Trackon Canada Private Limited
Asset Onboarding and Off-boarding Process

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

The purpose of the Physical and Environmental Security Policy is to provide direction for the development and implementation of appropriate security controls that are required to maintain the protection of information systems and processing facilities from physical and environmental threats.

1.3 Scope

The Physical and Environmental Security Policy applies to the India Delivery Centres of the Organization and Delivery Centres, their supporting functions, and the human resources that are located within these physical boundaries.

2 Asset (ISO 27001 Control: 11.2)

2.1.1 Asset siting and protection *(ISO 27001 Control: 11.2.1)*

1) Assetsset shall be sited and protected appropriately to prevent the loss, damage, theft, or compromise of information and information processing facilities leading to interruption of Trackon Canada Pvt Ltd's operations.

2) Trackon Canada Pvt Ltd equipment shall be located and protected in line with its criticality and classification defined in the "Trackon Canada Pvt Ltd _Asset Management Procedure;"

3) Adequate air conditioning equipment shall be installed to ensure the information assets are protected from environmental threats.

4) Supporting equipment such as photocopiers, printing devices, and fax machines shall be protected from unauthorized physical access.

5) Consumption of eatables and beverages inside Trackon Canada Pvt Ltd server rooms shall be prohibited; and

6) Storing of flammable objects within Trackon Canada Pvt Ltd server rooms shall also be prohibited.

2.1.2 Supporting utilities *(ISO 27001 Control: 11.2.2)*

1) Supporting utilities like air conditioning, humidity control, electric power, etc. support operations of information processing facilities and adequate controls shall be implemented to ensure minimal impact to Trackon Canada Pvt Ltd in case of unavailability of supporting utilities; and

2) Facilities and Administration Team shall ensure that the supporting utilities are maintained and reviewed periodically.

2.1.3 Cabling security *(ISO 27001 Control: 11.2.3)*

1) Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

2) Appropriate controls shall be developed and implemented to ensure protection.

3) Network cables, power cords, and patch cables shall be uniformly marked, color coded, and labeled by the cabling standards.

4) Network cabling shall be appropriately protected from unauthorized access, interception, damage, and/or interference.

5) Power and telecommunications cabling shall be appropriately protected from damage and/or disruption; and

6) Access to patch panels and cabling rooms (if separate) / cabinets shall be controlled.

2.1.4 Asset maintenance *(ISO 27001 Control: 11.2.4)*

1) Preventive maintenance shall be performed periodically for all supporting utilities/equipment; and

2) Review of preventive maintenance activities shall be conducted periodically.

2.1.5 Removal of assets *(ISO 27001 Control: 11.2.5)*

1) Removal of assets from Trackon Canada Pvt Ltd's premises (temporarily or permanently) physically shall undergo the prior approval of authorized personnel from the CE Team and appropriate records shall be maintained for future reference.

2) Removal records shall include items removed temporarily and items removed for repairs; and

3) Asset movements shall be registered and reviewed.

2.1.6 Security of equipment and assets off-premises *(ISO 27001 Control: 11.2.6)*

Security shall be applied to off-site assets considering the different risks of working outside the Organization's premises. Users shall be made aware of their roles and responsibilities, and adequate measures to be taken when assets are used off-site.

2.1.7 Secure disposal or re-use of equipment *(ISO 27001 Control: 11.2.7)*

Media shall be disposed of securely and safely when no longer required. Information may be leaked to outside personnel through careless disposal of media. Formal procedures for the secure disposal of media shall be established to minimize this risk (Refer – Trackon Canada Pvt Ltd _Asset Management Procedure); and

2.1.8 Unattended user equipment (ISO 27001 Control: 11.2.8)

All employees, sub-contractors, and partners with access to information assets shall be made aware of the information security requirements and procedures for protecting

unattended equipment, as well as their responsibilities for implementing such protection.

2.1.9 Clear Desk and Clear Screen Policy

Clear Desk Policy applies to paper (hardcopy), laptops, desktops, and removable storage media (pen drive, USB drive, etc.), and Clear Screen Policy applies to information processing systems to ensure unauthorized personnel does not have access to Trackon Canada Pvt Ltd's information.

Clear Desk and Clear Screen Policies shall be implemented and shall include:

Clear Desk Policy

1) Client Confidential / Trackon Canada Pvt Ltd Confidential paper assets (project-specific or product development papers) shall not be left unattended to avoid access by unauthorized personnel. They shall be locked in a cabinet when not in use.

4) Passwords must always be memorized and must never be written down on paper. Any paper that may contain passwords, for example, server passwords (Confidential assets), must be sealed and kept in a secured place

5) All workspaces must always be left clear before leaving for longer periods.

6) All unnecessary documents must not be left unattended or unprotected and should be destroyed by a shredder.

7) If a print is fired, then the concerned person must immediately collect the printout from the printer.

8) Documents must be collected as soon as they are received at the fax machine.

9) Authorized personnel from the Facilities and Administration Team shall shred all printouts left unattended at the printer by the end of the day.

10) Scanning paper items and filing them electronically in the user workstation should be considered as a Best Practice.

11) Desk and filing cabinets must be locked at the end of the day.

12) Mass storage devices such as CD-ROM, DVD, or USB drives must be secured in a locked dra/cabinet.

13) Eating and drinking should not be allowed in the server rooms; and

14) In case of an incident associated with information loss, the matter must be immediately escalated to concerned personnel and should follow the Information Security Incident Management Procedure. *(Refer – Trackon Canada Pvt Ltd _ Incident Management Procedure)*

Clear Screen Policy

1) Users shall lock their computers when leaving their desks and log off when leaving for an extended period. This ensures that the contents of the computer screen are protected from prying eyes and the computer is protected from unauthorized access.

2) Use of Laptop / Desktop Privacy Screens shall be considered in case required.

3) Users shall not keep files/shortcuts on the desktop screen; and

4) Users shall delete all the files from the re-cycle bin regularly.