BUSINESS CONTINUITY POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	BUSINESS CONTINUITY POLICY
Document Number:	COS/POL/08
Version:	1.0
Document Date:	17-06-2026
Prepared By:	HOD-IT
Reviewed By:	CISO
Approved By:	CEO
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Review Date	Version No.
1	Initial Basic Release	**17-06-2026**	1.0

Contents

1. PURPOSE

- The purpose of this Policy is to establish a framework to ensure that LLP can effectively respond to, manage, and recover from unexpected disruptions affecting business operations, information assets, and technology services.
- This Policy aims to minimize operational impact, protect critical business processes, ensure availability of essential services, and maintain confidentiality, integrity and availability of organizational information during disruptive events such as system failures, cybersecurity incidents, infrastructure issues, natural disasters, or third-party service interruptions.

2. SCOPE

- This Policy applies to all business processes, information assets, systems, applications, facilities, and resources of LLP.
- The Policy applies to partners, employees, consultants, contractors and third-party service providers involved in managing or supporting critical business operations.

3. POLICY STATEMENT

- LLP shall establish and maintain Business Continuity and Disaster Recovery arrangements to ensure timely recovery of critical operations during disruptive situations.
- The organization shall:
  - (i) Identify critical business processes, systems, information assets, and dependencies;
  - (ii) Assess potential risks and business impact arising from operational disruptions;
  - (iii) Define recovery priorities, responsibilities, and timelines;
  - (iv) Establish documented continuity and recovery procedures;
  - (v) Ensure protection and availability of critical information during emergency situations.

4. BUSINESS CONTINUITY PLANNING

- LLP shall maintain documented Business Continuity Plans covering:
  - (i) Roles and responsibilities of personnel involved in continuity activities;
  - (ii) Emergency response and escalation procedures;
  - (iii) Recovery strategies and required resources;
  - (iv) Communication mechanisms with internal and external stakeholders;
  - (v) Dependencies on third-party service providers.

- Continuity plans shall be reviewed and updated periodically to address changes in business operations, technology, and risk environment.

5. RISK ASSESSMENT AND BUSINESS IMPACT ANALYSIS

- The organization shall conduct appropriate risk assessments and business impact analysis to identify:
  (i) Critical services and processes;
  (ii) Potential disruption scenarios;
  (iii) Impact on business operations;
  (iv) Required recovery objectives and priorities.

- Identified risks shall be evaluated and appropriate preventive and recovery measures shall be implemented.

6. DISASTER RECOVERY AND DATA RECOVERY

- LLP shall maintain Disaster Recovery procedures to support restoration of critical systems and services following major disruptions.

- The organization shall ensure:
  (i) Appropriate backup and recovery mechanisms are implemented;
  (ii) Critical data is protected and recoverable;
  (iii) Recovery procedures are documented and tested;
  (iv) System restoration is performed within defined timelines.

7. TESTING AND CONTINUOUS IMPROVEMENT

- Business Continuity and Disaster Recovery plans shall be periodically tested through appropriate methods such as simulation exercises, recovery drills or table-top exercises.

- Testing results shall be reviewed, gaps shall be identified, and corrective actions shall be implemented to improve effectiveness of continuity arrangements.

8. TRAINING AND AWARENESS

- Personnel involved in business continuity activities shall be provided appropriate awareness and training regarding:
  (i) Their responsibilities during disruptions;
  (ii) Emergency response procedures;
  (iii) Recovery activities and communication requirements.

9. POLICY REVIEW & EXCEPTIONS

- Review annually or earlier or whenever significant changes occur in business operations, technology infrastructure, regulatory requirements, or security risks.
- Exceptions must be documented, risk-assessed, reviewed and approved.