Business Continuity Plan Development – Departmental Level

Critical Applications and Data Backup Strategies

Critical Application Name	RPO (BIA Outcome)	DR in place	Backup Frequency
Fraxium	1 Hour		
Cortex XDR	1 Hour	SaaS	Check with Harshvardhan
Trellix – DLP – to be removed	1 Hour		
Fortinet	4 Hours	High Availability (HA), Production in Mumbai, DR in place (at CHiS) in Bangalore	Daily

Response & Escalation Matrix

This entails predetermining the individuals accountable for prompt incident management and those to whom the incident should be escalated if it persists unresolved.

IT Processes

Types of Disruption	Level	Classification	Informed By	Informed To
Minor	Level 1	Affects a single user or minor functionality without affecting core services		
	Level 2	Involves more than one user with slight impact		
Moderate	Level 1	Affects limited areas of service or a specific function causing minor operational delays		
	Level 2	Affects multiple users or functional classes or specific application function		
	Level 3	Impacts multiple services or moderate loss of functionality affecting productivity		
Major	Level 1	Causes major disruption to key processes with significant impact on operations but no operational downtime and moderate financial impact		
	Level 2	Affects a critical application or function essential to operations, impacts multiple teams		
	Level 3	Significant disruption with immediate impact on operational downtime and moderate financial impact		
Critical	Level 1	Complete disruption with immediate impact on mission-critical services affecting entire operations		
	Level 2	System or service-wide failure having essential business functions and impacting large user base		
	Level 3	Total operational failure, severe business impact extensive financial and reputational loss		

Training & Awareness

FRP training programs shall be conducted by the Department Heads annually with the following objectives.

This document shall be maintained by respective owners, updates include version control and a comprehensive log of any changes made. This will be complemented by a clear process for updating the plan in response to test results or regulatory changes, and the following timely adjustments that reflect the latest insights and operational needs. Regular reviews will be scheduled to facilitate these updates, ensuring that all team members are informed and aligned with the most current information.

Recovery Objectives and Prioritized Activities

RTO and MTPD for each critical process are essential to effective business continuity planning.

Name of the critical process	Recovery Time Objective	Maximum Tolerable Period of Disruption
End User Computing Management (Critical Business Systems/Applications Support)	1 hour	8 hours
EOD / BOD activity	1 hour	4 hours
Security Operations Center	4 hours	12 hours
Data Loss Prevention - IS	4 hours	12 hours
Network operation center management (Firewall)	4 hours	12 hours
Cyber Crisis Management - IS	4 hours	8 hours
Database Administration	1 hour	4 hours
Data Centre Management - (Backup Service Management (Service), Sify Managed Service, Patch Management)	4 hours	8 hours
Capacity Management	4 hours	8 hours
Identity and Access Management	1 hour	4 hours
DR management	4 hours	12 hours
Privilege access management	4 hours	8 hours

Roles and Responsibilities

Detailed Responsibilities of Governance team are mentioned below:

Role	BAU Responsibilities	Crisis time Responsibilities
Board	• Exercise oversight in the BCM development, maintenance, and implementation • Review and endorse at least annually the organization's: ○ Critical business functions, business continuity objectives and the level of tolerance for risks • Ensure that adequate resources (e.g., budget, technology, and staff) are allocated	• Provide independent oversight to ensure that organization's response to the crisis is consistent with its core values and purpose

Role	BAU Responsibilities	Crisis time Responsibilities
Operational Risk Team	• Ensure effective implementation of BCM through established policies, processes, procedures and infrastructure capabilities and exercises • Provide strategic direction and approve the BCM annually and prioritize • Conduct BCM review meetings • Ensure that the Risk Team members is with BCP team for delivery to help ensure responsibilities • Approve the BCP schedule and activities • Ensure the adequate participation and engagement of all business units including senior management • Ensure that the Risk, recovery strategy and plans is implemented with required departments and that it is exercised and maintained • Ensure timely closure of the action plans raised from exercises, reviews and audit processes	• Conduct the discussion for assessing the crisis and provide guidance to teams • Continuously assess and adjust the composition and effectiveness of the teams during the crisis • Escalate the crisis to the Board necessary and coordinate the flow of information to Board • Formally declare return to normal operations post consultation with the FR team • Execute the crisis response, take responsibility for the recovery process • Maintain orderly communication and management information and decision-making during a crisis • Gather current data and consult with BCSC as necessary • Collate inputs on the incidents from the FRP Coordinator from the respective vertical/functions
FRP Coordinator	• Coordinate the initiation and approval of BCM schedule (i.e., activities and resources required) • Facilitate the approved BCM schedule and activities • Execute periodic reviews of the business continuity plan, implement the approved recovery strategy and ensure that the plan is in line with other departments priorities • Coordinate the implementation, testing, and exercise of business continuity plans • Implement the action plans raised from exercises, review and audit processes	• Serve as first level of escalation point and on-ground recovery team • Escalate the incident to the business risk governance team • Provide regular updates and incident assessment reports to the respective department heads • Develop a post-crisis report, facilitate debriefing process, apply lessons learned and coordinate the continuous improvement implementation • Gather feedback and consult with the BCSC as necessary • Provide inputs on the incidents to the Operational risk team alignment with the pre-defined plans

Critical Resource and Asset Requirements

Sr. No	Critical Process	Name of Employee	Primary Phone (Mob.)	Official Email	Alternative SPOC	Primary Phone (Mob.)	Official Email
1	End User Computing Management (Critical Business						
Sr. No	Critical Process	Name of Employee	Primary Phone (Mob.)	Official Email	Alternative SPOC	Primary Phone (Mob.)	Official Email
------	----------	----------	----------	----------	----------	----------	----------
2	Systems/Applications Support)						
2	EOD / BOD activity						
3	Security Operations Center						
4	Data Loss Prevention – IS						
5	Network operation center management (Firewall)						
6	Cyber Crisis Management - IS						

Sr. No	Critical Process	Name of Employee	Primary Phone (Mob.)	Official Email	Alternative SPOC	Primary Phone (Mob.)	Official Email
7	Database Administration						
8	Data Centre Management - (Backup Service Management (Service), Sify Managed Service, Patch Management)						
9	Capacity Management						
10	Identity and Access Management						
11	DR management						
12	Privilege access management						

Sr. No	No. of Workstations	No. of Laptop/Desktop	Software Required	General Assets (Telephone/printer/scanner)	Internet/Intranet	Vital Required (if required immediately)
------	----------	----------	----------	----------	----------	----------
1	NA	8	MS Office 365 VPN	NA	Yes	NA

Training Content

• Train employees and management who are members of the recovery organization or are required to execute any plan segments in the event of a disaster.

• Train employees and management who are required to help maintain the plan.

• Raise awareness about the FRPs among employees not directly involved in maintaining or executing the plan.

Testing

Functional recovery plan shall be tested annually by FRP coordinator. This test shall be conducted by process owner and designated test facilitator/coordinator. Test report shall be approved by Functional head and ORM team IT activities will be observed by IT team as per DR.

Review & Maintenance

ORM team shall review the FRP in consultation with process owner and function head. Once reviewed and approved, the updated plan shall be uploaded to QAS for required approvals.

Appendix

Attached Business Impact Analysis (BIA) is conducted to identify the effects of disruptions on critical business services and respective recovery objectives.

METHODOLOGY

1. Introduction

Functional Recovery Plan (FRP) aims towards effectively responding to a disruption and ensure recovery and resumption of its mission critical activities within the expected timelines, thereby minimizing business impact.

2. Objective & Scope

Following are the Business Continuity Management objectives in accordance with the ISO 22301:2019 standard:

• To ensure resumption and availability of critical services at a predefined level, within business acceptable timelines.

• Identify, advanced arrangements and procedures that will enable the agency to respond quickly to an emergency event and set the stage for the continuous performance of critical business functions.

• Protect essential facilities, equipment, vital records, and other assets.

• Facilitate effective decision-making to ensure that agency operations are restored in a timely manner.

• Identify alternative courses of action to minimize and/or mitigate the effects of the crisis and shorten the agency response time.

• Recover quickly from an emergency and resume full service to the public in a timely manner.

3. Document and Change Management

Business Continuity (Process flow)

Business continuity steps/recovery steps for resuming operations in case of disruption are as follows:

Information Technology

• In case of site unavailability, employees will be instructed to work from home (WFH). All employees have been installed on their laptops. If the VPN fails, employees will be expected to work from the alternative site at Worli. Admin duties must be performed from the datacenter.

• If critical resources are unavailable, alternative/backup resources are in place, and these resources are cross-trained.

• Disaster Recovery (DR) management within Information Technology follows a tiered approach involving L1, L2, and L3 support levels. L1 is responsible for monitoring infrastructure and handling alerts. If they are unable to resolve the issue, it is escalated to L2, who possess expertise in specific areas and manage respective domains. L3 involvement is determined by the nature and complexity for

Non-Zero RPO Applications Recovery

Document History

Title	Functional Recovery Plan
Version	1.0
Classification	Internal
Creation Date	12.12.2020

Document Log Control

Version No.	Reviewed By	Approved By	Change History	Date
1.0			First Draft	

Contents