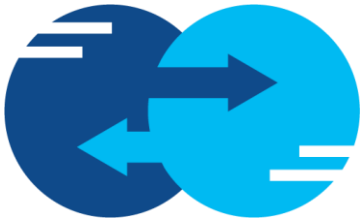

Trackon Canada Private Ltd
Incident Management and Response Policy

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 Purpose

Information Security Incident is a single or a series of unwanted or unexpected Information Security Events that have a significant probability of compromising business operations and threatening information security. It is related to exceptional situations or a situation that warrants the intervention of Senior Management. The purpose of the Information Security Incident Management Policy is to provide directions to develop and implement a robust process for identifying, managing, resolving, and communicating information security incidents.

1.3 Scope

The Information Security Incident Management Policy applies to all employees, sub-contractors, associated third parties, information systems and assets (assets as defined and classified as IT Infrastructure and Hardware, Services, Digital, Tangible and Human Assets in the “Information Assets Inventory”) that are owned by Trackon Canada Pvt Ltd.

2 Incident Management and Response Policy *(ISO 27001 Control: A.16)*

2.1 Management of information security incidents and improvements *(ISO 27001 Control: 16.1)*

2.1.1 Responsibilities and procedures *(ISO 27001 Control: 16.1.1)*

1) Procedures for monitoring, detecting, analyzing, and reporting information security events and incidents shall be defined and implemented.

2) Competent personnel shall be identified to handle information security incidents.

3) In addition to normal contingency plans, the procedures shall also cover the following:

   - Analysis and identification of the root cause of the incident.
   - Containment.
   - Planning and implementation of corrective action to prevent a recurrence, if necessary.
   - Communication with those affected by or involved with recovery from the incident; and
   - Reporting the action to the appropriate authority.

4) Audit trails and similar evidence shall be collected and secured as appropriate for:

   - Internal problem analysis; and
   - Forensic evidence about a potential breach of contract or regulatory requirement or the event of civil or criminal proceedings.

5) Action to recover from security breaches and system failures shall be carefully and formally controlled. The Information Security Incident Management Procedure shall ensure that:

- Only clearly identified and authorized personnel are allowed access to live systems and data.

- All emergency actions taken shall be in line with the approved "Trackon Canada Pvt Ltd _Change and Release Management Procedure" and shall be documented in detail.

- Emergency actions shall be reported to management and reviewed in an orderly manner; and

- The integrity of business systems and controls is confirmed with minimal delay.

6) Responsibilities concerning Information Security Incident Management shall be communicated to the involved parties and Trackon Canada Pvt Ltd shall ensure that those responsible for Information Security Incident Management understand the organization's priorities for handling Information Security incidents.

2.1.2 Reporting information security events *(ISO 27001 Control: 16.1.2)*

1) Appropriate contacts with external parties and special interest groups that handle information security incidents shall be maintained.

2) All employees, sub-contractors, and partners shall immediately report observed or suspected information security events/incidents that might be, or could lead to, unauthorized access, loss, or inaccuracy of the Organization's information thereby resulting in the breach of information security-related policies and procedures; and

3) Types of information security incidents that may include, but are not limited to the following:

- Loss of service, equipment, or facilities.

- System malfunction or overloads.

- Human errors.

- Breach of policies or guidelines.

- Malfunction of software or hardware; and

- Access violations.

2.1.3 Reporting of information security weaknesses *(ISO 27001 Control: 16.1.3)*

1) Trackon Canada Pvt Ltd users shall also report any security weaknesses related to systems and services to the IT Security Head to prevent such weakness from converting into an information security incident.

2) Types of information security weaknesses that may include, but are not limited to the following:

   - Unauthorized disclosure of information.
   - Falsification of information.
   - Malicious code and hacker intrusion.
   - Unavailability of critical information assets; and
   - Installation of equipment not authorized by Trackon Canada Pvt Ltd.

3) Trackon Canada Pvt Ltd shall provide ongoing awareness to the users on identifying an information security weakness and reporting such weaknesses to the appropriate parties.

2.1.4 Assessment of decision on information security events *(ISO 27001 Control: 16.1.4)*

1) Information security incidents shall be assessed and classified based on associated impact and reported to appropriate Management levels based on the Risk Impact Matrix and adequate steps shall be taken to address the incident.

2.1.5 Response to information security incidents *(ISO 27001 Control: 16.1.5)*

1) Appropriate and timely corrective actions shall be implemented based on the classification of an information security incident and by the "Trackon Canada Pvt Ltd _Information Security Incident Management Procedure."

2.1.6 Learning from information security incidents *(ISO 27001 Control: 16.1.6)*

1) A knowledge base shall be established for the information gained from the evaluation of all information security incidents. The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be considered in the ISMS review process. Additionally, information security incidents shall be reviewed periodically to ensure appropriate corrective action has been taken so that repeated incidents don't occur.

2.1.7 Collection of evidence *(ISO 27001 Control: 16.1.7)*

1) As per the legal requirements the evidence shall be collected during incident analysis, maintained, and presented to the relevant authorities. The evidence shall be collected in a manner that does not destroy its evidentiary value. While collecting the evidence, the following shall be considered :

   - Applicability of evidence: the evidence can be used in a court of law; and
   - Weightage of evidence: the quality and completeness of the evidence.