POLICY NO.: BEIL / IT / 02/ 2025

SUBJECT: INFORMATION SECURITY POLICY

EFFECTIVE: 24th September 2025

---

1. Management Commitment to Information Security

Under the responsibility of the IT Team is the mandate for setting the strategic direction in Information Security. This strategic direction is covered in this policy and is owned and published by IT Team. This policy is reviewed and approved by the Management to ensure alignment with BEIL's strategic objectives.

Applicability

This policy applies to all BEIL employees, contractors, third parties, and business partners who access BEIL's information or IT resources, regardless of location or device. Compliance is mandatory, and violations may result in disciplinary or legal action.

---

2. BEIL's Information Security Objectives

The main objective of Information Security Policy is to establish and communicate management's commitment to information security, ensuring alignment with BEIL's business needs as well as applicable laws and regulations." BEIL adheres to the following security objectives:

1. **Confidentiality**: To ensure the protection of personal, sensitive, and business-critical data in accordance with applicable data protection laws and internal procedures, safeguarding all information assets from unauthorized access or disclosure.
2. **Integrity**: To ensure business and external stakeholders can trust BEIL data
3. **Availability**: To ensure that information and vital IT services are available when required
4. **Reliability**: To ensure that information security threats and cybersecurity risks are continuously monitored and effectively responded to, thereby preventing any disruption to BEIL's business operations.
5. **Compliance**: To ensure compliance with legal and regulatory requirements

---

3. Responsibilities

- IT team is responsible for the development and implementation of the Information Security Management System based on the direction provided by management.
- IT team has been entrusted to further improve the Information Security Management System framework
- All BEIL group employees, contractors and third parties are required to adhere to the Information Security Policy and derived documents. Non-compliance is subject to disciplinary action according to local regulations.
- Implement strict access controls, regular security audits and up-to-date software to prevent cybersecurity risks.

- Regular reviews and audits are performed to identify gaps, and proposed actions are considered to continuously improve BEIL's IT Security posture

4.Data Protection and Data Security

BEIL ensures that all personal, sensitive, and business-critical data is protected from unauthorized access, loss, or misuse.

- Information must be accessed only by authorized personnel, based on business need.
- Data retention must follow legal, regulatory, and business requirements; obsolete data must be securely disposed of.
- Regular backups are maintained to ensure recovery in case of data loss.
- Employees are responsible for handling data carefully and preventing unauthorized sharing or storage on unapproved devices or platforms.

5.Cybersecurity

BEIL is committed to protecting its IT systems and networks against cyber threats.

- All devices must run updated operating systems, security patches, and antivirus software.
- Network access is protected through firewalls, intrusion prevention systems, and strict access controls.
- Unauthorized software or hardware is strictly prohibited.
- Employees must report any suspicious emails, activities, or potential security incidents immediately to the IT Team.

6.Monitoring and Reporting Incidents

BEIL continuously monitors its IT environment to detect and respond to security risks and incidents.

- The IT Team is responsible for monitoring systems, networks, and applications for potential threats or unusual activity.

All employees must promptly report any suspected or actual security incidents (e.g., data loss, malware infection, unauthorized access) to the IT Team.

Date: 23-09-2025	B. D. Dalwadi	A. A. Panjwani
Place: Ankleshwar	C.E.O.	Director