

# Information Security Policy

At Balark, we recognise that **information is a vital business asset**, essential for operational efficiency, compliance, customer trust, and competitive advantage. Information security is a strategic priority in today's digital environment, where threats from cyberattacks, data breaches, and espionage are ever-increasing.

To address these challenges, the company has established a **comprehensive Information Security Policy (ISP)** that reflects our commitment to safeguarding the confidentiality, integrity, and availability of all business information. This policy applies to all forms of data—digital, printed, verbal, or otherwise—and to all employees, contractors, and third-party partners who handle company information.

## Objectives of the Policy

- **Prevent loss, theft, and unauthorised access** to business information.
- **Protect information systems** from internal and external threats such as viruses, malware, ransomware, hacking, and industrial espionage.
- **Ensure compliance** with all applicable legal, regulatory, and contractual obligations.
- **Promote a security-aware culture** within the organisation.

## Employee Responsibilities

- All employees must treat information security as part of their **daily responsibilities**.
- The **employment contract includes a confidentiality obligation**, covering all company-related data.
- Information stored on **electronic systems and physical documents** must be handled with care, ensuring it is not disclosed or modified without authorisation.
- **Security incidents or suspicious activity must be reported** immediately to the designated authority.

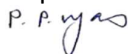
## Management Commitment

Balark is committed to:

- Providing **clear processes and controls** for information protection.
- Offering **ongoing training and awareness** programs for all employees.
- Ensuring **regular audits and assessments** to identify vulnerabilities and improve controls.
- Offering **guidance and support** to ensure effective policy implementation.

By adhering to this policy, we aim to protect our operations, reputation, stakeholder trust, and long-term success in an increasingly connected and regulated world.

1<sup>st</sup> April 2025



Paresh Vyas  
Director