreement with vendors for consistent supply of fuel during crisis
Public Infrastructure – Transportation	• Admin & Facility team should provide the user access to Cab Vendor Portal • Employees are empowered to book the cab through the Vendor Portal • Employees must carry the ID card while travelling on Official work	• Relationship with multiple vendors • Overnight stay or early pick up for critical resources • Liaison with local government transport authority
Pandemic	• Screening of Employees. • Allowing after thermometer checking of all employees and	• Medical examination for the employees

	contract staff shall be done on a daily basis in the morning before entering office at the entrance. If it is beyond 99°F, they will not be allowed to enter the workplace and the person will be sent home immediately. • Daily Disinfection	• ORGANISATION identified Doctor to be stationed inside the campus • Educating employees • Safe handling of trash, use of disinfectant cleaning products in restrooms, Dormitory, break rooms, Pantry and other common areas or facilities • Use accepted disinfection processes and procure supplies to minimize the spread of the contagion • Provide sufficient and accessible infection control supplies (e.g. hand-hygiene products, tissues, disinfecting wipes, surgical mask and receptacles) in work locations for employee use • Examine current cleaning services, food services, and maintenance contracts, in case those service providers are severely impacted • Disinfection of affected work areas • Deploying of antibacterial and antiviral cleansers inside the site • Minimal face to face interactions among employees
Nature/ Environment – Earthquake	• Evacuate the Building with the Fire & Safety Measures • Assemble at the Safe assembly point • Intimate to your superior & Family member of your position • Report to the incident to Law Enforcement Department • Get the confirmation of employee reached safely to their place	• Regular inspection of buildings for structural deterioration and timely repair • Anchoring with the building owner on all structures and tanks to the foundation • Inspection of non-structural systems such as air conditioning for any potential damage on a regular basis • Identification of any items that could fall, spill or break/move during an earthquake • Processes for storing hazardous materials in a safer place inside the site
Information Systems Disruption – IT infrastructure	• Redundant double ISP connection • Redundant switch for network distribution • Redundant AP (standby) for wireless network connectivity • Wired connection are ready in case of Wireless fails	• Connectivity is established through redundant service providers and established routing protocols, should there be a disruption in the connectivity at the primary site of ORGANISATION. • Backup systems available in case of any system failure

12 Plan Testing

An untested plan can often be more of a hindrance than help. The ability of the BCP to be effective in emergency situations can only be assessed if rigorous testing is carried out in realistic conditions. The BCP Testing Phase contains important verification activities, which should enable the plan to stand up to most disruptive events.

The BCP should be tested within a realistic environment, which means simulating conditions, applicable in an actual emergency. It is also important that the persons who would be responsible for those activities in a crisis carry out the tests.

13 Plan Maintenance

It is necessary for the BCP updating process to be properly structured and controlled. This would include an evaluation of the Disaster Recovery Plan (IT Plan) for potential change due to the dynamic nature of the threat population and system configuration

Whenever changes are made to the BCP they are to be fully tested and appropriate amendments should be made to the training materials. This will involved the use of formalized change control procedures under the control of the BCP Team Leader.

The following form should be used for the request and approval of such changes. Following approved changes to the plan, it is important that the BCP leader, BCP recovery team, Executive Sponsor and the IRM are kept fully informed.

14 Incident Management

Incidents occurring at the ORGANISATION primary site will be managed by the ORGANISATION Business Continuity Team in conjunction with ORGANISATION management team and affected client business unit contacts.

On completion of any incident, that impacts delivery of normal service, the BCP Team should prepare an incident analysis on your BCP plan. This is to assess the adequacy of the plan and any deficiencies.

The principal overall objectives in conducting the post incident analysis are to; verify that the business recovery/resumption plans are current and up to date, that the recovery/resumption plan performed effectively and recovered the affected functions, identify areas of the plan to improve, evaluate the flow of communications, and evaluate the effectiveness of the plan.

APPENDIX

15 CRITICAL CONTACTS

NAME	ROLE	CONTACT

16 LOCAL EXTERNAL KEY CONTACT LISTS

	#	ENTITY	CONTACT
Primary Location	1	Hospital & Trauma Care	
	2	Medical (Ambulance Service)	
	3	Police	
	4	Fire	

17 EMERGENCY RESPONSE ASSIGNMENTS

	#	TASKS	ASSIGNMENT
Primary Location	1	Accounting for All Personnel at the time of incident	Emergency Response Team
	2	Obtain Reports on injuries and missing personnel	Emergency Response Team
	3	Secure Transportation to Hospitals	Emergency Response Team
	4	Advise next of kin if there are any casualties	HR Team
	5	Immediate Human Resources	HR Manager
	6	Public Relations and Communications	Manager at CEO's Office
	7	Direction Business Continuity Team	Business Continuity Manager

	8	IT/Telecommunications	CISO
	9	Directing Alternate Site Invocation	Business Continuity Manager
	10	Client Contact	Customer Success Team
	11	Supplier Contacts	Supply Chain Lead
	12	Redirect eMail	Systems Admin
	13	Advise Insurer	Manager at CEO's Office

18 Mission Critical Activities

KEY BUSINESS AREA	BRIEF DESCRIPTION OF BUSINESS PROCESS	MAIN DEPENDENCIES

19 Back-Up, Recovery and Resumption Strategies

ESSENTIAL ACTIVITIES	SCHEDULED/ANTICIPATED OUTAGE Generally < (Time Frame?)	UNSCHEDULED OUTAGE – Short Duration < (Time Frame?)	UNSCHEDULED OUTAGE- Long Duration > (Time Frame?)
(Name Activity Here)			
Potential Disruption			
Potential Impact:			
Recovery Strategy			
Resumption Strategy			

20 Incident Management Template

Date of incident:	Time:
Description of incident:	
What critical function/functions were interrupted during this incident?	
Did your BCP address the recovery of the interrupted critical function effectively?	
If not, what areas of the recovery plan can be improved?	
Did communication flow effectively?	
Where there any problems getting or receiving communications?	
Where all phone numbers accurate and available?	
What changes need to be made to the BCP?	
Who will be making the changes to the plans?	
Will changes need to be tested?	

21 CRITICAL VENDORS

NAME OF VENDOR	SERVICES PROVIDED	NORMAL CONTACT DETAILS	EMERGENCY CONTACT DETAILS

<END OF DOCUMENT>

FOLLOW US ON LINKEDIN FOR MORE FREE TEMPLATES

PLAYBOOK MADE WITH ❤ MINISTRY OF SECURITY