Trackon Canada Private Limited

Asset Management Policy and Procedures

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

1.2 Purpose

The purpose of the Information Asset Management Policy is to specify the importance of information assets including identification of the asset owner, asset custodian, asset user, asset classification, and determining confidentiality, integrity, and availability ratings of the assets. Additionally, the policy establishes the requirements of controls that need to be implemented for protecting information assets.

1.3 Scope

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

2 Information Asset Management Policy *(ISO 27001 Control: A.8)*

2.1 Responsibility for information assets *(ISO 27001 Control: 8.1)*

1) Information assets shall be broadly divided into the following types: IT Infrastructure and Hardware, Digital, Service, Tangible, and People assets.

2) Asset inventory shall be created and maintained for each Department / Function within the scope of ISMS to identify the information assets utilized for processes of the respective Department / Function.

3) These shall be captured in the Information Asset Inventory and shall be maintained by the IT Security Manager.

4) The Information Asset Inventory shall be prepared and maintained accordingly to the guidelines provided within the "Trackon Canada Pvt Ltd _Asset Management Procedure".

5) Ownership of assets (Asset Owner) shall be assigned when the assets are created/commissioned or when they are transferred to the Organization.

6) If the current Asset Owner cannot continue in that role, the ownership shall be reassigned to an appropriate individual as assigned by the respective department. Change in ownership of information assets shall be updated in the inventory of information assets to reflect the new Asset Owner.

7) Asset Owners may place assets under the custodial control of another person or entity to support operations and maintenance activities associated with the asset; and

8) Return of assets is essential to ensure that the assets entrusted by the Organization are returned in a timely and appropriate manner. HR, CE, and Facilities and Administration Teams shall ensure that all employees, sub-contractors, partners, and third-party users return all of the Organization's assets (including IT and non-IT assets) in their possession upon termination or change of employment based on the contract or agreement.

2.2 Acceptable use of Assets Policy *(ISO 27001 Control: 8.1.3)*

1) Users shall be authorized to utilize Trackon Canada Pvt Ltd information resources only for business purposes for which they have been authorized. Any other use, except for reasonable and occasional personal use, is strictly prohibited.

2) Users must avoid accessing Trackon Canada Pvt Ltd networks for which they do not have a valid business need. While networks are intended to share information, it is each user's responsibility to exercise judgment over the information they access.

3) Usage of Trackon Canada Pvt Ltd's information systems to store, process, download or transmit data that can be construed as biased (politically, religiously, racially, ethnically, etc.) or supportive of harassment shall be strictly prohibited.

4) Downloading, redistribution, and printing of copyrighted articles, documents, or other copyrighted materials to Trackon Canada Pvt Ltd information systems shall be strictly prohibited.

5) Receiving, printing, transmitting, or otherwise disseminating proprietary data, organization secrets, customer data, or other critical information in violation of organization policy or proprietary agreements shall be strictly prohibited.

6) Downloading inappropriate material such as picture files, music files or video files for personal use shall be strictly prohibited.

7) Users shall terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, for example, a password-protected screen saver.

8) Users shall be prohibited from changing the configuration, removing, de-activating, tampering with, or bypassing any security controls such as antivirus or malware prevention/ detection software, modifying registry entries, and logging on the Trackon Canada Pvt Ltd computers or servers used by them.

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

10) Trackon Canada Pvt Ltd's resources shall not be used for commercial or personal use. Resources include but are not restricted to faxes, telephone, printers, scanners, hardcopy, or electronic media. The commercial and personal use includes commercial or personal advertisements, solicitations, or promotions of any outside business, political lobbying or promoting political activities, or any commercial purpose other than official Trackon Canada Pvt Ltd's business activities.

11) Introduction, storage, processing, or transmittal of unauthorized copies of the licensed software and hardware (piracy/copyright and patent infringement) to Trackon Canada Pvt Ltd information assets, and the copying of such material is prohibited.

12) Introduction of Open-source, Freeware, and Shareware Applications whether downloaded from the Internet or obtained through any other media to Trackon Canada Pvt Ltd information assets shall be subject to a formal evaluation and approval process. Only approved and authorized software shall be installed.

13) Introduction of pornographic material into any Trackon Canada Pvt Ltd information systems environment shall be strictly prohibited. The storage, processing, or transmittal of pornographic material on systems, by Trackon Canada Pvt Ltd employees, contractors, or third-party personnel shall be strictly prohibited.

14) Playing computer games on Trackon Canada Pvt Ltd premises shall be prohibited. Users shall not install any computer games in Trackon Canada Pvt Ltd systems.

15) Introduction of destructive programs (for example viruses, self-replicating code, etc.) to cause intentional damage, interfere with others, gain unauthorized access, or inhibit the production of Trackon Canada Pvt Ltd's information systems, shall be strictly prohibited.

16) All users shall limit their usage of external services (for example bulletin boards, online service providers, Internet sites, commercial databases, etc.) to authorized business purposes only. All users shall further comply with the policies, standards, and procedures of the external service (for example bulletin board, online service provider, Internet sites, commercial databases, etc.) that they are using.

17) Internet:

a) Users shall use Trackon Canada Pvt Ltd's internet services appropriately, responsibly, and ethically.

b) theehe internet access may not be used in a way that violates Trackon Canada Pvt Ltd policies, rules, or administrative orders.

c) Users shall only use Trackon Canada Pvt Ltd internet services for business-related activities. The illegal or non-business use of such services shall not be permitted.

d) Do not share, download or upload any confidential, defamatory, discriminatory, proprietary, or copyrighted content

e) Do not post any comments or news about Trackon Canada Pvt Ltd or its clients on social media

networks like Facebook, Twitter, LinkedIn, or public blogs unless authorized to do so.

f) Do not view, store, post, or transmit threatening, harassing obscene or pornographic material

g) Users shall not use Trackon Canada Pvt Ltd internet services for illegal or unlawful purposes, including but not limited to copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, hacking and computer tampering (e.g., spreading computer viruses). Any such activity may result in disciplinary action in line with the "Trackon Canada Pvt Ltd _Human Resource Disciplinary Procedure".

h) Do not click on any unsolicited or suspicious links or popups. Avoid installing any add-ons

i) Users using Trackon Canada Pvt Ltd systems on discovering that they have connected with a website that contains potentially offensive material shall immediately disconnect from the website.

j) Users shall be aware that Trackon Canada Pvt Ltd accepts no liability for the exposure to offensive material that they may have access to via the internet, and

k) The ability to connect with a specific website does not in itself imply that users of Trackon Canada Pvt Ltd's systems are permitted to visit that site.

18) Passwords provide a means of validating a user's identity and thus establishing access rights to information processing facilities or services. All users shall:

a) Keep their passwords confidential.

b) Shall immediately change the initial password provided by the IT Team.

c) Avoid keeping a paper record of passwords, unless this can be stored securely.

d) Change passwords whenever there is any indication of possible system or password compromise.

e) Not reveal the password in an email message.

f) Do Not reveal passwords on questionnaires or security forms.

g) Not reveal the password to co-workers.

h) Select complex passwords which are easy to remember, and not easily guessable or obtained using personal information.

i) Change their password at regular intervals and avoid re-using or cycling old passwords as far as possible; and

j) Do not include their authentication information in any automated log-on process, for example, stored in a macro or function key.

19) Virus Protection:

a) Users shall not open any files attached to an e-mail from an unknown, suspicious or untrustworthy source. Although attachments like '.exe', '.vs.' etc. shall be blocked by the anti-virus software; care shall be taken in case these types of attachments are received.

b) Users shall not open any files attached to an e-mail whose sender and/or subject line is questionable or unexpected. If there is a need to do so, they shall always save the file to the hard drive before doing so.

c) Users shall delete chain/junk e-mails and not forward or reply to any of the chain/junk mails. These types of e-mails are considered Spam, which is unsolicited and intrusive and clogs up the network. Users shall report the delivery of such types of emails to the CE Team.

d) Users shall exercise caution when downloading files from the Internet and shall download only from a legitimate and reputable source. Verify that an

anti-virus program checks the files on the download site; and

e) When in doubt, always err on the side of caution and do not open download, or execute any files or e-mail attachments.

20) Email:

a) All employees shall be responsible for the contents of their email and all actions performed using their email login credentials.

b) Email shall be used only for business purposes. Personal or non-business use of email shall not permit.

c) Automatic forwarding of emails shall be available to only authorized personnel based on approval from the respective Functional Heads.

d) Users shall not send 'Confidential' information via email.

e) Email shall not be used to transmit statements that contain any material that is offensive, defamatory, or threatening to others; and

f) Users shall not send unsolicited bulk mail messages (also known as "junk mail" or "spam"). This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious email, including but not limited to "mail bombing," is prohibited.

21) Additionally, procedures related to the handling of assets shall be adhered to.

a) Asset owners shall ensure that information assets shall be appropriately handled.

b) Information asset handling and labeling process shall be by policy

c) Trackon Canada Pvt Ltd _Asset Management Procedure shall address the information security requirements related to classification, secure

processing, storage, transmission, disposal, destruction, chain-of-custody, and logging of Trackon Canada Pvt Ltd’s information assets.