Trackon Canada Private Limited

Segregation of Duties Policy and Procedures

Version Number: 1.1

Last Updated: July 2022

Next Update: January 2023

Approved By: Jaspreet Singh, Director

Senior Officer Approval for Program: Jaspreet Singh, Director

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.

2 Segregation of Duties Policy and Procedures

2.1 Purpose

The purpose of this policy is to define a suitable Information Security Organization Structure and define roles and responsibilities for coordination of Information Security activities within the organization.

2.2 Scope

This policy applies to all Trackon Canada Pvt Ltd's employees, sub-contractors, and partners to provide clear direction and visible management support for Information Security activities.

2.3 Segregation of duties Requirements *(ISO 27001 Control)*

- As per ISO 27001, ***'The duties and areas of responsibilities of personnel shall be segregated and records shall be maintained to reduce the opportunities of unauthorized or unintentional modification or misuse of the information assets.'***
- In cases segregation of duties is not possible; approval of the Functional Head shall be obtained before allocating responsibilities to the personnel. Also, appropriate compensatory controls such as monitoring of activities, audit trails, management supervision, and independent reviews shall be implemented; and
- All processes shall adopt the principle of segregation of duties to the maximum extent possible.

2.4 Internal Organization *(ISO 27001 Control: 6.1)*

Management of Trackon Canada Pvt Ltd shall actively support information security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. Additionally, aspects related to segregation of duties, contacts with authorities & special interest groups, and information security requirements in project management shall be addressed.

2.4.1 Information Security Roles and Responsibilities *(ISO 27001 Control: 6.1.1)*

All Information Security responsibilities regarding the protection of Trackon Canada Pvt Ltd assets associated with information and information processing facilities shall be clearly defined through job descriptions, work allocation, and delegation of tasks.

The defined Information Security responsibilities shall be formally allocated and accepted across the organization. Such responsibilities shall include (but are not limited to):

- The overall responsibility for the development and implementation of information security and related processes.
- Identifying the information assets and the security processes associated with each asset.
- Defining and documenting the asset ownership, the level of responsibility, and authorization levels.
- Classification and labeling of information assets by the Asset Management Procedure
- Identification and implementation of controls that shall be termed necessary to adequately protect assets.
- Reviewing and approving user access privileges by the Access Control Procedure and
- Other information security tasks and responsibilities assigned by ISMC from time to time.

2.4.2 Contact with authorities *(ISO 27001 Control: 6.1.3)*

Appropriate contacts shall be maintained with the relevant authorities such as law enforcement authorities, fire department, emergency services, service providers, legal counsel, etc. to ensure:

- Continued compliance with applicable laws and regulations and
- Anticipate and prepare for upcoming changes to such laws and regulations.

2.4.3 Contact with special interest groups *(ISO 27001 Control: 6.1.4)*

Special interest groups, specialist security forums, and professional associations shall be identified, and IT Security Head shall maintain appropriate contacts with such groups, forums, and associations.

2.4.4 Information security in project management *(ISO 27001 Control: 6.1.5)*

Information security shall be integrated into Trackon Canada Pvt Ltd's project management methods to ensure that information security risks are identified and addressed as part of a project. The project management methods in use shall require that:

- Information security objectives are included in project objectives.
- An information security risk assessment is conducted at an early stage of the project to identify necessary controls; and
- Information security is part of all phases of the applied project methodology.

Information security implications shall be addressed and reviewed regularly in all projects; and

All the projects within Trackon Canada Pvt Ltd's scope shall undergo periodic security assessments by the MS Product Development Process.