MOREPEN LABORATORIES LIMITED

CIN: L24231HP1984PLC006028

Registered Office: Village Morepen, Nalagarh Road, Near Baddi Distt. Solan, Himachal Pradesh–173 205
Email: plants@morepen.com, Website: www.morepen.com,
Tel.: +91-1795-266401-03, 244590, Fax: +91-1795-244591

Corporate Office: 2nd Floor, Tower C, DLF Cyber Park, Udyog Vihar-III, Sector-20, Gurugram, Haryana-1221016; Email: corporate@morepen.com, Website: www.morepen.com,
Tel.: +91-124-4892000

BUSINESS CONTINUITY POLICY

TABLE OF CONTENTS

1. Policy

1.1 This policy outlines the requirements for developing a Business Continuity Plan to protect the information/ information assets associated with Morepen Laboratories Limited.

2. Purpose

2.1 The purpose of Business Continuity Policy is to minimize the impact on the organization and recover from loss of information/ information assets, systems, applications, equipment and network devices resulting from anticipated or unanticipated events to an acceptable level.

3. Scope

3.1 This policy applies to all employees, consultants, vendor staffs, trainees, and other personnel working for Morepen Laboratories Limited in physically or virtually from any location approved by Morepen Laboratories Limited.

4. Responsibility

The IT HOD is primarily responsible for ensuring adherence to the Business Continuity Policy.

5. Guideline

5.1 Business Continuity

5.1.1. Planning Business Continuity

5.1.1.1 Morepen Laboratories shall develop and implement an effective Business Continuity Plan, in order to mitigate the impacts of all possible service disruptions due to manmade or natural disasters / causes.

5.1.1.2. Business continuity plans shall be developed and implemented to ensure timely resumption of essential services, followed by eventual resumption of all services.

5.1.1.3. Business continuity management shall include controls to identify and reduce risks to the availability of critical services in addition to the general risks assessment process, limit the

consequences of damaging incidents, and ensure that information required for business processes is readily available.

5.1.1.4. Business process owners shall be responsible for reviewing the key events that can cause disruption to their processes are identified and their potential adverse impact are adequately addressed in the Business Continuity Plan.

5.1.1.5. The scope of the Business Continuity Plan (BCP) shall take into account applicable factors including customer requirements, legal regulations and industry requirements. The following but not limited to; shall be considered while implementing BCP:

5.1.1.5.1. Identify critical business functions, applications and supporting technologies.

5.1.1.5.2. Develop an appropriate cost-effective recovery strategy.

5.1.1.5.3 Identify alternate / backup locations with the necessary infrastructure to support the recovery needs.

5.1.1.5.3.1 An updated and documented BCP copy shall be maintained at Morepen Laboratories cloud storage location and with individual BCP actors.

5.1.1.5.3.2 Application code and configuration details backup shall be maintained on a secure remote backup, including its past versions in the version control.

5.1.1.5.3.3 Backup schedules, successful backup and backup capacity shall me managed by IT HOD having the overall responsibility.

5.1.1.5.3.4 Data Backup & Storage

- Data backups: Production databases are backed up every day through automated jobs.
- Critical applications are backed up twice a day. One incremental and full backup during the midnight.
- For Gurgaon file servers, one incremental backup is done during the day. Weekly, full backup is taken.
- Customer data backup is taken once a day.
- The backup data shall be store in an encrypted format.
- Location: The primary database is located in Gurgaon and the backup is taken on hard drives and one copy of backup is stored on Azure cloud.

- Employee Data Backup: When an employee exits the organization, the employee data, emails and files are dumped on the cold storage of Azure.

5.1.1.5.4. Identify the management and membership of the disaster response and recovery teams.

5.1.1.5.5. Identify and document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan.

5.1.1.5.6. Train the recovery teams in the performance of their specific tasks; and

5.1.1.5.7 Develop an ongoing testing and maintenance program to ensure that all processes are in a constant state of recovery readiness.

5.1.2. Implementing Business Continuity

5.1.2.1. BCP policy/ plan shall be protected and considered confidential information. BCP policy/plan shall be stored securely.

5.1.2.2. BCP shall be designed such that restoration or maintenance of business operations is done in the required time following any interruption of service or disaster. Therefore, the following elements, at a minimum shall be included in the plan:

5.1.2.2.1. Failover conditions or requirements necessary to invoke the plan.

5.1.2.2.2. Recovery sequence and dependency map of critical systems, applications, and processes.

5.1.2.2.3 Documentation of all systems, resources or assets necessary for recovery.

5.1.2.2.4 Documentation of all roles, responsibilities, and reporting structures during the execution of the BCP.

5.1.2.2.5 Training and education schedule for all affected or involved personnel.

5.1.2.2.6 Testing and updated schedule for the plan.

5.1.3. Verify, Review and Evaluate Business Continuity

5.1.3.1 Verify

5.1.3.1.1 Ensure that all aspects of the business continuity plan are documented comprehensively. This includes emergency response procedures, recovery strategies, and communication plans.

5.1.3.1.2 Conduct adequate tests and exercises to verify the effectiveness of the BCP. This can include tabletop exercises, simulations, and full-scale drills to validate response procedures and identify gaps.

5.1.3.1.3 Assess various scenarios that could disrupt operations (e.g., natural disasters, cyber-attacks) and verify that the BCP addresses these adequately.

5.1.3.1.4 Identify dependencies on critical infrastructure, suppliers, and key personnel, and verify that contingency plans are in place to address disruptions.

5.1.3.2 Review

5.1.3.2.1 Conduct periodic risk assessments to identify new threats or changes in existing risks that may impact business continuity. Update strategies accordingly.

5.1.3.2.2 Evaluate the resilience of IT systems, data backups, and recovery capabilities. Ensure that technological solutions support rapid recovery and minimal downtime.

5.1.3.2.3 RTO and RPO are calculated and defined as below:

Recovery Time Objective (RTO): RTO has been accepted as 30mins.

Recovery Point Objective (RPO): RPO has been accepted as 5mins.

** Recovery Time Objective (RTO): RTO defines the maximum permissible time that a system resource can remain unavailable before there is an unacceptable impact on other systems resources and business functions.
** Recovery Point Objective (RPO): RPO represents the point in time, prior to a disruption or system outage, to which business process data must be recovered (given the most recent backup copy of the data) after an outage.

** The BCP policy shall be reviewed and updated on an annual basis in conjunction with the BCP plan, Risk assessment.

** MLL shall setup a Disaster Recovery (DR) site to ensure that organization can continue operating in the event of a major disruption or disaster.

5.1.3.3 Evaluate

5.1.3.3.1 Evaluate performance against defined metrics such as RTO & RPO regularly.

5.1.3.3.2 Analyze past incidents and disruptions to identify lessons learned and areas for improvement in the BCP. Use post-incident reviews to refine strategies and response procedures.

5.1.3.3.3 Gather feedback from stakeholders, including employees, customers, and suppliers, on their experiences during disruptions. Use this feedback to improve communication and response efforts.

6. Information Security in Business Continuity

6.1 Information Security during disruption

The organization shall plan how to maintain information security at an appropriate level during disruption to protect information and other associated assets.

6.2 ICT readiness for Business Continuity

Information and Communication Technology (ICT) readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

7. Crisis Management: Coordination, Communication and Training

7.1 BCP Coordinator

a. The BCP Coordinator (BCPC), when indicated, declares an emergency and activates the BCP.

b. The IT HOD is designated as the BCP Coordinator (BCPC). In the event the IT HOD is not available to respond, the responsibility will automatically be delegated to backup/ reserved authorized personnel.

7.2 Communication

The available Information Technology department members shall assist the IT HOD in formulating the communication information.

Appropriate and adequate communications shall be done with all relevant stakeholders.

7.3 Notification Procedures

a. A user may notify the BCP Coordinator as per the Incident Reporting process. All known information must be relayed to the BCP Coordinator.

b. The BCP Coordinator will invoke the BCP, as warranted by the reported event/incident.

The inherent BCP shall be implemented and handled as an incident, through the Incident Management Plan to be resolved through emergency procedures.

8. Enforcement

All employees are expected to comply with the Business Continuity Policy. Non-compliance may result in disciplinary action or punishment, which shall vary as per the severity of the incidence.