

**Business Continuity Management**

Policy Template

Customer Name

Author Name: Gouri Mahendru

Version: 2.1

Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Summary of Changes | Author | Approved By |
| 1.0 | 10-Apr-14 | Initial Document | Sujatha | Sekar T |
| 1.01 | 1-May-17 | Change GAVS logo | Emmanuel F | Sekar T |
| 2.0 | 20-Jan-23 | Revised Policy Statements (section 5.0) | Gouri Mahendru | Sekar T |
| 2.1 | 16-Mar-23 | Updated as per new GS Lab | GAVS document format | Gouri Mahendru | Sekar T |

|  |
| --- |
| Statement of Confidentiality |
| This GS Lab (Great Software Laboratory) and/or GAVS (GAVS Technologies) artefact and/or document and/or presentation is strictly confidential. It contains proprietary information intended only for recipients.  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, publicly divulge, or further distribute it, in whole or in part in any form, without seeking the express written permission from GS Lab and GAVS.  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 GS Lab’s and/ or GAVS’s current product offerings and best practices which are subject to change without notice. Please note that GS Lab and GAVS collaborate 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 improper activity is suspected, all available information may be used by GS Lab and /or GAVS for any remedy or for lawful purpose. |

Table of Contents

[**1.** **Purpose** 4](#_Toc130468625)

[**2.** **Scope** 4](#_Toc130468626)

[**3.** **Definitions** 4](#_Toc130468627)

[**4.** **Definitions** 5](#_Toc130468628)

[**5.** **Applicable Laws, Regulations, and Industry Standards** 5](#_Toc130468629)

[**6.** **Policy Statements** 5](#_Toc130468630)

[**7.** **Roles and Responsibilities** 6](#_Toc130468631)

[**8.** **Non-compliance** 7](#_Toc130468632)

## **Purpose**

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

This policy supports the [Client Name] mandate for Business Continuity Management (BCM), a comprehensive program concerned with improving the resilience of [Client Name]. [Client Name] will take appropriate steps to detect, prevent, minimize, and manage the impact of disruptive events through BCM activities.

The BCM program has the following objectives:

* Improve [Client Name] resilience against disruption of its ability to deliver key business objectives before a disruption occurs.
* Deliver proven capabilities to manage business disruption and protect [Client Name] value-creating activities, such as increasing market share; generating revenue; and protecting stakeholder interests, reputation, and brand image.
* Restore [Client Name] ability to deliver key processes to an agreed level within an agreed time following a disruption.

## **Scope**

Define to whom and to what systems this policy applies. List the employees required to comply or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions that are out of scope, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This BCM Policy applies to the whole of [Client Name], including all global subsidiaries, and to any outsourcing or joint venture entered into by [Client Name] or its subsidiaries.

Third parties, including service providers upon whom [Client Name] is critically dependent for the provision of services, must be considered an essential part of business continuity planning, and appropriate contingency arrangements must be ensured by means of contractual agreements assuring business continuity of external parties in accordance with [Client Name] standards.

## **Definitions**

Define any key terms, acronyms, or concepts that will be used in the policy or accompanying procedures. A standard glossary approach is sufficient. An example definition:

This BCM Policy applies to the whole of [Client Name], including all global subsidiaries, and to any outsourcing or joint venture entered into by [Client Name] or its subsidiaries.

Third parties, including service providers upon whom [Client Name] is critically dependent for the provision of services, must be considered an essential part of business continuity planning, and appropriate contingency arrangements must be ensured by means of contractual agreements assuring business continuity of external parties in accordance with [Client Name] standards.

## **Definitions**

Define any key terms, acronyms, or concepts that will be used in the policy or accompanying procedures. A standard glossary approach is sufficient. An example definition:

Business Continuity Management (BCM): “A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.”[[1]](#footnote-2)

Business Continuity Plan (BCP): “Ddocumented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.”[[2]](#footnote-3)

Disaster Recovery Plan (DRP): A plan to restore IT application and infrastructure services following a disruption. The DRP is a component of the BCP.

Crisis Management Plan (CMP): A plan to manage a wide range of crises, from health and safety incidents to business disruptions and reputational damage. The CMP is a component of the BCP.

## **Applicable Laws, Regulations, and Industry Standards**

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no applicable laws, regulations, or industry standards delete this section.

|  |  |
| --- | --- |
| Guidance | Section |
| ISO 20000-1:2018 | Section 8.7 (Service Assurance – Service Continuity Management) |

## **Policy Statements**

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Subdividing this section into subsections may be preferable, depending on the length or complexity of the policy.

**Basic Policy Requirements:**

* [Company Name] will develop its ability to detect, prevent, minimize, and manage events that disrupt business activities, in accordance with applicable laws, regulations, and industry standards.

**Derived Policy Requirements:**

*Business Impact Analysis and Threat Assessments*

* A Business Impact Analysis (BIA) will be conducted at least annually for each key COMPANY location using approved BCM templates.
* A Threat Assessment will be completed at least every [interval – suggest two years] for each key COMPANY location.
* The BIA will be reviewed by the BCM Team and IT Management and validated to ensure alignment with the IT Disaster Recovery Plan (DRP).

*Business Continuity and Disaster Recovery Plans*

* Each business unit will fully document its own Business Continuity Plan (BCP) using BCP template materials.
* Each business unit will review its BCP at least annually or when the BIA is reviewed, whichever comes first. Any changes or updates must be approved by that business unit’s management team.
* Business units will test their plans every [minimum time interval – suggest at least annually].
* IT Management is responsible for DRP documentation for each IT service, system, and application.
* The full IT DRP will be reviewed at least [interval – suggest annually]. The BIA and DRP documentation will be revisited and updated as required by change management processes.
* IT will test the DR recovery plan every [minimum time interval – suggest at least annually].

*Incident Escalation and Crisis Management*

* [Client Name] will establish a company-wide Core Crisis Management Team (CCMT) and Crisis Management Plan (CMP) that will operate from COMPANY global headquarters.
* Each global subsidiary of [Client Name] will establish an Operational Crisis Management Team and CMP to identify, assess, and manage regional crises.
* Each CMP will identify participants, communications methods, and primary and alternate command centers.
* The BCM Team will define the incident escalation process and will set trigger levels for invoking BCPs and DRPs.
* The BCM Team will establish and define the Crisis Management Governance Structure and will have it approved by the Enterprise Risk Committee.
* All [Client Name] premises will have a formal building evacuation plan. The evacuation plan will be tested at predetermined intervals.
* Other plans (pandemic plans, facilities plan, etc.) will be created as appropriate by the respective business units.
* The Communications Department will be responsible for the creation and maintenance of the Crisis Communications Plan. The Crisis Communications Plan will be activated as needed by the Crisis Management Team.

## **Roles and Responsibilities**

* The [Client Name] **Board of Directors** is accountable for [Client Name] BCM program.
* The [Client Name] **Business Continuity Management Committee** (BCM Committee) will advise Executive Management and management team members on BCM. The BCM Committee will define and recommend investments in business continuity based on [Client Name] risk profile.
* **Executive Management** (headed by the Chief Executive) is responsible for oversight of the COMPANY BCM program and will:
  + Implement strategies and policies approved by the BCM Committee
  + Ensure roles and responsibilities for BCM are clearly defined within all business units
  + Endorse and fund business continuity activities.
  + Ensure COMPANY remains compliant with all applicable legal, regulatory, and industry related BCM requirements
* **Management**, at all levels, must understand their tasks and responsibilities in the [Client Name] Business Continuity Plan. Managers responsible for business activities will establish the extent and nature of required business continuity measures and mitigations.
* A **BC Coordinator** will be appointed for each business unit. Business continuity activities will be included in the performance measures and job description of each coordinator. The BC Coordinator will:
  + Implement and communicate the BCM program.
  + Report BC readiness to the BCM Team

All Staff must understand their role and responsibilities in Business Continuity Management. Staff will observe, support, and incorporate procedure and process changes related to BCM as required.

## **Non-compliance**

Clearly describe consequences (legal and/or disciplinary) for employee noncompliance with the policy. It may be pertinent to describe the escalation process for repeated noncompliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Client Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Client Name] policies
2. Termination of employment
3. Legal action according to applicable laws and contractual agreements

1. BCI, 2013. “Business Continuity Good Practice Guidelines”, p. 5. [↑](#footnote-ref-2)
2. ISO 22301:2012. “Societal Security – Business Continuity Management Systems – Requirements”. [↑](#footnote-ref-3)