Netweb TECHNOLOGIES

BUSINESS CONTINUITY PLAN

1. PURPOSE

The primary purpose of this Business Continuity Plan (BCP) is to strengthen the resilience of Netweb Technologies India Limited ("NTIL") by building its capability to proactively detect, prevent, mitigate, and respond to disruptive events.

In the event of disruption, this BCP ensures NTIL's critical operations can continue with minimal interruption, recover efficiently, and resume normal activities swiftly.

The Plan aims to:

- Safeguard the continuity of operations by minimizing damage to premises, personnel, infrastructure, records, and reputation.
- Establish a structured framework for delivery of critical services during unexpected events or emergencies.
- Incorporate lessons learned, recent threats, and organizational changes through a *regular review* mechanism.

2. SCOPE

This BCP is activated in case of significant disruptions or disasters and covers:

- Restoration of critical and priority services vital for day-to-day operations.
- All employees, contractors, vendors, third-party service providers involved in business continuity efforts.
- All systems, operations, infrastructure, and records critical to NTIL's survival and client commitments.

Note:

- Routine operational issues or daily problem-solving activities are not within the scope.
- Extreme catastrophic events (e.g., nuclear war) are beyond the scope.

3. OBJECTIVES

This BCP is designed to:

- Guide NTIL's leadership teams with a clear action and decision framework during emergencies.
- Provide detailed procedures for rapid recovery and restoration of normal operations.
- Ensure minimal confusion through structured emergency response plans and regular testing.
- Identify alternate suppliers, infrastructure, and contingency plans.
- Ensure reliable data recovery from backups (Cloud-based) in case of data loss.
- Protect critical records and make them readily retrievable.

4. KEY PRINCIPLES

- **Resilience:** Build resistance into NTIL's operations against any foreseeable disruption.
- **Recovery:** Enable rapid restoration of critical activities following an incident.
- **Responsiveness:** Ensure timely communication internally and externally to mitigate impact.
- **Responsibility:** Clearly assign roles for executing continuity and recovery tasks.
- **Review:** Regularly audit, update, and test this Plan to incorporate improvements.

5. OPERATIONAL PREREQUISITES FOR RECOVERY

- Key personnel (or designated alternates) will be available to manage recovery.
- Critical data, applications, and resources are regularly backed up and stored securely offsite (Cloud).
- Infrastructure and critical records are protected with built-in redundancies.
- External support (emergency services, suppliers) may be engaged as needed.

6. ORGANIZATIONAL STRUCTURE FOR BCP

a) **Business Continuity Manager (BCM):** The Business Continuity Manager (BCM) is responsible for the overall coordination, management, and execution of the Business Continuity Plan during disruption.

The responsibilities will include:

- Lead the Emergency Management and Recovery Team (EMRT) and communicate with internal and external stakeholders during emergencies.
- Evaluate and assess damage, recommend recovery actions, and determine the financial and operational impacts of business interruptions.
- Set restoration priorities based on damage assessments and coordinate restoration activities with insurance providers and government agencies.
- Maintain regular communication with customers and suppliers to reinforce stakeholder confidence during disruptions.
- Coordinate disaster recovery efforts, including disaster declaration, mobilization of recovery resources, and restoration of normal business activities.

b) **Emergency Management and Recovery Team (EMRT):** The Emergency Management and Recovery Team (EMRT) is responsible for the operational execution of the recovery tasks, performing damage assessments, communicating with employees, and providing emergency support during and after a disaster. Each EMRT member is required to designate an alternate and ensure that emergency contact details are updated regularly. Both physical and cloud-based access to these details must be maintained for easy retrieval.

Support Activities:

- Evacuation or facility shutdown: Upon the declaration of an emergency, the team will ensure necessary actions, such as evacuating personnel or shutting down operations, are carried out promptly. They will also initiate communication with employees.
- Recovery support: Provide direct recovery assistance to the affected operations, including restoring services to operational status.
- Recovery of communication systems: Work to recover essential systems such as voicemail and email systems as a priority.
- Review of operational requirements: Assess the minimum acceptable operational requirements and ensure sufficient resources are available to support ongoing business operations.
- Work with management: Collaborate with management to recover critical systems, applications, and infrastructure at designated recovery sites.

c) **IT/Technical Support Team:** Restores IT infrastructure, salvages equipment, ensures data recovery from the Cloud, and sets up alternate IT operations.

7. KEY OPERATIONAL COMPONENTS

- **Emergency Communication Framework**

  - Maintain a centralized, Cloud-based emergency contact database.
  - Contact includes employee family numbers, customer contacts, and service provider contacts.
  - Implement multi-channel alerts (email, SMS, fire alarms, exit signage, etc.)

- **Data Backup & Recovery**

  - Full and incremental backups performed regularly.
  - Cloud server redundancy maintained.
  - Random backup audits and restoration drills conducted.
  - Immediate Cloud access provided to key personnel during disruption.

8. EVENT-SPECIFIC RESPONSE PROTOCOLS

- **Natural Disaster Response**

  - Immediate notification to CMD.
  - Employee evacuation and activation of remote working protocols (e.g., "work from home").
  - Rapid server backup recovery tests.
  - Communicate with clients and other stakeholders regarding continued service availability

- **Fire Incident Management**

  - Categorize fire severity (Minor/Major).
  - Attempt extinguishing minor fires; evacuate on major fires.
  - Activate fire alarms, alert EMRT and Building Security.
  - Prevent unauthorized access to the disaster site

- **Water Damage/Flood Response/ Earthquake, terror, riots**

  - Assess intrusion severity.
  - Power down critical equipment if necessary.
  - Evacuate affected areas.
  - Alert relevant department if external support required.

9. INSTRUCTIONS FOR USING THE PLAN

a. **Invoking the Plan**

The Business Continuity Plan becomes effective upon the occurrence of a disaster or significant disruption that impacts normal business operations. The BCM is responsible for initiating the Plan, coordinating its implementation, and ensuring that all team members are activated according to the prescribed procedures. The Plan remains in effect until operations are fully restored either at the original location or a designated alternative site. Once the operations have been fully restored, control will be returned to the appropriate functional management.

b. **Disaster Declaration**

The BCM holds the responsibility for declaring a disaster, specifically for technical operations. Upon such a declaration, the BCM will promptly notify the EMRT. This notification will activate the recovery efforts outlined in the Plan. The EMRT, under the direction of the BCM, will then proceed with the damage assessment, recovery actions, and resource mobilization as per the defined recovery strategy.

10. DISASTER DECLARATION PROCESS

Once a disaster is declared, the EMRT is mobilized to initiate and coordinate the recovery efforts. The team remains at the affected site to perform a preliminary damage assessment (if permitted) and gather critical information.

a. **Conduct detailed damage assessment:** Under the direction of local authorities, EMRT will:

- **Assess Damage to Physical and Digital Records:** Conduct on-site inspections to assess damage to essential hardcopy records (e.g., files, manuals, contracts, documentation) and electronic data.
- **Evaluate Facility Damage:** Inspect the physical structure for any environmental conditions or damage to furniture, fixtures, and other infrastructure. Vendors or providers of installed equipment should be consulted for expert opinions on equipment conditions.
- **Develop Restoration Priority List:** Identify vital records and equipment that are critical for business recovery and can be restored quickly to resume operations.
- **Develop Salvage Priority List:** Identify records, assets, or sites that can be salvaged for future recovery.
- **Resource Requirements:** Make recommendations on the resources needed for recovery.
- **Evaluate Recovery Phase:** Decide whether to enter the long-term business recovery phase (for severe, extended disruptions) or if recovery efforts can be completed in a shorter period, allowing work to return to the primary location.

b. **Determine whether to continue to business recovery phase**

Based on the gathered information from the damage assessment, the EMRT will evaluate whether it is necessary to move into the Business Recovery Phase of the plan. If the situation does not require full recovery efforts, the EMRT will continue addressing the situation at the affected site, while providing regular updates to the Business Continuity Manager.

11. BUSINESS RECOVERY PHASE

The Business Recovery Phase includes the necessary steps to fully restore systems, facilities, and operations, especially if the disruption is expected to last for an extended period.

a. System and facility operations requirement: Re-establishing normal operations will require the restoration of the Company's system and facility configurations. These configurations are crucial for ensuring that services are fully operational and can be sustained in the recovery phase.

b. Recover data from third party provider: Data required for resuming normal business operations (e.g., customer details, operational records, legal documentation, insurance records) will be retrieved from Cloud-based backups. The designated IT/Technical Support

staff will be responsible for recovering the data from the cloud, ensuring its availability for use at the recovery site or remotely, allowing business operations to continue.

c. **Operations recovered**: Once the relevant operations have been restored, and employees are in place to support the operations, the Company will declare that normal business activities are functioning again, either at the recovery site or a designated location.

12. EMPLOYEE TRAINING AND DRILLS

Employee readiness is critical to ensure effective response and recovery during emergencies. All employees must actively follow the Business Continuity Policy, ensuring both their health and safety. The Company encourages employees to take a proactive approach in identifying potential hazards and reporting them to supervisors.

➢ Training and Drills

- **New Hire and Periodic Training:** New employees will receive orientation on emergency procedures, and existing employees will undergo regular training to ensure their preparedness.
- **Training Focus:**
  - Individual roles and responsibilities during an emergency.
  - Information on various threats, hazards, and protective actions.
  - Notification, warning, and communication procedures.
  - Procedures for locating family members in an emergency.
  - Emergency response, evacuation, shelter, and accountability procedures.
  - Location and usage of common emergency equipment.
  - Emergency shutdown procedures.

➢ Drills and Exercises

Employees will participate in various drills and exercises that simulate real-life emergency situations. These will include:

- Fire drills.
- Evacuation drills.
- Business continuity scenario exercises. These exercises will be used to assess and reinforce the preparedness and response capabilities of the staff.

13. PLAN REVIEW, TESTING, AND UPDATES

- Annual Review: Full policy and contact list review each year.
- Regular Testing: Annual drills (mock fire, evacuation, IT failover simulation) and disaster equipment recovery testing.
- Continuous Improvement: Incorporate findings from incidents and drills into updated versions of BCP.
- Secure Storage: Latest BCP version stored physically and on Cloud, accessible to BCM and EMRT

14. REVIEW AND REVISION

This policy will be reviewed periodically to ensure its effectiveness and compliance with evolving laws and best practices. Updates or revisions will be communicated to all employees.

****

APPENDIX A: EMERGENCY CONTACT LIST

1. Business Continuity Manager

Name	Email Address
Hemant Agrawal	hemant@netwebindia.com

2. Emergency Management and Recover Team

Name	Email Address
Mukesh Golla	mukesh@netwebindia.com
Anuj Kumar	anuj@netwebindia.com

3. IT/Technical Support Member

Name	Email Address
Rohit Kumar	rohit.kumar@netwebindia.com

4. Internal Audit Team

Name	Email Address
Arjun Sirohi	arjunsirohi@netwebindia.com
Machhindra Ghorpade	machhindra.g@netwebindia.com