EPACK Durable Limited

Business Continuity Plan

Objectives

The objective of this Business Continuity Plan ("BCP" or "Plan") is to ensure that EPACK Durable Limited ("Company", "EPACK") handle unexpected emergencies effectively, ensuring critical business processes remain operational and mitigating the severity of impacts on the organization.

- Safety First: Prioritize the health and safety of employees, customers, partners, and the community.
- Operational Continuity: Minimize disruption to day-to-day manufacturing and business operations.
- Resource Prioritization: Identify and secure critical resources (personnel, equipment, and data) necessary to sustain essential services.

Scope

This BCP applies to EPACK Durable Limited and its subsidiaries.

1. Incident Classification and Escalation

The Company to classify incidents based on severity, operational impact, and recovery complexity to ensure timely escalation and decision-making.

Incident Level	Description	Escalation Authority
Level 1	Minor operational disruption with limited impact	Plant Head
Level 2	Significant disruption affecting production or systems	CEO / Senior Management
Level 3	Enterprise-wide crisis causing prolonged shutdown	Managing Director / CEO and, where required, the Risk Management Committee and Board

2. Risk Scenarios Covered Under the BCP

The Plan covers, but is not limited to, the following scenarios:

- Fire Incident
- Natural Disasters
- Technical/System Failure
- Cyber Resilience and Information Security
- Supply Chain Disruption Management

The Company may periodically conduct Business Impact Analysis (BIA) to assess critical business functions and operational dependencies.

3. Recovery Objectives

The Company may identify recovery priorities, indicative recovery timelines, and data restoration requirements for critical business processes and information systems, based on the nature and severity of disruption.

- Recovery Time Objective (RTO): The targeted maximum duration within which a disrupted activity, process, or system must be restored following an incident.
- Recovery Point Objective (RPO): The maximum tolerable data loss measured in time prior to disruption.

4. Emergency Response Procedures

a. Fire Incident

Immediate Actions

i. Raise Fire Alarm Immediately

Any employee identifying smoke, fire, sparks, burning smell, or abnormal heat generation shall immediately activate the nearest fire alarm call point without delay. Early alarm activation is critical to minimize injury, loss of life, and property damage. Employees shall also verbally warn nearby personnel if safe to do so.

ii. Inform Emergency Response Team and Security

The incident shall immediately be reported to:

- Plant Head / In-charge
- EHS (Environment, Health & Safety) Team

Employees trained in emergency response procedures may take reasonable measures to control minor incidents using appropriate safety equipment, subject to safety considerations

Recovery Actions

i. Assess Damage to Facility and Equipment

After the fire is controlled and the area is declared safe:

- A detailed damage assessment shall be conducted for buildings, machinery, electrical systems, inventory, IT systems, and utilities.
- Root cause analysis shall be initiated to determine origin and contributing factors.
- Photographic and documentary evidence shall be collected for insurance and regulatory purposes.

Assessment shall include operational, financial, environmental, and safety impacts.

ii. Restore Utilities and Operations

Operations shall resume only after formal clearance from:

- Local fire authorities (where applicable)
- Plant Management

b. Natural Disasters

Natural disasters such as earthquakes, floods, cyclones, storms, lightning, extreme rainfall, heatwaves, landslides, or other severe environmental events may significantly impact manufacturing operations, employee safety, infrastructure, utilities, supply chains, and business continuity.

During Disaster

i. Suspend Plant Operations if Required

Upon identification of a severe natural disaster threat or warning issued by government authorities, management may initiate partial or complete suspension of plant operations to ensure employee safety and prevent damage to facilities and equipment.

ii. Evacuate Employees Where Necessary

Where there is risk to human life or safety, immediate evacuation shall be initiated in accordance with emergency evacuation procedures.

Plant heads or supervisors shall ensure:

- Complete evacuation of their respective areas,
- Proper headcount verification,
- Immediate reporting of missing personnel.

iii. Protect Critical Equipment and Documents

Where time and safety conditions permit, designated teams shall take reasonable measures to protect critical organizational assets.

Priority shall always remain employee safety over asset protection.

iv. Follow Instructions Issued by Local Authorities

The organization shall comply with all directives, advisories, evacuation orders, and emergency instructions as may be issued by:

- Disaster management authorities
- Meteorological departments
- Other competent government authorities.

Post-Disaster Recovery

i. Conduct Structural and Safety Assessment

After the disaster subsides, detailed inspections and assessments to be conducted before resumption of operations.

Assessment activities shall include:

- Structural integrity inspection of buildings
- Inspection of machinery, utilities, and electrical systems
- Identification of damage, leakages, cracks, or contamination
- Evaluation of fire protection systems

Only qualified personnel or authorized external experts shall certify operational safety of the facility.

ii. Prioritize Critical Manufacturing Activities

Following disruption, management shall prioritize restoration of critical business and manufacturing functions based on:

- Customer commitments
- Product criticality
- Regulatory obligations
- Inventory availability
- Revenue impact
- Supply chain dependencies

iii. Coordinate with Suppliers and Logistics Providers

The Supply Chain and Procurement team shall engage with:

- Raw material suppliers
- Transport and logistics partners
- Customers and distributors

The objective shall be to:

- Assess supply chain disruptions
- Identify material shortages
- Determine transportation constraints
- Arrange alternate suppliers or routes
- Minimize delays in production and delivery commitments.

c. Technical / System Failure

Technical or system failures may include breakdown of production machinery, ERP failure, server outage, network disruption, software malfunction, database corruption, cyber incidents, communication failure, power instability, automation failure, or any disruption affecting critical business and manufacturing operations.

Response Actions

i. Report Issue to IT Team Immediately

Any employee identifying a technical malfunction, system error, network issue, abnormal system behaviour, unauthorized access attempt, or operational disruption shall immediately report the incident to IT Department.

ii. Activate Backup Systems and Servers

Upon confirmation of system disruption, the IT Team shall initiate predefined backup and disaster recovery procedures to maintain continuity of critical operations.

This may include:

- Activation of backup servers
- Switching to redundant network infrastructure
- Restoration of cloud-based systems

iii. Restrict Unauthorized Access During System Restoration

During system failure investigation and restoration activities, strict access control measures shall be implemented to prevent:

- Unauthorized system access
- Data breaches
- Malware propagation
- Accidental data corruption
- Cybersecurity vulnerabilities

Only authorized IT personnel shall be permitted to access affected systems and infrastructure.

Recovery Actions

i. Restore Systems Using Latest Backups

The IT Team shall restore affected systems, applications, databases, and operational platforms using the latest verified backups.

Recovery activities may include:

- Data restoration
- Server rebuilding
- Software reinstallation
- Network reconfiguration
- Cybersecurity patch deployment
- Recovery of production control systems

ii. Verify Integrity and Functionality of Restored Data

After restoration, the IT Team and concerned business functions shall validate:

- Accuracy and completeness of restored data
- System functionality
- Application performance
- User accessibility
- Integration between systems
- Security controls and permissions

iii. Monitor Systems for Abnormal Activity

Following restoration, enhanced monitoring shall be conducted to identify:

- Recurring system failures
- Cybersecurity threats
- Unusual network activity
- Unauthorized access attempts
- Performance degradation
- Data synchronization issues

d. Cyber Resilience and Information Security

The Company shall establish and maintain robust cyber resilience and information security mechanisms to protect critical business information, manufacturing systems, digital infrastructure, operational technology (OT), and information technology (IT) systems from cyber

threats, unauthorized access, data breaches, ransomware attacks, malware infections, system failures, and other cybersecurity incidents.

Preventive Measures

i. Firewall and Antivirus Protection

The Company shall implement appropriate firewall, endpoint protection, antivirus, and anti-malware solutions across critical systems and networks to prevent unauthorized access, malicious attacks, and harmful software intrusion.

ii. Multi-Factor Authentication (MFA)

The Company to implement appropriate cyber security controls such as firewalls, access restrictions, anti-malware solutions, multi-factor authentication, periodic patching, and employee awareness measures, based on risk assessment and operational requirements.

Authentication mechanisms to include:

- OTP verification,
- Authentication applications,
- Biometric verification,
- Hardware security tokens.

iii. Restricted User Access Controls

Access to systems, applications, databases, and confidential information shall be granted strictly on a need-to-know and role-based access basis. Inactive accounts, terminated employee access, and unnecessary privileges shall be removed promptly to minimize cybersecurity exposure. Sensitive systems and manufacturing controls shall be accessible only to authorized personnel.

iv. Regular Software Updates and Patch Management

The IT Team shall ensure timely installation of:

- Security patches
- Firmware updates
- Operating system updates
- Vulnerability fixes.

v. Employee Cyber Security Awareness Training

Employees shall receive periodic cybersecurity awareness and information security training to improve organizational resilience against cyber threats.

Training programs shall cover:

- Phishing and email fraud awareness
- Password security practices
- Safe internet and device usage
- Data protection requirements

Employees shall be encouraged to immediately report suspicious emails, unauthorized system activity, or cybersecurity concerns to the IT Team.

Response to Cyber Incident

i. Immediately Isolate Affected Systems

Upon identification of a cybersecurity incident, malware infection, ransomware attack, suspicious activity, or unauthorized access attempt, affected systems shall immediately be isolated from the network to prevent further spread or compromise.

ii. Inform IT Team

The cybersecurity incident shall immediately be reported to:

- IT Department
- Relevant department heads.

Where required, the Company may also notify:

- External cybersecurity consultants
- Regulatory authorities

Incident escalation shall follow predefined communication and reporting protocols.

iii. Assess Extent of Breach or Malware Infection

The IT and cybersecurity teams shall conduct detailed investigation and analysis to determine:

- Nature of the cyberattack
- Systems and data affected
- Source and attack vector
- Extent of malware spread
- Data breach or information compromise
- Operational and financial impact.

iv. Restore Systems from Secure Backups

Affected systems and data shall be restored using verified and secure backups after ensuring removal of malware, vulnerabilities, or unauthorized access mechanisms.

e. Supply Chain Disruption Management

The Company recognizes that disruptions in the supply chain may significantly impact manufacturing operations, production schedules, deliveries, inventory management, and overall business continuity. Supply chain disruptions may arise due to economic, geopolitical, environmental, operational, technological, regulatory, or vendor-related factors.

Potential Disruptions

i. Raw Material Shortages

Manufacturing operations may be affected due to shortage or non-availability of raw materials caused by:

- Supplier production failure
- Market scarcity
- Price volatility
- Quality rejection
- Natural disasters
- Geopolitical instability
- Regulatory restrictions

ii. Transportation Failure

Supply chain operations may be disrupted due to transportation-related failures including:

- Vehicle breakdown
- Transport strikes
- Extreme weather events

iii. Vendor Shutdown

Operations of suppliers or vendors may be interrupted due to:

- Financial instability
- Labor unrest
- Regulatory non-compliance
- Fire or industrial accidents
- Natural disasters,
- Operational shutdowns

Mitigation Measures

i. Maintain Safety Stock

The Company shall maintain appropriate safety stock levels for raw materials, components, packaging materials, and spare parts based on:

- Production criticality
- Lead time
- Supplier dependency
- Historical consumption patterns

ii. Develop Alternate Vendor Base

To reduce dependency on single-source suppliers, the Company shall strive to identify, evaluate, and develop alternate vendors for critical materials and services wherever feasible.

Vendor diversification strategies may include:

- Multiple approved suppliers
- Regional supplier diversification
- Backup procurement arrangements

iii. Monitor Supplier Performance and Risk Exposure

The Procurement and Supply Chain team shall periodically monitor supplier performance and associated risks through:

- Vendor evaluations
- Delivery performance reviews
- Quality assessments
- Compliance reviews

5. Plan Maintenance and Testing

The Company may periodically conduct awareness sessions, walkthroughs, tabletop discussions, or simulation exercises to assess preparedness and identify improvement areas:

- Tabletop Exercise: Hypothetical scenario discussions with senior officials to identify plan weaknesses without mobilizing resources.
- Functional Exercise: Realistic simulations involving the short-term mobilization of personnel and equipment to test functional capabilities.

6. Additional Crisis Considerations

- Media Communications: Only personnel authorized by the management shall communicate with external stakeholders, regulatory authorities, or media to ensure consistent and controlled communication..
- Neighbouring Facilities: Keep nearby facility managers informed of potential dangers and coordinate for mutual safety.
- Pandemic-Specific Measures: If applicable, implement temperature checks at entrances, sanitization of transit areas twice daily, and interpersonal distancing.

7. Review & Update

This Plan may be reviewed and updated from time to time based on business requirements, operational experience, regulatory developments, and changes in applicable laws.

Overall oversight of business continuity and related risks shall rest with the management and the Risk Management Committee in accordance with the Company's governance framework. The Board of Directors of EPACK Durable Limited shall have the authority to amend, modify, or update this Policy, as may be necessary, from time to time. This Policy shall remain valid and in force on an ongoing basis from the date of its approval and shall continue to remain effective unless revoked by the Board of Directors.

8. Version Control

Version	Description	Date
Version 1	Business Continuity Plan	August 11, 2026