THE REINALT-THOMAS
CORPORATION

Information Classification and Handling Policy

4/15/2024

Amendments to this Policy will be posted on the Knowledge Center
and will be effective when posted.

Confidential Information

Revision	Description of Change	Date	Initials
1.0	Initial version		ILM Team

Contents

1. Overview and Purpose

Consistent with The Reinalt-Thomas Corporation and its affiliates' (the "Company") requirements and sound business practices, it is the policy of the Company to retain and manage its business, financial, employee, and other records and Information in accordance with guidelines, best practices, and procedures put forth by the Company's Information Lifecycle Management (ILM) program.

The Company collects and holds important information about Our Customers, Our People, and its business functions and methodologies. This information needs to be protected, while ensuring that it can also be used appropriately and effectively.

One of the foundations for successful information protection is information classification. Different types of information are identified and labeled according to their sensitivity and the risks associated with disclosure of that information. The purpose of this policy is to define standard levels of classification that determine the security protections that must be used for the information. These protections can then be built into the tools and processes Our People use to access, manage, and use Company information.

2. Scope

This Policy applies to Company employees, contractors, affiliates and subsidiaries and their management of records, information, and data generated, maintained, or received in the ordinary course of business regardless of medium, format, characteristics, or storage location.

3. Roles and Responsibilities

Business Information Owners. Business information owners understand the sensitivity of their information and the risks associated with its disclosure. Business information owners determine and apply the appropriate levels of classification for the information they create, receive, manage, and use.

Information Security. The Information Security team translates the Business Information Owners' classification requirements into appropriate security capabilities and access controls.

Enterprise Architecture. The Enterprise Architecture team works with the Information Security team to design technology solutions that can meet the Business Information Owners' classification requirements.

Information Lifecycle Management (ILM). The ILM Program Head collaborates with Business Information Owners, Information Security, Enterprise Architecture, and other stakeholders as needed to facilitate consistent classification levels and practices.

Employees. Employees protect the security and confidentiality of information in their position, custody, or control. Employees understand their information and its need to be classified at the appropriate classification level. Questions about the interpretation or implementation of this Policy should be directed to the ILM Program Head.

4. Classification Levels

The classification levels described below are the results of collaboration between the Business Information Owners, Information Security, Enterprise Architecture, and ILM.

Classification Level	Definition	Examples
Restricted	Information of the highest confidentiality and sensitivity to the organization. Improper access or disclosure could result in financial, regulatory, and reputational harm. Access is restricted to only those employees who require it to fulfill specific job-related tasks. Includes sensitive customer and employee personal information.	**Information Security:** Cryptographical records, encryption keys, passwords, etc. PCI **Human Resources:** PHI, SPI, SSN, termination reason, salary
Confidential	Information deemed private in nature, such as personal information of customers and employees and company business and financial information.	Customer/ employee PI (e.g., name, DOB, address, email, gender) Business strategy, Company financial and legal information, intellectual property
Internal	Information that is internal to Discount Tire that includes limited or company-wide distribution with appropriate access permissions.	Internal Company documents (e.g., PnPs, project plans, job descriptions, org charts), internal Company announcements, email, and other info not explicitly approved to be made public.
Public	Information that is publicly available or that Discount Tire makes readily available to the public.	Press releases, authorized marketing materials, customer service phone numbers, etc.

5. Managing Highly Restricted Data

These classification levels ensure consistency in the access, use, and management of Company information. However, business information owners may determine that they need additional levels of security and/or access controls for particularly sensitive information. In such cases, additional sub-categories of permissions may be defined and implemented within a classification level.

6. Monitoring and Review

The Company expects full compliance with this policy. The ILM program executes periodic reviews and monitoring activities to support and confirm compliance with this policy.

The Company reviews this Policy to determine whether legal or business requirements warrant its amendment annually. The ILM Program Head is authorized to approve amendments to this Policy.

7. Related Policies

The following Policies and Best Practices are related to the elements contained in this Policy and may be of value to employees charged with its execution.

a. Information Security Policies and Procedures
b. Acceptable Use Policy
c. Data Obfuscation Matrix