Information Technology Policy - Prima Plastics Limited

VERSION CONTROL	
Information Technology Policy	
Version Number	V1
Date Approved	
Effective Date	21 May 2026
Supersede Version	-

1. Introduction

This Information Technology (IT) Policy describes the framework in accordance with the Internal policies and practices of the Company.

Prima Plastics Limited ("Company") has built a comprehensive IT Governance framework for measuring, monitoring and managing the technology and cyber security risk arising from the usage of technological hardware and software in the Company. The central theme of the IT framework is the management of the Company's entire technology ecosystem with a view to ensure operational resilience of the IT system and robust cyber security crisis management.

2. Objective

The IT Policy serves the following objectives:

a. To establish and develop a robust IT framework in the Company
b. To prepare the Company and its stakeholders for cyber crisis and assess and mitigate cyber risks effectively and efficiently
c. To incorporate governance best practices pertaining to information technology
d. To define the access and password management protocols for the Company
e. To define the roles and responsibilities for Board of Directors and Senior Management in IT Risk Management
f. To define the procedures for data backup and restoration

3. Maintenance, Review and Approval of Policy

The undersigned shall be responsible to own, maintain and update this policy by engaging with relevant functional units. The Policy shall be reviewed by Mr. Dharmesh R. Sachade, Chief Financial Officer and the policy shall be subsequently put up for final approval before the Board of Directors.

Sd/-	Sd/-
Ms. Nehal Goyal **(Company Secretary)**	**Mr. Dharmesh R. Sachade** **Chief Financial Officer**

The policy shall be reviewed on an annual basis to ensure relevance and compliance with the applicable statutory provisions.

4. Access Management

- Access to system and software is granted strictly on a "Need-to-Know" basis where a valid business need exists. Access to systems (ERP, Email, File Servers) is granted based on the basis of user's role, not seniority.
- Personnel with elevated system access entitlements are closely supervised with all their systems activities logged and periodically reviewed.
- Company has adopted multi-factor authentication for privileged users of
    i. critical information systems; and
    ii. for critical activities

- User Lifecycle:
    - Creation: Requires written approval from HR and Department Head
    - Modification: Reviewed upon transfer/promotion, if any.
    - Revocation: Access is disabled immediately upon exit from the organisation and external email access is stopped upon resignation
- Department Heads perform a User Access Review (UAR) periodically, i.e., on a quarterly basis.

5. Password Management

- All user access passwords must be a minimum of eight (8) characters. To ensure strength, they include a combination of alphabetic characters, numbers, and at least one special character.
- Passwords shall not be shared, written down, or stored in any open, unsecured, or visible format where they may be easily compromised.
- Passwords shall not be stored or transmitted in plain text (readable form). Appropriate encryption or hashing must be used during storage and transmission.
- Initial passwords must be communicated to users through secure channels. The system must force a mandatory password change immediately upon the user's first login.
- All system-generated or vendor-supplied default passwords must be changed before any software or hardware is deployed into the production environment.
- Passwords for critical or privileged accounts (e.g., Administrators, Root users) must be changed at least every sixty (60) days.
- The system shall notify users to change their passwords at defined regular intervals. Regardless of the rotation schedule, passwords must be changed immediately if there is any suspicion of compromise or accidental disclosure.

6. Roles and Responsibilities

Well-defined roles and responsibilities of Board and Senior Management are critical, while implementing IT Governance. Some of the roles and responsibilities include:

a. Board of Directors

- Ensure that the Company has put in place processes for assessing and managing IT and cybersecurity risks
- Guide in preparation of IT Strategy and ensure that the IT Strategy aligns with the overall business objectives
- Satisfy itself that the IT Governance framework is effective and efficient and has well defined objectives and unambiguous responsibilities for each level in the organisation
- Review the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery Management annually.

b. Senior Management

- Execute the Board approved IT Framework
- Create a culture of IT risk awareness and cyber hygiene practices in the Company
- Assist the Board in IT Planning and ensuring efficiency and effectiveness of the framework
- Ensure implementation of a robust IT framework meeting statutory and regulatory compliance
- Put in place an effective Disaster Recovery (DR) setup and Business Continuity Plan (BCP)

7. Cyber Incident Response

- This policy intends to develop and implement processes for preventing, detecting, analysing and responding to information security incidents.
- Company addresses the classification and assessment of incidents; including a clear communication strategy and plan to manage cyber incidents, contain exposures and achieve timely recovery.
- Company analyses cyber incidents for their severity, impact and root cause and takes measures, corrective and preventive, to mitigate the adverse impact of incidents on business operations.
- Company has written incident response and recovery procedures including identification of key roles of staff/ outsourced staff handling such incidents.
- Company has clear communication plans for escalation and reporting the incidents to the Board and Senior Management, as required.
- Company ensures effectiveness of crisis communication plan by specifying a clear Escalation Matrix.

8. Approval Matrix and Escalation Matrix

Approval Matrix

Function	Approval Authority	Backup/ Alternate Authority
New IT User Creation	HoD	IT
System Modification	IT	CFO
Incident Reporting	HoD	IT
Data Restoration	IT	CFO
Vendor Onboarding	HoD	CFO

Escalation Matrix

Severity Level	Description	Escalation Timeline	Stakeholders Informed
Critical	Enterprise-wide outage, Data Breach, Ransomware	Immediate	CFO, MD, CS
High	Critical Dept Down (e.g., Dispatch/ Accounts)	1 hour	IT, HoD
Medium	Single User/ Non-critical system issue	4 hours	IT

9. IT Infrastructure Management

- Maintain a detailed inventory of Information Asset with distinct and clear identification of the asset.
- Avoid using outdated and unsupported hardware or software and shall monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis.
- Develop a technology refresh plan for the replacement of hardware and software in a timely manner before they reach End-of-Support (EOS) date.

- Adoption of new or emerging technologies shall be commensurate with the risk appetite and align with overall Business strategy of the Company. It should facilitate optimal creation, use, or sharing of information by a business in a secure and resilient way.

10. IT Risk Management Framework

- The Company has implemented comprehensive internal controls and processes to mitigate/ manage identified risks. The implemented controls and processes are reviewed periodically on their efficacy in a risk environment characterised by change.
- The Company has defined roles and responsibilities of stakeholders (including third-party personnel) involved in IT risk management. Areas of possible role conflicts and accountability gaps are specifically identified and eliminated or managed;
- Identification of critical information systems of the organisation and fortification of the security environment of such systems; and
- Definition and implementation of necessary systems, procedures and controls to ensure secure storage/ transmission/ processing of data/ information.

11. Data Leakage Prevention (DLP)

- The Company has implemented DLP tools to monitor email, file transfers, USB devices.
- There are restrictions on forwarding confidential data outside the organization.
- The staff is well-advised to not share confidential data over emails. However, if the same is necessary, watermarking and encryption of sensitive documents is done before sharing.

12. Data Backup and Restoration

a. <u>Scope and Classification of Critical Data</u>

- The IT Department shall identify and classify "Critical Business Data" essential for the Company's continued operation and statutory compliance. This scope includes, but is not limited to:
    - ERP Databases: Financial transactions, Inventory, and Supply Chain records.
    - Intellectual Property: Formulations, CAD designs, Moulds, and R&D data.
    - Operational Technology (OT): SCADA/PLC configurations and machine controller logic.
    - Corporate Functions: HR records, Legal contracts, and Email archives.

b. <u>Data Backup Strategy</u>

- To ensure resilience against data loss, hardware failure, or ransomware attacks, the Company shall strictly adhere to the 3-2-1 Rule:
    - Three (3) Copies: Maintain at least three copies of data (Production data + 2 Backup copies)
    - Two (2) Different Media: Use two different storage media types (e.g., Disk-based local storage and Magnetic Tape or Cloud Storage) to prevent media-specific failures.
    - One (1) Offsite Copy: Keep at least one copy in a physically separate location to protect against site-level disasters (fire, flood).

c. <u>Backup Frequency and Schedule</u>

Backups must be automated to minimize human error and adhere to the following schedule based on data criticality:

- Critical Data (High Availability): Daily Incremental Backups (at close of business) and Weekly Full Backups (during non-peak hours).
- Non-Critical / Static Data: Weekly or Monthly Full Backups.
- Endpoint Data: Key personnel laptops shall be configured for automatic background syncing to the corporate server/cloud to prevent data loss from device theft or failure.

d. Encryption and Security

- All backup data must be encrypted using industry-standard algorithms, both, while being transferred and when stored.
- Access to backup repositories is restricted to authorized IT personnel only.
- To defend against Ransomware, the offsite/cloud backup must be configured as "Immutable" or "Read-Only" for a defined period, preventing deletion or alteration by attackers.

e. Restoration Testing (Audit & Compliance)

- Merely taking backups is insufficient. The IT Team must conduct Annual Restoration Drills on a random sample of critical data to verify integrity and recoverability
- A "Restoration Log" detailing the date of test, data set used, time taken to restore (RTO), and outcome (Success/Failure) must be maintained for review by Internal Auditors.

f. Data Retention & Purging

Data shall be retained for sufficient period of time depending on the statutory requirements and internal policies of the company, vis-à-vis, Policy on Preservation of Documents and Archival Policy. Broadly, the documents and retention thereof can be categorised as below:

- Statutory Records (Tax/MCA): 8 Years.
- Employee Records: Duration of employment + 3 Years
- Email Archives: 3 Years.

Data exceeding retention periods must be securely deleted using industry-standard wiping tools to ensure non-recoverability.

13. Phishing Simulations & Awareness

- The IT Department conducts bi-annual phishing simulations.
- Employees failing the simulation undergo mandatory remedial training within 3 days.
- General Information Security Awareness training is mandatory for all new joiners during induction.

Business Continuity Plan and Disaster Recovery Procedure - Prima Plastics Limited

1. Introduction

This Business Continuity Plan (BCP) and Disaster Recover (DR) Procedure describes Company's strategy to set out how the business will operate following cyber crisis and how it expects to return to 'business as usual' at the earliest.

2. Purpose

The purpose of this document is to define the policy to ensure continuity, resumption, and recovery of critical business processes in the event of disruptions.

3. Maintenance and Updation

This document shall be reviewed by the Company from time to time to ensure relevance and compliance with the applicable laws. Compliance to this policy and implementation status shall be evaluated at least annually in keeping with assurance requirements indicated above and reported to the board.

4. Business Continuity Plan

a) Business Continuity Plans (BCP) / Disaster Recovery plans (DRP) shall be developed based on a Business Impact analysis (BIA).

b) BIA shall be conducted / reviewed at least once annually

c) Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) will be identified and considered when establishing the business continuity plans and disaster recovery plans.

d) BCP shall be regularly tested under different scenarios for all possible types of contingencies, to ensure that it is up-to-date and effective. Testing of BCP shall include all relevant aspects and constituents i.e. People, Processes and Resources (including Technology).

e) Periodicity of DR drills for all systems shall be at least on a yearly basis. Any major issues observed during the drill shall be resolved and tested again, to ensure successful conduct of drill before the next cycle. The DR testing shall involve switching over to the DR / alternate site and thus using it as the primary site for sufficiently longer period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.

f) Shall document recovery strategies / details of the actions that the teams will take in order to continue or recover prioritized activities within predetermined timeframes and to monitor the effects of the disruption and the organization's response to it.

g) Shall document on communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate.

h) BCP / DR plans shall be updated / revised based on the outcomes of the tests where required.

i) BCP / DR plans shall be reviewed annually and updated when significant changes are made to the business processes or the underlying IT infrastructure and application ecosystem.

j) BCP / DR shall be considered in all new projects / new initiatives.

k) DR shall be tested for all new applications / infrastructure before deployed in production

l) Data shall be backed up and periodically restored to check its usability. The integrity of such backed up data shall be preserved along with securing it from unauthorised access.

m) In a scenario of non-zero RPO, a documented methodology for reconciliation of data shall be formulated, while resuming operations from the alternate location.

n) Ensure that the configurations of servers, network devices, other products and deployed security patches at the DC and DR are identical.

o) Relevant personnel shall be trained on business continuity and disaster recovery plans and informed about their roles and responsibilities.

p) Documentation of the BCP/DR plans shall be maintained (including off site as necessary) to ensure it is accessible when the business continuity plan or the disaster recovery plan has to be invoked.

q) BCP / DR plans shall also consider vendors / suppliers / third parties as part of establishing, documenting, evaluation / testing and maintaining the BCP / DR plans.

Cyber Incident Response Plan - Prima Plastics Limited

1. Introduction

This Cyber Incident Response Plan ("Plan") formulated by Prima Plastics Limited ("Company") provides practical guidelines on responding to cyber security and data breach incidents in a consistent and effective manner. The plan establishes a team of first responders to an incident with defined roles, responsibilities, and means of communication.

While this plan is primarily oriented around cyber-related incidents and breaches, it can also be utilized for data breaches that are not related to computer systems.

2. Objective

When a cybersecurity incident occurs, timely and thorough action to manage the impact of the incident is a critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

a) Preserve and protect the confidentiality of constituent and employee information and ensure the integrity and availability of the Company's systems, networks and related data.
b) Help the Company personnel recover their business processes after a computer or network security incident or other type of data breach.
c) Provide a consistent response strategy to system and network threats that put the Company data and systems at risk.
d) Develop and activate a communication plan including initial reporting of the incident as well as ongoing communications, as necessary.
e) Address cyber related legal issues.
f) Minimize the Company's reputational risk

3. Incident Response Team

A team comprised of company staff shall be responsible for coordinating incident responses and known as the Incident Response Team (IRT). The IRT shall consist of the individuals listed below, having the noted roles and responsibilities. This team will have both primary members and secondary members. The primary members of the IRT will act as first responders or informed members to an incident that warrant IRT involvement, according to the incident's severity. The entire IRT would be informed and involved in the most severe incidents. IRT members may take on additional roles during an incident, as needed. There shall be a member of the IRT designated as the Incident Response Manager (IRM), who will take on organizational and coordination roles of the IRT during an incident where the IRT is activated for response to the incident.

S.No.	Designation	Role
PRIMARY MEMBERS		
1	Chief Financial Officer	Incident Response Manager (IRM)
2	IT Manager	Executive level manager in charge of Information Technology functions
3	Vice President	Executive level manager in charge of Financial Management, HR and Company Operations
SECONDARY MEMBERS		
4	Company Secretary	Legal Representative

5	Software Vendor	Security event monitoring vendor

4. Incident Response Life Cycle Process

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response process elements that comprise the Cyber Incident Response Plan include:

S.No.	Process Phase & *Approximate Timing*	Process Detail Steps
1	Preparation *Ongoing*	• Ensuring that systems, networks, applications, and data handling processes are sufficiently secure • Ensuring employee awareness training is in place • Practice exercises for the IRT are conducted periodically
2	Identification *Few Hours*	• Identify and confirm that the suspected or reported incident has happened and whether malicious activity is still underway. • Determine the type, impact, and severity of the incident. • Take basic and prudent containment steps.
3	Notification *1 Day*	• Inform or activate the IRT, based on the severity of the incident, and provide the type, impact, and details of the incident to the extent that they are known. • Determine the need for Subject Matter Experts (SME) to be involved in the Containment, Eradication, and Recovery processes.
4	Containment *2 Days*	• Take immediate steps to curtail any on-going malicious activity or prevent repetition of past malicious activity. • Re-direct public facing websites, if needed. Provide initial public relations and legal responses as required.
5	Eradication *Few Days*	• Provide full technical resolution of threat and related malicious activity. • Address public relations, notification, and legal issues.
6	Recovery *Few Weeks*	• Recover any business process disruptions and re-gain normal operations. • Address longer term public relations or legal issues, if required, and apply any constituent remedies.
7	Post-Incident *Few Months*	• Formalize documentation of incident and summarize learnings. • Apply learnings to future preparedness.

5. Communication Methods

Company communication resources (email, phone system, etc.) may be compromised during a severe incident. Primary and alternate methods of communication using external infrastructure shall be established and noted on the IRT member contact list to provide specific methods of communication during an incident. The IRT and any other individuals involved in an incident resolution will be directed as to which communication method will be used during the incident.

6. Information Recording

Information recording is very important during an incident, not only for effective containment and eradication efforts, but also for post-incident lessons learned, as well as any legal action that may

ensue against the perpetrators. Each member of the IRT shall be responsible for recording information and chronological references about their actions and findings during an incident.

7. Incident Response Exercises

The IRT should conduct 'table-top' exercises to practice the response process on a periodic basis, but at least annually, so all members of the IRT are familiar with the activities that would occur during an actual incident and their related responsibilities. The exercises may provide the opportunity for enhancing the coordination and communication among team members