Information Security and Data Privacy Policy.

Introduction

Emmbi Industries recognizes that information is a critical asset underpinning our procurement, manufacturing operations, research & development, enhancing client trust, and ensuring regulatory compliance. This policy establishes Emmbi's commitment to protecting all information assets; digital & physical, against internal and external threats, ensure business continuity, and uphold responsible information management practices throughout the information lifecycle.

The policy is aligned with ISO 27001:2022 (Information Security, Cybersecurity & Privacy Protection) along with global privacy frameworks such as the GDPR.

Scope

This policy applies to:

- All employees, including permanent, contractual, and temporary staff across Emmbi's manufacturing units, R&D centers, and corporate offices.
- New hires, who must undergo mandatory induction and compliance training.
- Supervisors and managers, responsible for ensuring that their teams receive adequate training aligned with regulatory requirements and organizational goals.
- Third-party contractors and suppliers, who must complete safety and compliance training before engaging in operations within Emmbi's facilities.

Information Security Objectives

The core objectives of the Information Security policy are to:

1. Protect the confidentiality, integrity, and availability (CIA) of all information assets.
2. Ensure lawful collection, processing, storage, and disposal of personal data.
3. Embed responsible information management practices into daily operations.
4. Prevent unauthorised access, loss, misuse, or alteration of information.
5. Strengthen client and stakeholder trust through transparency and accountability.
6. Maintain business continuity through resilient information systems.

Data Privacy

In addition to the core objectives, Emmbi integrates the following principles to ensure data is handled ethically and sustainably:

Data Minimization and Retention

- Principle: Collect and retain only the minimum amount of information necessary for legitimate business purposes or legal requirements.
- Control: Implement and enforce a Data Classification and Retention Schedule that defines retention periods for all project, client, and personnel data. Information past its mandatory retention period must be securely disposed of.

Ethical Use and Transparency

- Principle: Ensure information is used only for the purpose for which it was collected and that its processing is transparent to data owners and subjects.
- Control: Prohibit the use of project data, client specifications, or intellectual property for any unauthorized purpose, particularly those that may conflict with Emmbi's sustainability or ethical policies.

Data Quality and Accuracy

- Principle: Maintain the accuracy and completeness of critical data to support reliable decision-making in R&D and manufacturing.
- Control: Implement version control and data validation processes for all engineering documents files, material specifications, quality control records) to prevent the use of erroneous or outdated information.

Sustainable Data Infrastructure

- Principle: Consider the environmental impact of information technology infrastructure and data processing.
- Control: Prioritize energy-efficient hardware, utilize cloud services with demonstrable environmental sustainability credentials, and optimize data storage to reduce energy consumption associated with large-scale project data archives.

Data Lifecycle Management

Emmbi manages information through its entire lifecycle to ensure security and privacy:

- Collection: Obtain data lawfully and transparently, informing individuals of purpose and rights.
- Processing: Use only for authorised purposes, applying need-to-know access.
- Storage: Store securely using encryption and approved repositories.
- Sharing: Share data only under contractual confidentiality or legal obligation.
- Retention: Retain data per defined schedules; regularly review necessity
- Deletion: Destroy or anonymise data securely once retention expires
- Archival: Archive essential records in compliance with legal requirements.

Policy Implementation and Controls

Risk Assessment and Treatment

A formal, structured Information Security Risk Assessment process shall be conducted at planned intervals and when significant changes occur. Risks shall be treated based on the level of tolerance set by Emmbi's management, with appropriate controls.

Supplier and Third-Party Relationships

Procurement contracts involving access to Emmbi's information assets (including outsourced IT services, cloud providers, and joint venture partners) must include mandatory information security and data privacy clauses aligned with this policy, ensuring security is extended across the supply chain.

Incident Management

Emmbi shall maintain a formal Information Security Incident Management Process to ensure security events and breaches are reported, classified, investigated, and resolved in a timely manner, including post-incident analysis to prevent recurrence. All security or privacy incidents must be reported immediately to the Information Security Officer at the earliest possible. Emmbi will investigate all data breach issues within 2 days of becoming aware of the issue and take appropriate steps to mitigate and/or reverse the damage, and document all incidents promptly. Where required by law, affected individuals and authorities will be notified within the stipulated timeframe.

Roles and Responsibilities

- Top Management: Approve policy, allocate resources, review ISMS performance.
- Information Security Officer (ISO): Manage implementation, risk assessments, and awareness programmes.
- Data Protection Officer (DPO): Ensure compliance with Data Protection laws and with ISO 27001, handle data subject requests, and oversee DPIAs.
- IT Department: Implement technical controls and monitoring systems.
- All Employees: Follow data-handling procedures and report any incidents or suspected breaches immediately.
- Vendors & Partners: Comply with contractual data protection obligations and support audits when required.

Awareness, Training & Behaviour

- 100% of employees shall complete annual Information Security & Data Privacy Training and all new employees shall complete the training within 30 days of joining.

- Tailored sessions will be held for teams handling sensitive or personal data (HR, Procurement, Projects, Finance).
- Regular internal communications (e.g. awareness emails, phishing simulations) will reinforce responsible digital behaviour.

Review and Improvement

This policy as well as the ISMS shall be formally reviewed by Top Management at least annually, or following major business/technological changes, to ensure continued suitability, adequacy, and effectiveness.

Managing Director
EMMBI INDUSTRIES LTD.