Business Continuity & Disaster Recovery Policy

Owner Name: Process Excellence Team (PeX)

Version: 2.0

neurealm

	Designation	Name
Prepared by	Sr .Manager – Process Excellence	Shalot Leely
Reviewed & Approved by	Director - PeX Team	Ambrish

Change History

Version No.	Release Date	Process Improvement Proposal Reference No.	Summary of Changes	Prepared by	Approved By
1.00	30th April 2014	1	Initial Version	Hariharan Madhavan	Sridhara Sundararaj
1.01	27th Nov 2015	PIP # 19	Revised based on Annual Review carried out in Nov-15.	Hariharan Madhavan	Security Council
1.02	15th Dec 2016		Reviewed Policy and no changes required	Hariharan Madhavan	Security Council
1.03	2nd Mar-17	NA	Replaced old GAVS logo with new GAVS logo	Sekar T	Sekar T
1.04	06-Nov-2017	NA	Updated with Zero incident logo	Blessy Sara Bobby	Sekar. T
1.05	15-Jan-18	NA	Annual Policy review – No changes to BC&DR policies	Sekar T	Security Council
1.06	19-Mar-19	NA	Annual Policy review – No changes to BC&DR policies	Mesiya A	Sekar T
1.07	09-Mar-20	NA	Annual Policy review – No changes to BC&DR policies	Shivaram J	Security Council
1.08	08-Mar-21	NA	Annual Policy review – No changes to BC&DR policies	Ravi G	Security Council
1.09	30-Mar-22	NA	Annual Policy review – No changes to BC&DR policies	Rajesh	Sekar T

1.10	22-May-23	NA	Annual Policy review – No changes to BC&DR policies	Rajesh	Sekar T
1.11	16-Apr-24	NA	Annual Policy review – No changes to BC&DR policies	Rajesh	Sekar T
2.0	07-May-25	NA	Updated to Neurealm format	Shalot	Ambrish

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.

TABLE OF CONTENTS

Introduction

This Business Continuity & Disaster Recovery policy acts as a framework for the implementation and continuous compliance of business continuity and disaster recovery practices in Neurealm across all business units and to promote business & service continuity awareness. Other procedures and best practices within the organization are designed to be consistent with this policy.

Scope

This policy includes common BC & DR requirements applicable for all the managed service delivery projects and dependent business enablement & support functions, systems and personnel.

Reference

- ISO 27002:17
- NIST CSF: ID.BE, PR.IP, RS.RP, RS.CO, RS.IM, RS.RP, RC.IM, RC.CO
- Information Classification and Management Policy
- Business Continuity Plan
- Disaster Recovery Plan

Business Continuity Policy

Business Continuity focuses on sustaining the organization's critical business processes during and after a disruption.

- Neurealm must create and implement a Business Continuity Plan ("BCP").
- The BCP must be periodically tested and the results should be shared with executive management.
- The BCP must be reviewed and updated upon any relevant change to the organization, at the conclusion of plan testing, or least annually.
- The BCP must be communicated and distributed to all relevant internal personnel and executive management.
- Business continuity planning should ensure that:
  - The safety and security of personnel is the first priority;
  - An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence.
  - Documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event.
- The BCP must include, at a minimum:
  - A risk assessment for critical business processes and operations (Business Impact Analysis);
  - An inventory of critical systems and records, and their dependencies;
  - Requirements for ensuring information security throughout the process;
  - Identification of supply chain relationships and the organization's role to support critical infrastructure;
  - Processes to ensure the safety of personnel;
  - Communication strategies for communications both inside and outside the organization;
  - Mitigation strategies and safeguards to reduce impact;
  - Strategies to address and limit the reputational impact from an event;
  - Contingency plans for different types of disruption events;
  - Protection and availability of plan documentation;

- Procedures for plan tests, review, and updates.

Disaster Recovery Policy

Disaster Recovery focuses on restoring the technology systems that support both critical and day-to-day business operations.

- Neurealm must create and implement a Disaster Recovery Plan ("DRP") to support business objectives outlined in the (BCP/critical processes identified by a Business Impact Analysis).
- The DRP must be tested annually, at a minimum.
- The DRP must be reviewed and updated upon any relevant change to IT Infrastructure, at the conclusion of plan testing, or least annually.
- The DRP must be communicated and distributed to all relevant internal personnel and executive management.
- The Neurealm DRP must include at a minimum:
  - Roles and responsibilities for implementing the disaster recovery plan;
  - List of potential risks to critical systems and sensitive information;
  - Procedures for reporting disaster events, event escalation, recovery of critical operations, and resumption of normal operations;
  - Requirements for ensuring information security throughout the process;
  - An inventory of backups and offsite storage locations;
  - Contingency plans for different types of disruption events;
  - Protection and availability of plan documentation;
  - Procedures for plan tests, review, and updates.

Managers are responsible for implementing the BC & DR policy within their business areas, and for adherence by their team. It is the responsibility of employee to adhere to this policy

This policy has been approved by top management and shall be reviewed annually. This policy has the endorsement at the highest level and is actively practiced by Neurealm members at all levels.

Policy Exceptions

Any exceptions to this Policy, Standard, or Procedure must be applied for and authorization received in writing.

Disciplinary Process

Any personnel authorized by the company to act on its behalf found in violation of this policy shall be subjected to disciplinary action based on the nature of incident and its impact on business

Managers must refer to their human resources representative for advice on handling non-compliance with this policy.