RAJA

Information Security Policy

Introduction: Rajapack Ltd, a distributor of supplies and equipment, processes substantial amounts of data including customer, supplier, employee, and stakeholder information. This policy ensures consistent information security across the organization, specifying the handling, access, and protection of information.

Policy Objective: To protect the information assets that Rajapack handles, stores, exchanges, processes, and has access to, ensuring the ongoing maintenance of their confidentiality, integrity, and availability. This includes implementing controls that are proportionate to the value of the information assets and the threats they face. Rajapack aims to comply with all relevant legal, customer, and third-party requirements and to continually improve its Information Security Management System (ISMS) to withstand threats to information security.

Scope: This policy and its sub-policies apply to all people, processes, services, technology, and assets involved in information security. It also applies to all employees and subcontractors who access or process Rajapack's information assets. The policy is reviewed annually or as needed due to regulatory or business changes.

Information Security Management System (ISMS):

- **Implementation and Certification:** Rajapack follows the PDCA model (Plan, Do, Check, Act) and complies with ISO 27001:2022 standards. The ISMS is independently certified to ensure compliance.
- **Risk Management:** Coordinated risk management processes are in place to identify and mitigate risks to information resources.
- **Legal and Regulatory Compliance:** Regular privacy risk assessments, control frameworks, intellectual property protection, and data retention policies are implemented to ensure compliance with GDPR, the Computer Misuse Act, and other regulations.

Core Policies:

- **Data Protection:** Ensure data is securely maintained throughout its lifecycle and disposed of according to specified retention periods.
- **Incident Management:** All information security incidents must be reported to the IT Director and violations of this policy may be subject to disciplinary action.
- **Training and Awareness:** Provide appropriate information, instruction, and training to ensure all employees are aware of their responsibilities and legal duties.
- **Business Continuity and Disaster Recovery:** Maintain and regularly test plans to ensure business continuity and effective disaster recovery.

Responsibilities:

- **Executive Management:** Demonstrate leadership and provide necessary resources to support the ISMS.
- **IT and Security Teams:** Implement and maintain technical controls, monitor security systems, and respond to incidents.
- **Employees:** Follow security policies and report incidents, participate in training, and ensure secure handling of information.

Continuous Improvement: Rajapack is committed to continually improving its ISMS. Regular monitoring of security threats, testing of control measures, and reviewing the appropriateness and effectiveness of the policy are integral to achieving this goal. This commitment must be supported by all employees and contractors as part of their daily work.

This Policy is publicly available to interested external parties on request.

Signed..   Date: 24th May 2024

Tom Rodda – Managing Director