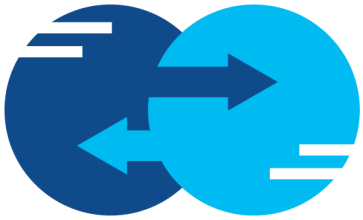

Trackon Canada Private Limited

Data & Financial Security Control Policy

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 different training materials for staff, which include quizzes designed to test the effectiveness of training.

2 Data Access Control Policy

2.1 Business requirements of Access control *(ISO 27001 Control: 9.1)*

The access to Trackon Canada Pvt Ltd's assets associated with information (Operating Systems, Applications, Domain Controllers, Databases, Networks, etc.) shall be according to the principles of 'least privilege' and 'need to know basis. The activities shall be administered to make sure that the appropriate level of access control is applied to these assets to protect them from unauthorized access, modification, disclosure, or destruction. This shall ensure that information stored or processed by these assets remains accurate, and confidential and is available when required.

The following shall be considered as part of the Access Control Policy:

1) Identification of security requirements for critical business applications.

2) Access shall be granted based on 'least privilege' and 'need to know basis.

3) Access rights shall be granted based on information classification.

4) Legal, regulatory, and contractual aspects shall be kept in mind before granting access.

5) Access commensurate with the roles and responsibilities of the user shall be granted.

6) A formal user access management procedure for granting, modifying, and revoking user access shall be followed. Access shall be based on approval from authorized personnel.

7) Access rights shall be periodically reviewed by authorized personnel (such as Functional Head/ CE Head/ Cloud Function Manager, as applicable).

8) Privileged access shall be provided to authorized personnel only based on approval from the Functional Head/ CE Head/ Cloud Function Manager (as applicable).

9) Physical access to information and information processing facilities shall be controlled.

10) Users are provided access only to the services that they are specifically authorized to use.

11) The authorization process shall be implemented to ensure that only users who are allowed can access the network segments and services; and

12) Vendor/guest access to Trackon Canada Pvt Ltd's networks shall not be provided.

2.2 System and application access control*(ISO 27001 Control: 9.4)*

13) Access to assets associated with information shall be controlled. Access to applications and infrastructure shall be controlled to ensure that access is granted as per the user's job roles and responsibilities including providing menus to control access to application system functions, and controlling the access rights like reading, writing, deleting, etc.

14) The operating systems of servers, workstations, and/or network devices shall be controlled through a log-on procedure. The log-on procedure shall not disclose any information about the system. Secure log-on procedures shall include:

- Session Time-out: Information systems and applications shall have session time-out control to clear the session screen and terminate both the application and the network sessions after 7 minutes of inactivity.
- Password being entered shall not be displayed and shall be masked.
- Passwords shall not be transmitted in clear text over a network.

- The remote log-on procedure shall be designed with consideration of encryption of information during its transmission; and
- A secure network channel shall be established for remote access (wherever applicable).

15) Password Management System: Passwords provide a means of validating a user's identity and thus establishing authorized access to information and information processing facilities. Following aspects shall be considered:

- Minimum Password Length: 8 characters.
- Password Complexity: Passwords shall not contain all or part of the user's account name and passwords shall contain a mix of alphabetic and special characters and digits.
- Enforce Password History: Last 8 passwords are remembered.
- Maximum Password Age: 90 days.
- Minimum Password Age: 1 day.
- Users shall change their initial password after first log-on.
- Inactive system lockout: 15 minutes.
- Account Lockout Threshold: 5 invalid logon attempts; and
- Account Lockout Duration: 15 minutes.

16) Due to system limitations or business necessity, if any of the password parameters or account policy parameters cannot be followed, specific mechanisms shall be put in place to obtain approvals (exceptions) and implement countermeasures to mitigate the risk of not following the Password Management System.

17) Process for storage and management of critical passwords (associated with Administrator accounts and super-user access) shall be defined and implemented.

18) The use of utility programs that could override the system and application controls shall be restricted and tightly controlled. Only system utilities authorized for the remote management of the servers, workstations, and network devices shall be used. Vendor default utilities shall be disabled during new server, network device, or workstation commissioning. If for troubleshooting purposes there is a need to use these utilities, Administrators of the servers and network devices shall ensure that such utilities are enabled for an authorized activity and are disabled immediately after the use. They shall ensure that activities carried out by using such utilities are logged; and

19) Access to the program source code of operational systems shall be controlled to prevent any corruption of the application programs. Central storage such as SVN shall be implemented to control access to program source libraries and reduce the potential for corruption of computer programs. Trackon Canada Pvt Ltd shall follow appropriate version management processes to ensure the integrity of the program source codes.

2.2.1 Physical entry controls *(ISO 27001 Control: 11.1.2)*

20) Access to the premises shall be controlled and appropriate physical entry controls shall be implemented to limit instances of unauthorized access. Access shall be granted by authorized personnel from the Facilities and Administration Team and monitored periodically. Access shall be revoked on a timely basis if not required.

2.2.2 Securing offices, rooms, and facilities *(ISO 27001 Control: 11.1.3)*

21) Offices, rooms, and facilities shall be secured during and after office hours.

22) Sensitive and/or critical information processing facilities shall be identified and appropriately segregated into protected zones; and

23) Doors and windows of unattended information processing facilities shall be locked and periodically reviewed.

2.2.3 Working in secure areas *(ISO 27001 Control: 11.1.5)*

1) Appropriate physical protection procedures and guidelines for working in secure areas shall be defined, documented, and implemented.

2) All work performed in secure areas shall be authorized and supervised.

3) An authorized Trackon Canada Pvt Ltd on employee shall escort visitors and third-party vendor personnel at all times.

4) Employee, sub-contractor, third party user (housekeeping staff and security personnel) and visitor movement shall be recorded; and

5) Unless specifically authorized by the IT Security Head in consultation with IT Security Manager, personal electronic devices such as, laptops, mobile phones, and USB devices shall not be permitted into restricted information processing facilities.

2.2.4 Delivery and loading areas *(ISO 27001 Control: 11.1.6)*

1) Adequate controls shall be implemented in delivery and loading areas and the activities conducted in these areas shall be monitored. The movement of all incoming and outgoing materials shall be documented, and incoming materials shall be inspected for potential threats; and

2) All incoming and outgoing items, packages, and/or materials shall be registered and inspected by the Facilities and Administration Team.

2.3 Cryptographic Controls *(ISO 27001 Control: 10.1)*

2.3.1 Policy on the use of Cryptographic Controls *(ISO 27001 Control: 10.1.1)* and Key Management *(ISO 27001 Control: 10.1.2)*

Employees, sub-contractors, and partners that plan, design, review, deploy, operate and monitor systems/applications/media that store, transmit and process information shall identify the need for using cryptographic controls considering:

24) Legal, Regulatory and Contractual

- requirements to encrypt information at rest and transit and the type of encryption standards and parameters to be used.
- restrictions on importing or exporting software, and applications for performing cryptographic functions.
- restrictions on developing software or hardware which is intended to perform cryptographic functions.
- restrictions on the usage of encryption; and
- Mandatory or discretionary methods of access by the countries' authorities to information encrypted.

25) Requirements to protect external-confidential and internal-confidential (where applicable) information at rest and transit (over public and private networks).

26) Requirements to protect Personally Identifiable Information (PII), or Sensitive Personal Information (SPI); and

27) The access controls/storage location of the media used to store the information.

The following guidelines shall be considered while using cryptography to protect the confidentiality, authenticity, and/or integrity of information.

28) Appropriate cryptography type, algorithm, key length, and key shall be chosen that are sufficient to defend against threats of unauthorized decryption.

29) Trackon Canada Pvt Ltd Teams that need to use cryptographic methods shall consult the Information Security team for deciding the cryptographic methods to be employed.

30) Individuals shall not use their encryption systems or services to encrypt data. Approved encryption services only shall be used to encrypt data.

31) Entities that need to encrypt communications between themselves shall authenticate themselves to each other using secure and effective processes before they start to exchange data.

32) Encrypted data received from an external source shall be inspected for the presence of security threats after decrypting and before it is processed any further. Encrypted data sent to an external destination shall be examined for the presence of security threats before encryption and transmission.

33) All encryption keys shall be securely stored, and only authorized users shall be able to recover them in case they are lost and are needed to recover information.

34) All encryption keys shall be securely exchanged.

35) Encryption keys that are compromised shall be rendered unusable.

36) Encryption keys shall be changed at a frequency determined by

- The risks to which they are exposed.
- Legal and contractual obligations; and
- Business requirements.

3 Financial Controls Policy

There may be financial risks to Trackon Canada Pvt Ltd which might result in financial losses to the company. Such major risks may include:

1. Theft of Property, assets, and information/data of the Trackon Canada Pvt Ltd
2. Legal proceedings and cases against the company
3. Penalties from regulators
4. Non-payment of the company's receivables by the debtors
5. Damage to Company's property

Financial Controls:

<u>Controls to avoid Theft of Property, assets, and information/data of the Trackon Canada Pvt Ltd</u>

Trackon Canada Pvt Ltd will follow the Data access controls policy defined above to protect the information and data of the Trackon Canada Pvt Ltd

Controls to avoid Legal proceedings and cases against the company and Penalties from regulators

It will be ensured that there is no non-compliance with regulatory requirements. Employees will also be trained on compliance requirements. Trackon Canada Pvt Ltdon will develop a compliance training schedule for its employees where employees will be provided training for the compliance requirements that Trackon Canada Pvt Ltd is legally obligated to.

Following training will be provided to employees (new as well as existing) in a calendar year:

Compliance with legal and contractual requirements including:

- Identification of applicable legislation and contractual requirements
- Intellectual property rights (IPR)
- Protection of records
- Privacy and protection of personally identifiable information
- Regulation of Cryptographic Controls

Information security Compliance includes:

- Information review of information security
- Compliance with security policies and procedures

3.1.1 Protection against external and environmental threats *(ISO 27001 Control: 11.1.4)*

1) Protection against damage from environmental threats shall be designed and implemented.

2) Trackon Canada Pvt Ltd shall ensure that sensitive and/or critical information processing facilities are appropriately equipped and maintained with security controls to safeguard the information contained within the facility against man-made or environmental threats.

3) Trackon Canada Pvt Ltdon shall conduct regular awareness and training programs, for employees on how to identify, respond to and manage external and environmental threats; and

4) Trackon Canada Pvt Ltdon shall conduct periodic fire and safety drills and evaluate employee participation and response.

3.1.2 Physical security perimeter *(ISO 27001 Control: 11.1.1)*

37) Physical security perimeter shall be defined for all physical site's basis the criticality of the information and information processing assets hosted at these locations. Subsequently, physical access restrictions, commensurate with the criticality rating of assets located at these sites and management expectations shall be implemented at these perimeters.

38) Perimeter security controls such as walls, card-controlled entry gates, and/or manned reception desks shall be implemented to protect areas that contain information and information processing facilities; and

All external doors and windows shall be suitably constructed and protected against unauthorized access, with control mechanisms such as bars, alarms, and/or locks.