This document outlines Synthite Industries Pvt. Ltd.'s core IT policies aimed at ensuring secure, compliant, and effective management of its IT systems and data assets. These policies draw upon industry best practices and regulatory expectations, aligning with our commitment to operational excellence and data integrity.

1. Password Protection Policy

Objective: To establish minimum standards for password complexity, management, and usage to protect systems and data from unauthorized access.

Policy Guidelines:

• All system passwords (e.g., Windows, SAP, VPN, Email) must be a minimum of 8 characters and include at least one uppercase letter, one lowercase letter, one number, and one special character.

• Default and vendor-supplied passwords must be changed immediately upon system deployment or user onboarding.

• Passwords must never be shared, written down, or stored in unencrypted files or documents.

• Passwords must be changed at regular intervals:

  – User accounts: Every 60 days
  – Privileged/admin accounts: Every 30 days

• Password history must prevent reuse of the last 5 passwords.

• Password entry fields must be masked, and systems should lock out users after 5 failed login attempts for a defined cool-off period.

• Systems must enforce password expiry and complexity rules centrally.

• Two-Factor Authentication (2FA) must be enforced for VPN, remote access, and administrative logins.

• Passwords suspected to be compromised must be changed immediately and the IT Security team notified.

Prepared by	Approved by
DM-IT	SVP- Information Systems

2. Record Retention Policy

Objective: To ensure systematic retention and disposal of records in compliance with business needs, legal obligations, and audit requirements.

Retention Categories:

- SAP transactional and financial data – Retained for 10 years
- Invoice and audit logs – 8 years
- Email communications – 7 years
- IT logs (e.g., user activity, firewall, access logs) – 3 years
- Legal records and contracts – As per statutory compliance

Data Classification and Retention Controls:

- All data must be tagged with appropriate classification: Public, Internal, Confidential, or Restricted.

- Records must be retained in secure digital or physical formats approved by the IT and Compliance teams.

- Periodic reviews of stored records must be conducted to ensure continued compliance and relevance.

- Data subject to retention periods must not be deleted or overwritten unless formally approved.

Secure Disposal:

- Expired records must be securely deleted through certified erasure tools or physical destruction (for printed records).

- Disposal of media must be documented and authorized by the IT Head or Compliance Officer.

3. Incident Response Policy

Objective: To define structured response procedures for identifying, reporting, managing, and recovering from information security incidents.

Scope: Applies to all information assets, systems, employees, vendors, and locations of Synthite.

Incident Types: Unauthorized access, data breach, malware, phishing, denial of service, system compromise, physical theft of IT assets.

Incident Response Lifecycle:

1. Detection – Monitoring tools or users identify a potential incident.

2. Reporting – All incidents must be reported to the IT Helpdesk or Security Officer within 30 minutes of discovery.

3. Containment – Immediate steps are taken to limit the impact (e.g., disabling accounts, isolating systems).

4. Investigation – The Security Team performs a root cause analysis and logs forensic evidence.

5. Communication – If needed, notify internal stakeholders and regulatory bodies based on the nature of the breach.

6. Remediation – Systems are restored and vulnerabilities patched.

7. Post-Incident Review – Within 7 business days, a report with corrective and preventive actions must be submitted to the CIO.

Responsibilities:

- IT Security Team: Lead investigations and coordinate resolution.
- All Employees: Promptly report suspicious activities or breaches.
- Department Heads: Cooperate in providing access and information during investigation.

Communication-

Periodic communications are made available to external and Internal stakeholders through website, Internal newsletters, emails and updates whenever there is a change.

-END-

Prepared by	Approved by
DM-IT	SVP- Information Systems