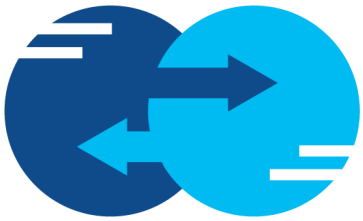

Trackon Canada Private Ltd

Security Policy

Version Number: 1.1

Last Updated: July 2022

Next Update: January 2023

Approved By:

Senior Officer Approval for Program:

TABLE OF CONTENT

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 Operations Security Policy is to establish appropriate controls that need to be implemented to ensure the correctness and security of operations of information processing facilities, protection of information against malware, and other security requirements like backup, change management, capacity management, event logging, technical vulnerability management, etc. The policy intends to establish the controls required to ensure the integrity of the operational systems and to prevent exploitations of technical vulnerabilities.

1.3 Scope

The Operations 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 Security Policy *(ISO 27001 Control: A.12)*

2.1 Operational procedures and responsibilities *(ISO 27001 Control: 12.1)*

2.1.1 Documented operating procedures (*ISO 27001 Control: 12.1.1)*

Standard Operating Procedures (SOPs) for system activities associated with information processing and communication facilities shall be documented and made available to all users who need them. SOPs shall be approved by the respective Functional Head. These procedures shall be developed, documented, and approved when a new information system or service is introduced (wherever applicable). The procedure shall include the roles and responsibilities, the necessary activities to be carried out for the operation, maintenance of the system or service, and actions to be taken in the event of a failure and shall be designed and developed to ensure confidentiality, integrity, and availability of the specific platform or application. Security baselines shall be developed, reviewed, approved, and applied consistently to protect the Company's information assets. Responsibilities for developing, reviewing, approving, and implementing security baselines shall be clearly defined.

2.1.2 Separation of development, testing, and operational environments (*ISO 27001 Control: 12.1.4)*

Development, Test, and Production (operational) environments shall be physically and logically separated from one another as far as possible to reduce the risks of unauthorized access or changes. Access to different environments shall be controlled with due importance given to the segregation of duties. Transfer of changes/information to the production environment shall be strictly controlled based on requisite customer and Trackon Canada Pvt Ltd management approvals.

2.2 Protection from malware *(ISO 27001 Control: 12.2)*

Controls shall be established to ensure that information and information processing facilities are protected against malware. Following guidelines shall be followed to implement, detect and recover from malware:

1) Trackon Canada Pvt Ltd shall protect its network by using anti-virus protections and the network shall be regularly reviewed and updated with the latest anti-virus definition files.

2) Users shall inform any detected variance on their workstations the CE Team. Any anomaly on servers shall also be informed to the CE Team.

3) Upon notification to the CE Team, the malicious activity shall be logged as an Information Security incident. The activity shall be treated and/or terminated as per the Trackon Canada Pvt Ltd - Information Security Incident Management Procedure *(Refer - Trackon Canada Pvt Ltd _Information Security Incident Management Procedure)*; and

4) An incident report shall be submitted to the IT Security Head to ensure that action is sufficient, systems are restored, and appropriate preventive actions are taken.

2.3 Backup *(ISO 27001 Control: 12.3)*

Backup copies of information are essential to recover and restore original data in the event of data loss. Data that has been backed up should be secured from unauthorized access, should be available when required and its restoration should be tested periodically to ensure its validity.

1) A backup schedule shall be prepared to ensure that business requirements are addressed including the retention period of backup.

2) The backup schedule shall provide the details and frequency of the backup to be taken such as daily, weekly, monthly, and yearly.

3) Verification checks shall be performed on the backed-up data to ensure that backup jobs are completed successfully.

4) Backup records (including backup software logs) shall be kept up to date when the backup process starts and ends. In case the backup fails, the occurrence shall be recorded, Root Cause Analysis (RCA) shall be performed, and appropriate corrective action shall be taken and reported to the CE Head / CE Function Manager / Cloud Function Manager (as applicable).

5) Backup software logs shall be monitored, and they shall also be stored securely for possible future reference.

6) Monitoring of backup shall be performed by authorized personnel periodically.

7) Backup media shall be stored on-site and off-site and the backup media shall be given the appropriate level of physical and environmental protection.

8) Tape movement register shall be maintained at the onsite and off-site locations and only authorized personnel from the Finance and CE Teams shall have access to the media.

9) Restoration testing of backed-up data shall be performed periodically based on the criticality of data to ensure that Organization’s data availability requirements can be met.

2.4 Logging and monitoring *(ISO 27001 Control: 12.4)*

1) Event logs shall be enabled for all critical systems. It shall be ensured that the event logs recording the critical user activities, exceptions, and security events are enabled and stored for reasonable periods to assist in future investigations and access control monitoring. Logs shall be monitored and analyzed for any possible unauthorized use of information systems.

2) Security controls shall be built to ensure the integrity of logs. It shall be ensured that the Administrators do not have permission to erase or deactivate logs of their activities. Access to event logs and audit trails shall be provided to authorized users only.

3) Logging facilities and log information shall be protected against tampering and unauthorized access; and

4) The clocks of all relevant information processing systems or security domains shall be synchronized with an agreed and accurate time source. Users shall not have access to change the system date and time settings. The rights shall be restricted to authorized Administrators only.

2.5 Control of operational software *(ISO 27001 Control: 12.5)*

1) Appropriate controls shall be implemented to deploy the software on operational / production systems to minimize the risk of corruption in these systems.

2) Access to install software on operational / production systems shall be restricted to authorized personnel only.

3) Modifications to the operational environment shall be logged and previous versions shall be maintained for contingency/rollback purposes.

4) Operational/production systems shall hold only executable code; and

5) New executable code shall be implemented in the operational / production environment only after successful completion of testing and user acceptance of the system in a separate controlled environment (wherever applicable).

2.6 Information systems audit considerations *(ISO 27001 Control: 12.7)*

1) Information system audits shall be conducted by competent and authorized personnel.

2) Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed upon to minimize the risk of disruptions to business processes; and

3) Audit findings shall be reported in a timely and appropriate manner. Subsequent actions shall be taken based on approval from the IT Security Head / Functional Head (as applicable).