Business Continuity Management Policy

Introduction: How to Use This Policy Template

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

Policy Author	Name the person/group writing the document, if different from Policy Owner.
Policy Owner	Name the person/group responsible for this policy's management.
Policy Approver(s)	Name the person/group responsible for implementation approval of this policy.
Related Policies	Name other related enterprise policies both within or external to this manual, e.g. Identification and Authentication Policy.
Related Procedures	Name other related enterprise procedures both within or external to this manual, e.g. DRP Summary, Recovery Workflow Procedure.
Storage Location	Describe physical or digital location of copies of this policy.
Effective Date	List the date that this policy went into effect.
Next Review Date	List the date that this policy must undergo review and update.

Contents

Info-Tech Research Group

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 [Company Name] mandate for Business Continuity Management (BCM), a comprehensive program concerned with improving the resilience of [Company Name]. [Company 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 [Company 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 [Company Name] value-creating activities, such as increasing market share; generating revenue; and protecting stakeholder interests, reputation, and brand image.
- Restore [Company 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 [Company Name], including all global subsidiaries, and to any outsourcing or joint venture entered into by [Company Name] or its subsidiaries.

Third parties, including service providers upon whom [Company 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 [Company 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]

Business Continuity Plan (BCP): "Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption."[2]

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.

---

[1] BCI, 2013. "Business Continuity Good Practice Guidelines", p. 5.
[2] ISO 22301:2012. "Societal Security – Business Continuity Management Systems – Requirements".

Info-Tech Research Group

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 22301:2012	All Clauses

Policy Statements

Basic Policy Requirements:

- COMPANY 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

- [Company 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 [Company 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 [Company Name] premises will have a formal building evacuation plan. The evacuation plan will be tested at predetermined intervals.

- Other plans (pandemic plans, facilities plans, 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 [Company Name] **Board of Directors** is accountable for [Company Name] BCM program.

- The [Company 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 [Company Name] risk profile.

- **Executive Management** (headed by the Chief Executive) is responsible for oversight of the COMPANY BCM program and will:
  - o Implement strategies and policies approved by the BCM Committee
  - o Ensure roles and responsibilities for BCM are clearly defined within all business units
  - o Endorse and fund business continuity activities
  - o 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 [Company 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:
  - o Implement and communicate the BCM program
  - o 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.

Relevant Procedures

Consider creating formal procedure documents that reinforce and support the policy statements above. It is a best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Exceptions

Anyone seeking an exception to this policy must contact the Business Continuity Management Team.

Noncompliance

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

Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [Name of Policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

_____
Employee Name

_____   _____
Employee   Signature   Date

Revision History

Version ID	Date of Change	Author	Rationale

_____