Trackon Canada Private Limited
Fraud Prevention
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 3
1.1 Our Commitment 3
2 Fraud Prevention 3
2.1 Fraud Risk Map for Prevention of Fraud within Trackon Canada Pvt Ltd 3
2.2 Tools to identify, control and manage Fraud risk 4

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 Fraud Prevention

2.1 Fraud Risk Map for Prevention of Fraud within Trackon Canada Pvt Ltd

'A Fraud risk map is defined as a tool used for the identification, control, and management of risks regarding Fraud. It is also an iterative process that refines senior management's understanding of the risks the organization is exposed to in terms of Fraud risks and measures the effect of the mitigation strategies used to control risks.'

Fraud is any intentional act or omission designed to deceive others, resulting in a loss for the Company and/or its stakeholders or the perpetrator achieving a gain.

Senior Management Awareness

- Senior executive management should adopt a zero-tolerance culture toward Fraud. Any Fraud involving criminal elements should be reported to the regulatory bodies as soon as practicable.
- The Executive Committee and the Risk Management and Compliance Committee should receive updates as appropriate on Fraud types, trends, and effective Fraud prevention measures as well as costs against losses to ensure appropriate resources are applied to counter-Fraud operations. These should be included in the standard agenda of the meetings. The committees should have an up-to-date understanding of the current Fraud incidents and provide timely resolution on Fraud related matters. The Risk Management Department should have the responsibility to provide information and reports to assist the senior management in deciding on Fraud mitigation and investigation strategies.

Segregation of duties

- Segregation of duties and dual control procedures are an important safeguard against various kinds of Fraud and must be applied to high-risk processes (such as duties involving cash handling). Job rotation should be exercised where possible and managers of high-risk processes must exercise regular spot checks and random sampling to identify irregularities.
- When dual control has been established, it must never be relinquished to the alternate party in the control arrangement. An appropriate backup arrangement should be established for critical functions.

2.2 Tools to identify, control and manage Fraud risk

Staff Pre-Employment Screening

Criminal infiltration and employee collusion can lead to serious Fraud at both junior and senior levels of staff and management. The Trackon Canada Pvt Ltd should have an appropriate pre-employment screening in place for all employees (permanent, temporary, outsourced, consultants, etc.) to detect and prevent the employment of individuals or appointment of agents who have previously been involved in crime or conduct inconsistent with the code of conduct.

The pre-employment screening process should cover an applicant's background to verify the accuracy of his claims and to look into any possible criminal history. The thoroughness of screening depends on the position of the potential staff.

Common pre-employment screenings include:

1. Personal details (e.g., identity documents) verification
2. Criminal history screening
3. Credit history
4. Employment verification
5. Education document verification

Vendor and Contractor Vetting

Vendors or contractors often have significant access to Trackon Canada Pvt Ltd's systems and/or information and should be vetted to the same level as permanent staff. Trackon Canada Pvt Ltd should have appropriate vetting procedures to detect any previous misconduct or criminal activity.

Trackon Canada Pvt Ltd should not rely on experience with or prior knowledge of the vendor or contractor as a proxy for an objective, in-depth assessment of the vendor or contractor's ability to perform the activity in compliance with all applicable laws and regulations. Due diligence should be exercised to investigate the background.

The degree of due diligence should be commensurate with the level of risk and complexity of the relationship. As an example, when critical customer information is involved, onsite visits may be required to fully understand the vendor's or contractor's operation and capacity. The due diligence process should evaluate all available information about the vendor or contractor, inclusive of capability, financial strength, credit reference, past performance, corporate and individual reputation, and sanctions/ name screening against World Check or Actimize. Trackon Canada Pvt Ltd should ensure the vendor or contractor has appropriate policies and procedures in place to identify dishonest employees and suppliers and to mitigate the Fraud risk. In addition, the vendor or contractor should provide the "Non-disclosure Statement" to Trackon Canada Pvt Ltd when signing the service agreement to ensure they will not disclose any information about Trackon Canada Pvt Ltd or its customers to other parties.

Trackon Canada Pvt Ltd should select among a minimum of three contractors or vendors as far as practicable in particular when the service is long-term in nature or if the service fee is significant or if the contractor/ vendor has access to extensive customer information.

Computer System Access

fraud can be perpetrated by misusing business information in Trackon Canada Pvt Ltd. System and information access should be restricted to authorized personnel, justified on business requirements, and traceable to user identities. Staff should change their passwords regularly (i.e., monthly, or quarterly depending on the significance and sensitivity of the computer system).

IT Operations Department and different business departments must periodically review system access to ensure the staff member is still employed, the access is still necessary, and the level of access is appropriate to the current role.

There should be system access logs in place for IT Operations Department to detect suspicious activities such as frequent invalid login attempts, security violations, etc. In particular, activities for privileged accounts, such as those granted unrestricted access as system administrator and developer, should be closely monitored.

IT Operations Department should also ensure proper security controls and procedures are implemented with each IT system and infrastructure.

fraud awareness training

All employees, including temporary/ contract staff (with employment relationship for more than 6 months) should attend induction (within 90 days of hire) and regular training for Fraud awareness and reporting of suspicious activity. Staff Fraud training should be available for all business lines.

Training and Development Department should deliver annual Fraud awareness training through e-channel or classroom training or workshop which should cover the following areas:

1. Overview of the anti-Fraud policy
2. Definition of Fraud
3. Zero tolerance approach
4. Business department and division responsibilities
5. Employee responsibility for escalation and reporting of suspicious activity
6. Channel for reporting suspicious activity and whistleblowing programmed
7. fraud scenarios and red flags
8. fraud trends

Attendance at the Fraud awareness training is mandatory, and attendance is tracked by the Training and Development Department.

Compliance Department and Risk Management Department should share information on Fraud trends, new methods of operation, and successful strategies with other staff through training, bulletin board, or email announcements whenever the Compliance Department receive Fraud related information Risk Management Department observe certain Fraud trends monthly through the operational risk management reporting.