Trackon Canada Private Limited

Communication Policy and Procedure

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 3
1.1 Our Commitment 3
1.2 Purpose 3
1.3 Scope 3
2 Communications Security Policy *(ISO 27001 Control: A.13)* 4
2.1 Network security management *(ISO 27001 Control: 13.1)* 4
2.2 Information transfer *(ISO 27001 Control: 13.2)* 5

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

The purpose of the Communication Security Policy is to establish appropriate controls that need to be implemented to ensure the protection of information in networks and their supporting information processing facilities. The controls are intended to maintain the security of information transferred within the Organization and with any external entity.

1.3 Scope

The Communications Security Policy applies to all employees, sub-contractors, associated third parties, information systems, and assets that are hosted/located in Trackon Canada Pvt Ltd.

2 Communications Security Policy *(ISO 27001 Control: A.13)*

2.1 Network security management *(ISO 27001 Control: 13.1)*

1) Designated personnel shall be identified for managing the Trackon Canada Pvt Ltd network.

2) To ensure the security of the Trackon Canada Pvt Ltd network, devices such as routers, switches, intrusion prevention, and detection systems, firewalls, etc. shall be installed at the network perimeter.

3) Network monitoring tools shall be implemented to automatically provide protocol anomalies, traffic analysis, hardware malfunction signals, etc. These tools/devices shall be appropriately configured to customize the protection level of the network according to the Business requirements.

4) Logs of these tools/devices shall be regularly monitored by the CE Head/ CE Function Manager / Cloud Function Manager (as applicable).

5) Anomalies detected shall be communicated to relevant personnel and corrective actions shall be taken.

6) At the time of implementing any new network component, i.e., routers and switches, etc., the CE Team shall configure it to prevent the disclosure of the configuration of the internal network to external and unauthorized entities.

7) Access to network services shall be monitored periodically and any discrepancies shall be reported. Corrective actions shall be taken based on approval from CE Head / CE Function Manager / Cloud Function Manager (as applicable).

8) Remote access shall be controlled and allowed only after due approval from CE Head / CE Function Manager / Cloud Function Manager (as applicable).

9) Network diagrams shall be created, reviewed, and updated regularly.

10) Trackon Canada Pvt Ltd network shall be segregated into separate logical network domains. These domains shall be identified based on identified risks and different security requirements within each of the domains.

11) Data flow between separate network domains shall be controlled via a secure gateway(s); and

12) For wireless networks, an adequate risk assessment shall be carried out to identify controls to be implemented to maintain the segregation of networks

2.2 Information transfer *(ISO 27001 Control: 13.2)*

1) Appropriate security controls shall be implemented for the exchange of business information with third parties. The security controls shall include technical controls and contracts/agreements signed with third parties.

2) All removable media ports, such as USB, CD-DVD, Bluetooth etch, shall be blocked by default on all user computers and servers

3) Procedures for the detection of and protection against malware that may be transferred through the use of electronic communications shall be implemented.

4) Information and data shall be protected with appropriate controls based on the information's classification (For Example - Confidential, Restricted, Internal, and Public).

5) Automatic forwarding of electronic mail to external addresses shall be restricted.

6) Trackon Canada Pvt Ltd personnel shall take appropriate precautions, not to reveal 'Confidential' information and to avoid being overheard or intercepted when making a phone call by people in their immediate vicinity, wiretapping, or people at the recipient end.

7) Guidance as per the Acceptable Use of Assets Policy shall be followed by all personnel

8) Trackon Canada Pvt Ltd shall conduct a risk assessment to identify potential risks to the Organization's information assets as a result of outsourcing to the third party and appropriate controls shall be implemented to mitigate the risks.

9) Trackon Canada Pvt Ltd shall have agreements or contracts with the third-party vendors which shall address the secure transfer of business information between Trackon Canada Pvt Ltd and the vendors.

10) Incoming and outgoing emails shall be scanned for viruses including scanning of the attachments.

11) Email messages sent to domains other than the domain of the Organization shall contain a Disclaimer prohibiting unauthorized use, dissemination of the information, or copying of the message and notify the sender; and

12) Non-Disclosure Agreements (NDAs) shall be signed with external parties and Trackon Canada Pvt Ltd employees to address the requirements of protecting Trackon Canada Pvt Ltd's information. Content of the NDAs shall be reviewed and updated in case changes are required.

13) Customer shall log the issue in the Tool.

14) Production Engineering (Support) Team shall assess the issue and seek approval from the Trackon Canada Pvt Ltd Delivery/ Account Manager, Customer Representative (Director/ VP/ Accountable data owner) to copy the data (if necessary) from the Cloud Instance hosted datacenter to the Support Instance hosted in Trackon Canada Pvt Ltd.

15) On receiving the approvals, the Support Team shall inform the Cloud Engineering team to copy the data.

16) Cloud Engineering Team shall take approval from the IT Security/ CTO before copying the data.

17) On receiving the approval, Cloud Engineering Team generates the dump of the Production Instance hosted in the data center.

18) Cloud Security scans the dump for any confidential customer data and any such information is sanitized.

19) Once this is done, the Cloud Engineering team copies the dump to the Support Instance hosted in Trackon Canada Pvt Ltd Corporate network for the Support team to troubleshoot and resolve the issue.

20) After resolution, the Support team shall ask the Cloud Engineering Team to copy the data from Support Instance in India to the Test Instance hosted in Datacenter for testing.

21) Once the issue is tested, Cloud Engineering Team shall move the data to the Production Instance hosted in the data center after getting the necessary approvals.

22) The Cloud Security team will scan the Support Instance for any PII/ PHI/ PCI data.

23) The Support Team shall delete any customer data residing on the Support instance. The data should NOT be copied to any other servers or used machines.