Trackon Canada Private Limited Data Categorization and Classification Policy

Version Number: 1.1

Last Updated: July 2022

Next Update: January 2023

Approved By:

Senior Officer Approval for Program:

Table of Contents

1 Policy Statement

1.1 Our Commitment

Reading this policy and our all-staff procedure is currently required for all new hires. An attestation confirming that the policy and procedure are read and understood is kept as a training record. There are also separate training materials for staff, which include quizzes designed to test the effectiveness of training.

1.2 Information Categorization and Classification *(ISO 27001 Control: 8.2)*

1) Information assets shall be broadly classified as follows:

a) **Confidential:** Confidential information is the most sensitive information and disclosure or unauthorized access to the same is likely to impact the company's business adversely. Disclosure requires the Asset Owner's approval. Examples: Customer contracts, product pricing, process documents, strategic plans, new product development plans, unpublished financial statements, etc.

b) **Restricted:** Restricted information is limited for use by specific individuals or groups. Exposure of such information to persons outside the group may result in loss of customer confidence, major embarrassment, infringe on the privacy of individuals, security issues concerning availability and integrity of data, or operational inconvenience. For example: Personally, Identifiable Information, business plans, minimum baseline security configurations (MBSS), firewall and router configurations, customer-related information, internal audit findings, etc.

c) **Internal** (all departments and personnel): All information created within Trackon Canada Pvt Ltd is by default Internal and is for internal use only. Such information is restricted to the internal employees/employee groups and approved non-employees. This information needs to be protected from external access. Exposure to such information may result in embarrassment to the organization and potentially be misused by competitors. This form of information must be used within the Company and not shared externally or with third parties unless approved by the Competent Authority. For example, staff memos, company newsletters, staff awareness program documentation or bulletins, service contracts, etc.; and

d) **Public:** Sharing of such information has negligible or does not have any impact on the confidentiality, integrity, or availability of the information. This form of information is provided by the Organization to the public. For example news coverage, information published on internet portals, periodicals, public bulletins, published company financial statements, published press releases, etc.

2) Information labeling and handling steps shall be developed and implemented in line with the information classification levels.

3) Appropriate access controls shall be implemented based on the classification of assets to ensure that information security requirement are adhered to.

1.2.1 Compliance with security policies and procedures *(ISO 27001 Control: 18.2.2)*

1) Compliance with Trackon Canada Pvt Ltd's ISMS-related policies and procedures are required to ensure that ISMS can achieve its intended purpose and objectives. Functional Head shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with the information security requirements;

2) Any detected non-compliances with the related policies and procedures shall be investigated and preventive action shall be taken and reviewed; and

3) Such non-compliances as well as their preventive actions shall be further reported at the time of independent reviews.

1.2.2 Technical compliance review *(ISO 27001 Control: 18.2.3)*

4) Technical compliance reviews shall be conducted at least annually to ensure that controls have been appropriately implemented; and

5) In case of any non-compliance, a root-cause analysis shall be performed to ascertain the reasons and possible preventive actions for the future.