Service Continuity Plan

(Account Name)

Version 0.0

neurealm

Document History

Version	Date (DD/MM/YYYY)	Summary of Changes	Author	Approved By

	Designation	Name
Prepared by		
Reviewed by		
Approved by		

TABLE OF CONTENTS

1. Control Document

1.1 Distribution List –SCP

Sr. No	Person Name & Designation	Project SharePoint (Location Link)	Cloud SharePoint (Location Link)

1.2 Document Owner & Maintainer:

Name of the Person who shall maintain the SCP document

2. List of documents of and plans related to BCM.

Sr. No	Document Title	Location
1.	Evacuation Procedure	NEUREALM Policy Central
2.	Neurealm BC Plan	NEUREALM Policy Central

3. Purpose and Scope

The objective of the Service Continuity Plan is to ensure that all services being offered to <**Account Name**> are not affected and can continue with minimal interruption after a disaster or an emergency. The account level SCP gives the type of service requirements that are ensured from a project perspective. The plan presents the actions and procedures necessary to recover from an adverse event. At the organizational level, the BCP for the organization will establish availability of employees to carry out the designated assignments, data centre processing, network communications, and all business unit functions within desired time frames.

The objectives are as follows

a) To list the critical functions in priority order for recovery
b) To detail the activation procedure and roles and responsibility for staff
c) To detail the agreed actions following a disruption

3.1 Scope:

The Service Continuity Plan is limited in scope for recovery and business continuance from a serious disruption in activities due to any of the following impacts or crisis.

- Building or site incidents: for example, earthquakes, cyclones, explosions, flood, fire, terrorist attack on buildings affecting access to or from building and sites.
- Infrastructure incidents: for example, loss of power / telephony systems, loss of network

- Widespread environmental factors: for example, flu pandemic, fuel shortages

The primary responsibility for development and maintenance of a current and viable plan lies with the Customer Success Manger assigned for the project.

3.2 Office Facilities covered in this scope: -

<Neurealm Chennai, and Pune>

3.3 Service Provided & Criticality

Sr. No	Services Provided as per contract	Criticality

4. Roles & Responsibilities

Roles	Responsibilities
Centre Specific BCP Coordinator (Narasimha Shenoy – Chief Accounts & Administrative Officer)	• Identify and nominate the Centre specific BCP team with representation from various functional units. • Manage and direct the business continuity activities within the center. • Manage the recovery process within the center during disaster/emergency situations. • Initiate/approve the recovery plan for the center and inform the Centre Specific BCP Team to action. • Ensure periodic status updates are communicated to the Corporate BCP Coordinator/BCP Committee • Prepare a centre specific disaster recovery report on completion of recovery process and submit the report to BCP Committee
BCP Committee	• Develop and maintain the Corporate BCP Manual on a regular basis. • Develop and maintain the BCP plan on a regular basis. • Ensure that the plan is tested regularly. • Ensure that the BCP objectives are in line with the business requirements. • Identify & review the critical processes for restoration in case of a disaster. • Prioritize the list of projects to be recovered during a disaster. • Ensure effective communication across all associates/customers involved. • Review the detailed disaster recovery report prepared by the Centre Specific BCP Team members on completion of recovery process.
Centre Specific BCP Team	• Provide feedbacks to BCP Committee and Center Specific BCP

	coordinators, regarding development and Maintenance of the BCP plan on a regular basis. ● Identify and nominate the Center specific BCP Disaster Recovery team with representation from various functional units. ● Identify the critical processes for restoration in case of a disaster. ● Ensure effective communication across all Associates / customers involved. ● Instruct the Disaster Recovery Team to carry out the recovery process at the time of disaster. ● Inform concerned Project Managers to activate their Project Specific BCP. ● Review and publish a detailed disaster recovery report on completion of recovery process to Center Specific BCP Coordinator ● Ensure periodic status updates are communicated to the Center specific BCP Coordinator
Disaster Recovery Team	● Assess damage. ● Analyse the impact on business. ● Clearly relate damage assessment to business continuity of organization ● Identify and isolate damaged assets. ● Assess the reusability of damaged assets. ● Understand economics of repair versus replacement ● Implement the recovery process as per the plan. ● Periodically update the Centre Specific BCP Team on the status of recovery process. ● Coordinate with vendors/contractors for the recovery process. ● Carry out the business resumption activities at centre after the recovery process is over
Delivery Managers	● Coordinate with Functional Heads and Centre Specific BCP Team for implementation of the plan ● Ensure that project specific BCP is maintained. ● Ensure storage of a copy of the project specific BCP with the project team ● Ensure that the project specific BCP meets customer requirements. ● Inform the customer of the BCP activities relevant to the project. ● Instruct the Project team to carry out the recovery process for the Project at the time of the disaster and follow Project Specific BCP. ● Ensure the BCP tests carried out regularly.
Account Managers	● Coordinate with Project Managers and Regional Heads at the time of disaster for proper communication / escalation process to customers. ● Ensure that the project specific BCP meets customer requirements. ● Inform the customer of the BCP activities relevant to the Project. ● Communicate/share the Project specific BCP test details to the

	customer.
Functional Heads	• Develop current and viable plan for business continuity. • Identify and nominate the BCP team for the respective functional units. • Coordinate with the Corporate BCP Coordinator for maintenance of the plan • Identify and list out all critical functions and time frame for restoration of the services in case of a disaster. • Ensure that proper Escalation and Communication process is in place, and it is updated regularly. • Manage BCP activities within the function. • Monitor the implementation of the functional level plans during disaster/emergency situations. • Monitor the implementation of the tests as per the plan and schedule. • Prepare a unit specific disaster recovery report on completion of recovery process
Operations Head – On site	• Manage and direct the business continuity activities onsite. • Develop a communication/escalation process for onsite. • Ensure status updates are sent to all Regional • Heads/Account managers on the disaster and recovery process
Information Security Council	• Coordinate with Corporate BCP Coordinator for review of Corporate BCP once in six months • Review/Approve the corporate BCP Manual
Service Continuity Plan Owner	• Develop and document the Service Continuity Plan, ensuring it aligns with projects goals, compliance requirements and industry best practices. • Periodically review and update the plan to reflect changes in the account/project structure, operations, and external threat environment. • Conduct regular risk assessments to identify potential threats to service continuity and evaluate their impact on operations. • Develop and implement risk mitigation strategies to address identified threats and vulnerabilities • Act as the point of contact for all matters related to service continuity, engaging with stakeholders across the account to ensure alignment and cooperation. • Develop and maintain communication plans for internal and external stakeholders, ensuring that everyone is informed during a disruption. • Promote awareness of the Service Continuity Plan and ensure that employees understand the importance of continuity planning. • Organize and oversee regular tests and exercises of the Service Continuity Plan to ensure it functions effectively in real scenarios and analyze test results and exercise outcomes to identify areas for improvement in the plan. • Promote awareness of the Service Continuity Plan and ensure that employees understand the importance of continuity planning. • Organize and oversee regular tests and exercises of the Service Continuity Plan to ensure it functions effectively in real scenarios and analyze test results and exercise outcomes to

	identify areas for improvement in the plan.

5. Business Impact Analysis

(Provide the link of the Business Impact Analysis (BIA) document)

6. Emergency & Disaster Scenarios

A Disaster could be caused due to one or more of the following.

- Unauthorized access
- Loss of systems (IT or telecommunication)
- Loss of utilities e.g. electricity, flood, water
- Loss of, or access to office building (Cyclone, Floods, Earthquakes, Fire etc.)
- Loss of key personnel
- Fire
- Social unrest or terrorist attacks
- Neighbourhood hazards
- Disgruntled employees
- Hacking or other internet attacks

7. Communication & Escalation Process

Key Message	Owner / Who	Recipients	Communication Medium	When
Notification of a Disaster & SCP	Primary - Secondary -		Call	Within 10 minutes
Estimated Time of Recovery and Periodic updates	Primary - Secondary -		Email	Every 2 hours
Escalation - in the event of failure to provide service	Primary - Secondary -		Email	Every day update
Notification of disaster to the customer in the event of failure to provide service	Primary - Secondary -		Email	Within 10 minutes

Ongoing Updates (Status Reports on the recovery efforts)	Primary - Secondary -		Email	Every 2 hours

In the event of a disaster, the Service Continuity Plan Owner (@ Name of the SCP Owner) has the authority to activate the Service Continuity Plan (SCP)

The following details needs to be communicated as part of the escalation process:

- Details of disaster
- Impact of the disaster.
- Identify relevant existing recovery procedure and plan.
- If it is a new disaster scenario, prepare recovery plan/procedure.
- Time estimates for recovery.

8. Communication & Escalation Process

NEUREALM Chennai Office would have designated primary and alternate command centre where the SCP Team members would assemble to conduct an incident briefing in case of major disasters and chart out action plan for recovery. The incident briefing will be held within 1 hour of the incident to assess the situation and determine whether or not to activate the site recovery plan and SCPs.

Primary Command Centre	Alternate Command Centre
NEUREALM Chennai Office	Virtually connect everyone over Phone call or Online collaboration tool (MS Team Meeting) as the first option. In the event, communication got affected very heavily then employee may be advised to work from alternate NEUREALM Office location. (NEUREALM Chennai team may work from Neurelam Pune and vice versa)

The purpose of the Incident briefing is to acquire all pertinent information about the situation and determine whether or not to activate SCPs. The following information should be available.

Status of emergency response activities – Evacuation Status Description of incident or disaster such as

- Disaster type and impact
- Location and time of occurrence
- Suspected cause and possible potential for extended occurrence
- Potential for recurring outage
- Injuries and fatalities
- Facility or areas affected
- Security – Suspected security breaches
- Access to the facility
- Communication to onsite account managers and other relevant personnel

9. Alternate sites

The following are the designated intra-city and inter-city warm sites for recovering from any disasters.

Facility Name	Intra-city Warm Site	Inter-City Cold Site
NEUREALM Chennai	Note: NEUREALM Admin team will notify about the physical location & facility where employees can stay and provide service to clients	NEUREALM Pune Office

10. Disaster Scenario and Business Continuation Process

Sr. No.	Disaster Scenario	Functions Affected lead to disaster	Responsible for Recover	Criticality of Affected Services (C)	Likelihood of Occurrence (P)	Continuation Process	Concern Function of (P) & (C)
Major Disaster - Impact: – NEUREALM Chennai facility							
1.0	Facility is down due to manmade disaster or natural disaster	All	Centre Specific BCP Team	Vital	Low	• The evacuation process will be initiated • People safety will be taken care • Hot site will be activated within 4 hours • Intercity warm site will be activated within 2 to 5 days • Other services will be activated in the warm site /cold site as applicable • NEUREALM offshore -Team will connect from home immediately	Moderate
2.01	Personnel are not able to travel	All	Finance, Admin, IT,	Vital	Low	• Secure remote access VPN service would be provided to	Moderate

	to work due to local unrest		WFM, HR, Info Security			employees to work from home • If there is a need for team to work from Office facility, Escort would be arranged so that key personnel could travel to office for work, if it is not possible alternate resources shall be arranged or Core team shall work from home using Laptop and Data card. • If required, accommodation near centre shall be arranged to minimize transportations problems based on the BU Head communication sent to Admin / Travel desk. • FOREX agent will be contacted through phone or email and authorize to release foreign currency for critical on- site travel • Travel agent will be contacted through email or phone and authorized to book air ticket for critical travel	
2.02	Critical condition (swine flu, Dengue) encountered by an employee	Personnel belongs to respective function	Respective function, HR & Admin	Essential	Low	• Plan for utilizing backup resource to ensure continuity of service • Concerned Supervisor to inform HR about the critical condition of flu to	Moderate

						review the situation among other employees and take appropriate steps to ensure affected employee is work out of home and not from office to prevent spreading to other employees • HR team shall initiate necessary communication towards preventive measures to be taken for such critical flus	
2.03	Large scale epidemic in city	All	HR, Admin, WFM	Vital	Low	• Vaccination for all associates. Tie-ups with Global Hospital for mass hospitalization • Organise for a Helpdesk to facilitate • Identify affected staff and communicate the plan for working modality	Moderate
2.04	Unable to contact key personnel	Projects /WFM /HR /Finance	HR, IT, Finance, WFM, Admin	Essential	Medium	• Sufficient buffer of staff will be maintained always. • Backup resource will be utilized to ensure continuity in the service	Moderate
2.05	Disgruntled Employees	All	Admin	Essential	Low	• Upon intimation from HR access to facility will be denied • Security personnel will be informed	Moderate
2.06	Electrical power for the facility is down	Admin / IT	Admin	Vital	Medium	• Generators/UPS will be switched on	Major

2.07	UPS failure	All	Admin, IT	Vital	Low	• Backup UPS will take over automatically	Moderate
2.08	Work area affected due to fire or other incidents	Associates located in that work area	Admin	Necessary	Low	• Evacuation process will be initiated • People safety will be taken care • Admin staff will inform Fire service in case of major fire accident. • Intracity site will be activated	Minor
2.09	DNS failure	All	IT	Vital	Low	• Redirect to alternate DNS servers	Moderate
2.10	Network services affected due to hacking	All	IT	Vital	Low	• Review Firewall log and apply strict access rules to prevent / block unauthorised access.	Moderate
2.11	Virus Attack affecting internal systems (not client systems)	Projects	IT	Vital	Low	• Virus affected machines will be shutdown • Strict access rules will be applied immediately after analysing the log • Necessary security patches will be applied	Moderate
2.12	Phone system (EPABX) failure	All	IT	Essential	Low	• A few lines will be directly extended to • critical functions and projects	Moderate
2.13	VPN concentrator failure	All Projects having VPN connectivity	IT	Essential	Low	• In case of a problem with configuration, backup configuration will be restored • In case of hardware problem, the vendor shall provide	Moderate

						temporary replacement	
2.14	Network services within the centre is down	All Projects using the	IT	Vital	Low	• Redirect network traffic through Core switch primary or • Secondary whichever is available	Moderate
2.15	Internet connectivity is down	Projects needing internet connectivity	IT	Vital	Medium	• Redirect the traffic through backup internet connectivity	Major
2.16	Firewall is down	All	IT	Vital	Low	• Redirect the traffic through backup firewall	Moderate
2.17	Resources not available for any reason	Projects	WFM, Respective Function	Vital	Low	• Backup resource identified by the respective project / function will be utilized.	Moderate
2.18	Laptop / Desktop or Power failure / Internet connectivity failure at the team member location	All	IT	Vital	Medium	• Concerned PM will re-allocate the work / deliverable to other resource in the team • In the mean time talk to IT team to get the alternate laptop, if this option will not work request the concerned team member to come to Office and work	Moderate
2.19	In WFH situation, the employee is not able to support the project activities, due to power outage, network connectivity issue.	Project	HR, IT, Respective Function	Vital	Medium	• Inform the PM/CSM and relevant team members about the disruption. • Redirect critical tasks to other team members. • Consider working from an alternate location with power, such as a	Moderate

						coffee shop, hotel or a friend's house. • Make arrangement to travel office for work	
2.20	Large scale epidemic or pandemic	All	Leadership Team, HR, Admin & WFM,CSM	Vital	Medium	• Application of vaccination for all associates if applicable as per Health Care / Doctors advise. • Tie-up with Global Hospital for hospitalization or Health check / test. • Follow specific instruction – Do's and Don'ts circulated by NEUREALM Occupational Health and Safety function • In case any employee who return from affected countries, advise home quarantine for two weeks. • Employee got affected will be asked not to return to office and home quarantine until test result shows negative for the disease. • Organize for a Helpdesk to guide employees for availing Health Insurance, claims and directing to an appropriate Hospital. • Identify affected staff and communicate the plan with	Moderate

						function head and customer contact for working modality	
2.21	In the event, NEUREALM employee return to client office country (ME, USA or UK) from the COVID-19 affected country	All	Leadership Team, HR, Admin & WFM, CSM	Vital	Medium	• NEUREALM shall ensure that such employees are moved to a nominated quarantine location and stay for two weeks and notify customer about the action taken. • NEUREALM shall ensure that such employees get tested for COVID-19 • until test result shows negative they will not return to office / work	Moderate
2.22	In the event of NEUREALM employee found to be a suspected case of COVID- 19 or any of the following symptoms - respiratory symptoms such as fever, running nose, coughing, headache, throat pains or body pains	All	Leadership Team, Admin & WFM,CSM	Vital	Medium	• NEUREALM employees are advised for self-quarantine, if required employees get tested and will not return to work unless doctor advise. • NEUREALM employees are advised to follow specific instruction – Do's and Don'ts circulated by NEUREALM Occupational Health and Safety function including the following and not limited to these o Observe social distancing (2 m safe zone) among workforces inside the institution	Moderate

						○ All time wear face mask, hand- wash ● Follow the guidelines set by the Government. ● NEUREALM Team will continue to monitor the health of employee and keep customer informed about the safety measures taken and plan for return to work	
2.23	Possibility of NEUREALM employee getting affected by COVID-19	All	Leadership Team, HR, Admin & WFM,CSM	Vital	Medium	● NEUREALM employees advised to take vaccine for COVID-19 ● NEUREALM employees are advised to follow specific instruction – Do's and Don'ts circulated by NEUREALM Occupational Health and Safety function including the following and not limited to these ○ Observe social distancing (2 m safe zone) among workforces inside the institution ○ All time wear face mask, hand- wash ● Follow the guidelines set by the Government	Moderate

11. Critical Resource Requirements during a disaster

	Timelines		
Resources	**< 8 Hours**	**Upto 1 Week**	**Beyond a week**
Staff	1 resource	Minimum of 4 resources.	Entire CC team (12 members) including Core-team
Laptop	1 Nos	3 Laptops	4 Laptops
Internet Data Card	1 No. with roaming enabled	1 roaming enabled Data cards	2 roaming enabled Data cards
Mobile Phone	With ISD facility for Core Team, VoIP	With ISD facility for Core Team	With ISD facility for Core Team
Physical Seat	1 No.	2 No.	4 No.
Soft Phone	1	2	4
IT Applications	GM VPN Connect		

11.1 Team detail (Key Contact):

Sr. No	Name	Email Address	Phone	Team
1				
2				
3				
4				
5				

12. Service Continuity Test Report

(Provide the link of the Service Continuity Test Report)

13. Disaster Recovery Strategy

It is mandatory that the basic infrastructure is restored as a first priority which will be the base for all services. This will include network, systems and other infrastructure services to enable the customer specific services / support to continue their business operations smoothly.

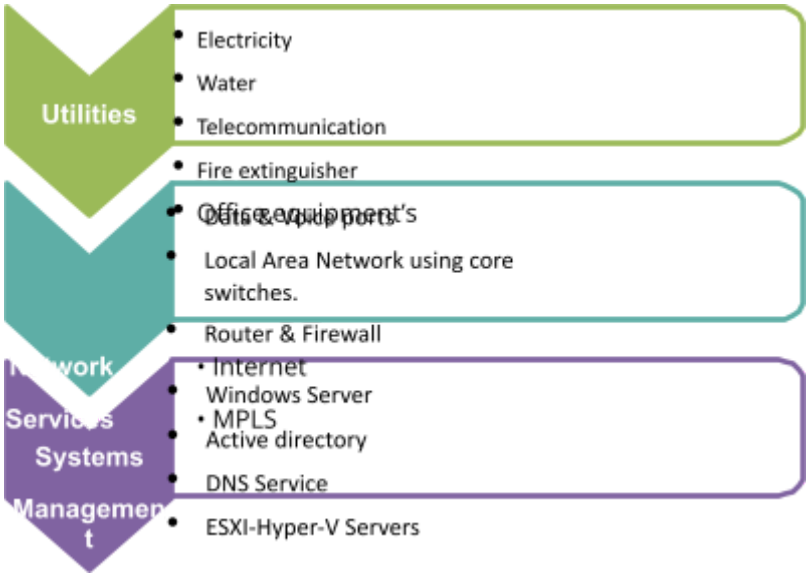
In disaster scenarios, the recovery strategy has been considered into two phases namely:

- Technical Recovery Phase (Infrastructure components)

- Business Recovery Phase (Business components)

13.1 Technical Recovery Phase

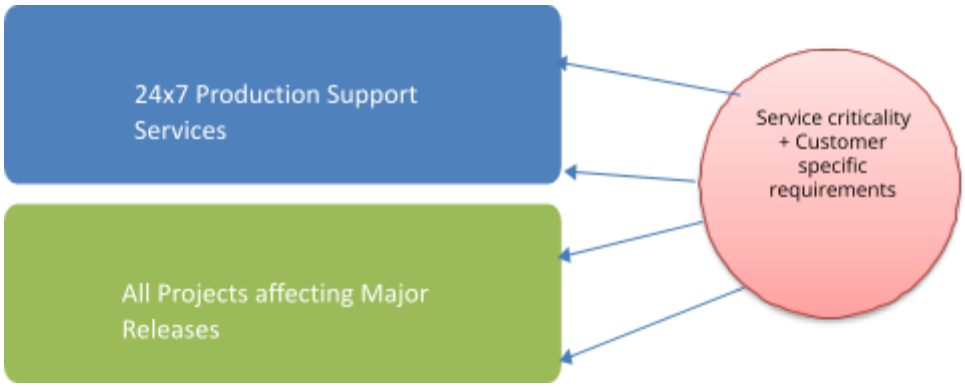
The order of restoration of services in the disaster recovery phase is as follows.



13.2 Business Recovery Phase

The Business Recovery phase involves the restoration of normal business operations after an unexpected event which has disrupted all or part of the business process. From a business perspective, this is the most critical phase of the whole BCP.

The order of restoration of services based on the service criticality. However, there can be some exceptions based on customer specific requirement. During a disaster, the recovery of projects will be decided by the BCP Committee in conjunction with the Line of Business Heads.



13.3 Criticality of service disruption

The services have been classified into one of the four based on the criticality of the services disruption. They are **Vital, Essential, Necessary and Desirable**. While arriving at the criticality, risk factors like Personal Safety, Services Risk, Operational Risk, Revenue Risk, Liability Risk and Goodwill (Societal Risk) have been considered and individual functional groups, projects and other stakeholders have been consulted. Guidelines for identifying the services as vital, essential, necessary, or desirable is given below.

Critical / Vital: -

Any disruption in service that would stop the business or function would be categorized as “Vital” Vital category will follow an SLA of less than 4 hours and all the services need to be restored within 4 hours. Also an update on hourly basis or completion of recovery of each critical stage or phase of the service (whichever is earlier) needs to be given as per the escalation proces s.

Essential: -

The criticality would be classified as ‘Essential’ if the service affects business but still the bare minimum activities can be carried out.
The SLA for Essential is 2 days and all the services should be restored within 2 days. The update of the recovery process can be communicated on a daily basis or stage-wise depending on the importance.

Necessary: -

‘Necessary’ services are the ones, which, if not available causes some inconveniences to the business or deliverable. The SLA for these services is 1 week and all the services should be restored within a week. The update of the recovery process can be communicated on a daily basis or stage-wise depending on the importance.

Desirable: -

All ‘Desirable’ services will fall into the category of cosmetic services where the downtime will not affect business in anyway. The SLA for Desirable would be 1 month and all the services should be restored within 1 month. The update of the recovery process can be communicated on a d aily basis or stage wise depending on the importance.

13.4 Level of Concern

Risk Appetite	
No	N/A - risk removed
Low	Acceptable risk and no further action required as the risk has been minimized and monitored as far as possible. Risks needs to be reviewed at least annually.
Moderate	Tolerable with further action required to mitigate risk or remove. Risk needs to be reviewed at least every 6 months.
High	Tolerable with further action required to mitigate risk or remove. Risk needs to be reviewed at least every 3 months.
Catastrophic	Unacceptable risk and urgent action required to mitigate or remove the risk. Risk needs to be reviewed monthly.

Consequences of the event on CIA (Confidentiality, Integrity, Availability) Guideline in qualitative words		
None	0	No consequences - for example the control has eliminated them
Insignificant	1	No visible impact to company reputation/customer satisfaction. No potential impact on market share/brand values
Minor	2	Potential impact on market share/brand values. Internal control significant deficiency
Significant	3	Visible reputation/satisfaction impact. Reputation and brand value will be affected in the short term. Internal control material weakness
Major	4	Visible adverse brand value/market share publicity. Key alliances are threatened. Loss of key customers. SEC investigation or matter. Financial restatement.
Critical	5	Major company reputation impact. Revocation of licenses or regulatory registrations. Major customer satisfaction impact. Inability to service customers. Loss of major

Likelihood Value				
		Guideline in qualitative words	Probability	Frequency
Impossible	0	The event is impossible - for example the risk source has been removed or activity has been stopped	0%	will not happen
Rare	1	The possibility of occurrence is so low. These are exceptional circumstances or it may never happen	<1%	it may never happen
Remote	2	Unlikely to happen	2-10%	doubt that it occurs
Moderate	3	Believe it could occur	11-50%	is at least 1 per year
Likely	4	May occur sometimes	51-90%	occasionally during a year
Frequent	5	Known to occur. Almost certain.	>90%	several times in a year

Risk Matrix

Risk Rating Matrix		Consequences					
		Critical	Major	Significant	Minor	Insignificant	None
Likelihood		5	4	3	2	1	0
Frequent	5	Catastrophic	Catastrophic	High	High	Moderate	No
Likely	4	Catastrophic	High	High	Moderate	Low	No
Moderate	3	High	High	Moderate	Moderate	Low	No
Remote	2	High	Moderate	Moderate	Low	Low	No
Rare	1	Moderate	Low	Low	Low	Low	No
Impossible	0	No	No	No	No	No	No

Avoid

Share/ Transfer

Accept

14. Business Resumption Process

Once the disaster recovery has taken place the business continues in the alternate site. However, it should be noted that the business should resume from the home site since the Alternate site is for a short period only.

For returning back to home site, the basic infrastructure should be set-up or recovered first. The order of restoration of services will be same as mentioned in the section 11 – Disaster recovery phases. The damage assessment report will form part of input to the service restoration process.

15. Training and Exercise Programme

Training	1) Induction for new staff includes Business Continuity Management (BCM). 2) Programme of briefings to ensure all staff are updated on BCM on an annual basis. 3) All staff who are named within this plan have been trained / briefed on their role and responsibilities.
Exercising	1) Back-up power and IT back up & restore is tested once in a year. 2) Quality Team will initiate Desktop / Tabletop exercise once in six months, covering a scenario relating to one of the highest risks and any Minor Risk to the business as detailed in the Risk Assessment, desktop exercise is carried out with all the delivery managers for all the accounts that they manage. - 3) Head of Information Security will review readiness of proposed DR site every year. (Exercise Type is Partial Test)
Test	1) Performance of Building Structural Stability Test – Once in three years 2) Earth Pit Test – Once in a year 3) Lift OEM – Once in a year 4) Emergency Drill – Once in a year 5) Test specific scenarios related to IT from Minor disaster scenarios - Quarterly

SCP Document History

Version	Date	Summary of Changes	Author	Approved By
1.00	25/Jan/2016	Initial Draft Release for Leadership Team's review	Shalot Leely	Sekar T
1.01	18/Feb/2016	Based on the review held with CEO on 17th Feb 2016	Shalot Leely	Sekar T
1.02	31/Mar/ 2016	Add the Bangalore location	Shalot Leely	Sekar T

1.03	30/May/2023	Removed Hyderabad & Bangalore Office details	Shalot Leely	Sekar T
1.04	25/July/2025	Aligning to Neurealm template and standard	Shalot Leely	Ambrish

Note: The above version history table is maintained by the Process Excellence Team. The Project Team should refrain from making any changes to it.

Statement of Confidentiality

This Neurealm Private Limited (formerly known as GAVS Technologies Private Limited) artefact and/or document and/or presentation is strictly confidential and it contains proprietary information intended only for recipients of Neurealm Private Limited (Neurealm). The recipient acknowledges and agrees that: (i) this artefact and/or document is not intended to be distributed (ii) the recipient does not have the right to implement, copy, reproduce, fax, print, publicly divulge, or further distribute it, in whole or in part in any form, without seeking the express written permission from Neurealm. Any unauthorized use of the contents of this artefact and/or document and/or presentation in any manner whatsoever, is strictly prohibited. The artefact and/or document and/or presentation represents Neurealm's current product offerings and best practices which are subject to change without notice. Please note that Neurealm collaborates in relation to some of its offerings.

All third-party trademarks used herein belong to their respective owners and may be protected by law. This artefact and/or document and/or presentation only refers to such trademarks under the doctrines of nominative and descriptive fair usage to illustrate and explain concepts without implying violation of any legal constraints. If any improper activity is suspected, all available information may be used by Neurealm for lawful purposes and to seek appropriate remedies. Neurealm complies with applicable privacy laws and regulations. Recipients are advised to handle the information contained in this Material in accordance with relevant privacy and data protection laws.