1. Purpose

The purpose of this Data Protection and Information Security Policy is to ensure that all data and information assets within Raviraj Foils Ltd. are protected against unauthorized access, disclosure, alteration, and destruction. This policy aligns with the Global Reporting Initiative (GRI) standards and applicable data protection laws, aiming to maintain the confidentiality, integrity, and availability of information.

2. Scope

This policy applies to all employees, directors, officers, contractors, suppliers, and any other stakeholders who have access to the company's data and information systems. It covers all types of data, including personal data, confidential business information, intellectual property, and any other information critical to the company's operations.

3. Core Principles

Confidentiality: Ensuring that sensitive information is accessible only to those authorized to have access.

Integrity: Protecting information from being altered, whether accidentally or maliciously, and ensuring its accuracy and completeness.

Availability: Ensuring that information and systems are accessible to authorized users when needed.

4. Quantified Objectives

Objective 1: Achieve 100% completion of data protection and information security training for all employees, directors, and officers annually.

PREPARED BY:	CHECKED BY:	APPROVED BY:
Safety Officer	Sr. EHS Officer	HR - Head
DATE: 20/08/2024	DATE: 20/8/2024	DATE: 20/08/2024

MASTER COPY

Objective 2: Ensure zero incidents of data breaches annually by implementing robust security controls and regular monitoring.

Objective 3: Conduct at least two internal audits per year focused on data protection and information security compliance.

Objective 4: Ensure 100% of third-party suppliers and contractors sign data protection agreements that align with this policy.

5. Data Protection Requirements

Data Collection and Processing: All data must be collected and processed lawfully, fairly, and transparently. Personal data should only be collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes.

Data Minimization: Only the data necessary for the specific purpose should be collected and processed. Efforts should be made to limit the collection and retention of unnecessary data.

Data Accuracy: All personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be corrected or deleted without delay.

Data Retention: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

Data Security: Appropriate technical and organizational measures must be implemented to protect data against unauthorized access, alteration, disclosure, or destruction.

6. Information Security Requirements

Access Control: Access to information systems and data must be controlled and limited to authorized users based on their roles and responsibilities. Multi-factor authentication and strong password policies must be enforced.

Data Encryption: Sensitive data, both in transit and at rest, must be encrypted using strong encryption standards to protect against unauthorized access.

Network Security: Firewalls, intrusion detection systems, and other security controls must be implemented to protect the company's network and information systems from external threats.

Incident Response: A documented incident response plan must be in place to detect, respond to, and recover from data breaches or security incidents promptly.

Physical Security: Physical access to data centers, server rooms, and other sensitive areas must be controlled and monitored to prevent unauthorized access.

7. Responsibilities

Board of Directors: The Board is responsible for ensuring that the company's data protection and information security program is effectively implemented and that resources are allocated to maintain a secure environment.

Data Protection Officer (DPO): The DPO is responsible for overseeing data protection compliance, conducting data protection impact assessments, and ensuring that the company adheres to data protection laws and regulations.

IT Security Officer: The IT Security Officer is responsible for implementing and maintaining the company's information security program, conducting security audits, and responding to security incidents.

Employees: All employees are responsible for understanding and complying with this policy, completing required training, and reporting any suspected data breaches or security incidents.

8. Training and Awareness

Mandatory Training: All employees, directors, and officers must complete mandatory data protection and information security training annually. This training will cover relevant laws, security best practices, and the importance of protecting company data.

Ongoing Communication: The company will conduct regular awareness campaigns to ensure that all stakeholders are aware of their obligations under this policy and are encouraged to report any concerns related to data protection or information security.

9. Data Protection and Security Monitoring

Regular Audits: The company will conduct regular audits to assess compliance with data protection laws and the effectiveness of information security controls. These audits will help identify vulnerabilities and areas for improvement.

Continuous Monitoring: Information systems and networks must be continuously monitored for security threats, vulnerabilities, and potential data breaches. Automated tools should be used to detect and respond to security incidents in real-time.

Third-Party Assessments: Third-party suppliers, contractors, and business partners who have access to company data must undergo regular assessments to ensure compliance with data protection and information security standards.

10. Reporting and Incident Management

Reporting Mechanisms: Employees and stakeholders are encouraged to report any suspected data breaches or security incidents. Reports can be made to the Data Protection Officer or IT Security Officer.

Incident Response Plan: The company must have a documented incident response plan that outlines the steps to be taken in the event of a data breach or security incident. This plan should include procedures for containment, investigation, notification, and recovery.

Protection from Retaliation: The company strictly prohibits retaliation against anyone who reports a data breach or security incident in good faith. All reports will be treated confidentially and investigated thoroughly.

11. Response to Data Breaches

Investigation: All reported data breaches will be promptly and thoroughly investigated by the Data Protection Officer or an appointed investigation team.

Notification: In the event of a data breach, affected individuals and relevant authorities must be notified as required by law. The company will take immediate steps to mitigate the impact of the breach and prevent future occurrences.

Corrective Measures: The company will implement corrective measures to address any identified weaknesses in its data protection and information security program and prevent future breaches.

12. Review and Revision

Regular Review: This Data Protection and Information Security Policy will be reviewed annually or as needed to ensure it remains effective and up-to-date with legal requirements and best practices.

Revision History: Any changes or updates to this policy will be documented in the revision history, and all stakeholders will be informed of the changes.

Sr. No.	Issue Date	Reason for revision	Revision No.	Obsolete Doc No.
1	20/08/2024	First Issue	00	-

PREPARED BY:	CHECKED BY:	APPROVED BY:
Safety Officer	Sr. EHS Officer	HR - Head
DATE: 20/08/2024	DATE: 20/8/2024	DATE: 20/08/2024

MASTER COPY