



PRESIDENCY UNIVERSITY

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956

Approved by AICTE, New Delhi

BUSINESS CONTINUITY MANAGEMENT POLICY

November 2019
[Version 1.0]

**[As Approved at the 13th Meeting of BOM and ratified by the BOG at its 13th Meeting, both held on
November 9, 2019]**

Jane
REGISTRAR  1

CONTENTS

1. PREAMBLE	3
2. SHORT TITLE AND APPLICATION	3
3. EXTENT AND APPLICABILITY	3
4. DEFINITIONS.....	3
5. OBJECTIVES.....	4
6. COMPOSITION OF BUSINESS CONTINUITY MANAGEMENT PROGRAM (BCMP)	5
7. ROLES AND RESPONSIBILITIES	5
8. PLAN STRUCTURE AND OPERATION.....	7
9. BUSINESS IMPACT ANALYSIS.....	7
10. BUSINESS CONTINUITY PLANNING (BCP)	7
11. ACTIVATION OF THE BUSINESS CONTINUITY PLAN.....	9
12. LINKS TO OTHER AREAS	9
13. AMENDMENTS	10

PRESIDENCY UNIVERSITY

BUSINESS CONTINUITY MANAGEMENT POLICY

1. PREAMBLE

- 1.1. The Presidency University allows Business Continuity Management (BCM) to proactively mitigate the operational risks arising from an incident that may have a negative impact on its working process. This increases the likelihood of the University not being able to continue its critical activities following a major disruption.
- 1.2. Business continuity is the capability of the University to continue delivery of services at acceptable and predefined levels following a disruptive incident.
- 1.3. The purpose of this policy is to support the University in clearly identifying its critical activities and capability to resume business as usual within agreed timeframes following the deployment of an emergency response.
- 1.4. Effective business continuity planning will increase resilience and minimise disruption. This provides the University with the capability to ensure continuity of teaching-learning and research and to supports its staff and students following any major incident.

2. SHORT TITLE AND APPLICATION

- 2.1. This Policy shall be called the “Presidency University Business Continuity Management Policy”.
- 2.2. This Policy shall come into effect from the date of approval by the Board of Management, Presidency University and ratified by appropriate higher bodies, if need be.

3. EXTENT AND APPLICABILITY

- 3.1. The extent and applicability of this policy shall apply to all of the University’s activities and operations.
- 3.2. The University community, facilities, equipment, IT infrastructure and systems, including University assets.
- 3.3. Certain types of emergencies or crises that become the responsibility of the University to seek appropriate management solutions.

4. DEFINITIONS

“Business Continuity Management” (BCM): The capability of the University to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

“Business Continuity Plan” (BCP) means a university’s risk management strategy for threats that may terminate or significantly disrupt core business. It involves mitigation activities and contingency planning for response and recovery actions.

[Signature]
REGISTRAR



3

“Business Continuity Management Program” (BCMP) implies the ongoing management and governance process supported by the University and appropriately resourced to implement and maintain Business Continuity Management.

“Business Impact Analysis” (BIA) is the process of analysing activities and the effect that a business disruption might have upon them.

“Crisis” means adverse incidents or series of incidents that have the potential to seriously damage University’s community, reputation, business operations, resources or property.

“Emergency” implies a sudden, unexpected event that endangers or threatens the University’s community or resources and requires an immediate response from internal or external agencies and emergency services.

“Event” means the occurrence of a or a set of circumstances that creates an actual or potential emergency or disaster or another crisis situation.

“Recovery Time Objective” is the period following an incident within which an activity must be resumed, or resources must be recovered.

5. OBJECTIVES

5.1. The University is committed to ensuring that an effective Business Continuity Management program is implemented to minimise the disruption of activities due to the unavailability of ‘business as usual’ resources, for example but not limited to:

- 5.1.1. Facilities, e.g., Flood, fire, power outage, chemical spill, denial of access
- 5.1.2. People, e.g., Pandemic/epidemic, industrial action, any natural calamity
- 5.1.3. Vital records, e.g., Electronic and hard copy records
- 5.1.4. Information and Communications Technology, e.g., computer hardware, applications, and telecommunications
- 5.1.5. Equipment, e.g., Cold rooms, research equipment, desks, and chairs
- 5.1.6. Externally-provided service or resource e.g., Contractors, software vendors.

5.2. The BCMP requirements will be assessed via a Business Impact Analysis (BIA) for activities undertaken by all Faculties and Portfolios.

5.3. The University is committed to implementing best practice in business continuity management throughout the institution, to minimise the effect of disruptions on staff, students, key stakeholders, and the general public, and to maintain the reputation of the University.

5.4. The University will take all reasonable steps to ensure that in the event of any major incident, critical activities will be maintained, and normal services resumed as soon as possible.

5.5. The University’s top priority is to ensure the safety of its people and the security of its work environment.

5.6. The University aims to:

- 5.6.1. Identify time critical activities across the University and ensure that appropriate business continuity arrangements are in place for these;
- 5.6.2. Establish a clear and comprehensive plan in order to respond to incidents;
- 5.6.3. Develop and review the plan in accordance with the University's strategic aims and best practice across the segments;
- 5.6.4. Embed business continuity into the culture of the University so that this, alongside risk management, becomes an integral part of decision making.
- 5.7. The business continuity processes will be delivered in conjunction with the risk management framework. Risk management aims to identify and manage risks; business continuity management and planning then handles the risk if it materialises.
- 5.8. Business Continuity Plans and Business Impact Analysis should be reviewed on an annual basis and reported to appropriate Higher Body of the University.

6. COMPOSITION OF BUSINESS CONTINUITY MANAGEMENT PROGRAM (BCMP)

- Vice Chancellor (Chair)
 - Pro Vice-Chancellor (Academics)
 - Registrar
 - Director (Administration)
 - Director (Housing)
 - Head (IT)
 - Dean (Student Affairs)
 - Director (Admissions)
 - Finance Officer
 - Deans of Schools
 - Heads of Departments
 - General Manager (Procurement)
 - Director (Human Resource) *
- * Business Continuity Manager and Convenor

7. ROLES AND RESPONSIBILITIES

7.1. University Business Continuity Manager

- 7.1.1. Raising the profile of Business Continuity across the University as an on-going responsibility and ensuring that information is available to staff (with the aim of embedding BCM into the activities of the University).
- 7.1.2. Providing advice and assistance throughout the BCM process.
- 7.1.3. Developing appropriate templates for the University to detail its arrangements, ensuring consistency in the program with flexibility to recognise the difference across faculties and departments.

- 7.1.4. Supporting departments in completing the documentation from Business Impact Analysis (BIA) to developing a Business Continuity Plan (BCP).
- 7.1.5. Assisting in the development of overarching arrangements to support departmental plans.
- 7.1.6. Ensuring that the University's arrangements are regularly reviewed and exercised.
- 7.1.7. Providing training to appropriate staff and leading on the development of corporate exercises to review arrangements that have been put in place.
- 7.1.8. Monitoring the level of Business Continuity planning in the University and reporting to the Business Continuity groups.
- 7.1.9. Reviewing the program to ensure it remains fit for purpose and to continuously improve the arrangements in place.

7.2. Business Continuity Representatives (School Level)

The role of the Business Continuity Representative is to assist the University Business Continuity Manager in "championing" BCM by

- 7.2.1. Acting as a single point of contact within the Faculty/Department for Business Continuity issues.
- 7.2.2. Being able to explain how it works, the benefits of undertaking it and ensuring that the faculty/department is engaged with the process.
- 7.2.3. Acting as a conduit for any queries / issues raised.
- 7.2.4. Providing feedback on progress of the plan.

7.3. Business Continuity Co-ordinators (Department level)

- 7.3.1. Attending relevant training and awareness sessions to develop knowledge and understanding of Business Continuity Management.
- 7.3.2. Completing the required documentation, with assistance/involvement from other members of the department.
- 7.3.3. Ensuring Business Continuity documentation remains fit for purpose and up to date.
- 7.3.4. Attending corporately run exercises and participate/lead in the running of exercises for the individual department as appropriate.
- 7.3.5. Attending, participating, and sometimes leading debriefs and other events as required to review and test the plan.
- 7.3.6. In some instances, the Co-ordinator will also be the Business Continuity Representative.

7.4. Staff

- 7.4.1. It is important that everyone at the University is aware of the BCM Programme. Staff should be aware of any arrangements in their department's plan that may affect them e.g., how they will be contacted / notified of an incident, where they should report to, if they are not able to access their usual place of work etc.

8. PLAN STRUCTURE AND OPERATION

Each department's Business Continuity Plan has three main components, each of which deals with separate but inter-related aspects of any emergency situation. These components are:

- 8.1. Business Continuity Plan: Activities, including substantial pre-planning and recovery efforts, aimed primarily at assuring that all critical functions and operations continue to be performed during and after any emergency situation.
- 8.2. Risk Assessment and Business Impact Analysis: Assessments based on worst-case scenarios to determine impacts of critical functions caused by disaster situations.
- 8.3. Testing and Review: Instructing all personnel on plan basics (communication, meeting place, priorities, etc), and evaluating competencies through tabletop exercises, drills, and simulations as part of campus testing initiatives.

9. BUSINESS IMPACT ANALYSIS

- 9.1. Business impact analysis (BIA) assist management in identifying critical functions that are essential to the survival of the department. BIA evaluates how quickly a department can return to full operation following a disaster situation. BIA also looks at the type of resources required to resume business.
- 9.2. BIA assumes the worst-case scenario such as infrastructure damage, destruction of records and equipment, absenteeism of essential employees, the inaccessibility of the site for weeks or months. The objective of the BIA is to help departments estimate financial impacts, intangible operational impact, and estimates the recovery time frame.

10. BUSINESS CONTINUITY PLANNING (BCP)

The assumptions made for this Framework are as follows:

- 10.1. In the event of a major business disruption and/or disaster, the University will not be operating at normal capability and performance. The University will be operating at reduced capacity, or a level which is sufficient to perform and maintain critical business functions.
- 10.2. Non-critical business operations will require time to resume full capability, capacity, and performance.
- 10.3. The University adopts a model that includes an organisation wide plan, where required.
- 10.4. Areas have to be identified by Business Impact Analysis.
- 10.5. Resources will be prioritised and made available based on the minimum requirements of all Faculties and Divisions in a disruption environment.
- 10.6. In accordance with best practice standards the University will incorporate the following elements:

Element	Responsibility	Frequency	Requirements
Threat Assessment	Business Continuity Manager	Initial, then on annual basis	<ul style="list-style-type: none"> Identify any threats that have the potential to harm the University and necessitate the use of a Business Continuity Plan and Specialist Recovery Plans. Identify sources of disruption risk that have greatest potential to result in activation of a Business Continuity Plan. Identify disruption scenarios which will form the basis for developing strategies that feed into the Business Continuity Plan and Specialist Recovery Plans.
Business Impact Analysis	Business Continuity Manager with Faculty/ Divisional representatives	Initial, then on annual basis	<ul style="list-style-type: none"> Identify recovery priorities. Identify Critical Business Functions, Recovery Time Objective and Maximum Allowable Outage and required resources. Assess potential business continuity events in relation to financial, student, staff, reputational, legal, operational and environmental impacts.
Business Continuity Plan Specialist Recovery Plans	Business Continuity Manager Faculty/ Divisional representatives	Initial, then on annual basis	<ul style="list-style-type: none"> Provide a guide to recover critical business functions during a business disruption including prevention, preparation, response, and recovery/restoration. Allow for a consistent structure and layout, containing unique Faculty and Division considerations based on outputs from the BIAs. Provide a standardized protocol for managing disruption events.
Recovery Strategies	Faculty/ Divisional representatives	Initial, then on annual basis	<ul style="list-style-type: none"> Identify strategies to recover critical business functions including stabilizing the situation and continuing or resuming critical business functions.
Training	Business Continuity Manager	Initial, then on annual basis	<ul style="list-style-type: none"> Maintain an overall awareness and understanding of business continuity principles and preparations.

Element	Responsibility	Frequency	Requirements
Testing and exercising	Business Continuity Manager	Initial, then on annual basis	<ul style="list-style-type: none"> • Testing and exercising should include: <ul style="list-style-type: none"> ○ Critical business functions, resources, infrastructure. ○ Recovery strategies. ○ Communications strategies outlined in the BCP and supporting recovery plans. ○ Recovery and support arrangements with third parties.
Review and Evaluation	Business Continuity Manager with Faculty / Divisional representatives	Every year or Immediately following an incident	<ul style="list-style-type: none"> • Facilitate prompt action when adverse trends are detected, or a non-conformity occurs. • Ensure that the Business Continuity Program continues to be an effective system for managing disruption related risk.

11. ACTIVATION OF THE BUSINESS CONTINUITY PLAN

11.1. Activation of the BCP and supporting specialist recovery plans will be in response to an actual or potential disruption to the University's critical business functions. Potential scenarios include:

- 11.1.1. Loss of key people/human loss.
- 11.1.2. Denial of access to students and/or Staff (Teaching and Non-Teaching) to premises (temporary/permanent).
- 11.1.3. Sustained loss of IT and/or communications systems.
- 11.1.4. Loss of material/critical service.
- 11.1.5. Loss of research.

12. LINKS TO OTHER AREAS

12.1. Risk Management

12.1.1. Business Continuity Management and Risk Management work closely together, as both are concerned with good governance and raising awareness about risks and mitigating them in time. However, the focus of the two areas is different; Business Continuity Management is only concerned with managing those risks or what might be termed as threats or vulnerabilities that could cause a disruption to the University's operations, whereas Risk Management has a wider remit.

12.1.2. BCM may be used as a treatment of some risks identified and noted by the University. When developing business continuity arrangements, priority should be given to treating threats or vulnerabilities identified as being most likely and having the greatest impact.

12.2. Internal Audit

12.2.1. As part of the review and monitoring of the Programme, in addition to the reviews undertaken by the University Business Continuity Manager, Internal Audit has an important role in ensuring that the Business Continuity Management Programme achieves its objectives as set out in this document.

12.3. Information Security

12.3.1. Information security covers the protection of all forms of information and is concerned with ensuring its confidentiality, availability, and integrity.

12.3.2. A key part of the Business Continuity process focuses on protecting against a potential loss of resources, including essential information, thereby ensuring it is stored appropriately and remains available after a disruption. Information Security should be considered when developing alternative arrangements to store/access key information.

12.3.3. The loss of university information either by a loss of access to it or by someone else being able to access it could have serious implications and depending on the severity, would be classed as an incident at department level and also ultimately to the University.

13.AMENDMENTS

This Policy will be reviewed periodically to rectify anomalies, (if any), and to incorporate feedback received from the stakeholders, through impact analysis and deliberations of the Focus Group, constituted by the Vice Chancellor.