Trackon Canada Private Limited
System Development Lifecycle Policy and Procedures

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 Systems Acquisition, Development, and Maintenance Policy is to assist in defining the security requirements such as access control, source code control, unauthorized modifications, misuse of application data, etc. that need to be identified and integrated during the development and maintenance of applications, software, products and/or services.

1.3 Scope

The System Acquisition, Development, and Maintenance Policy apply to all employees, sub-contractors, and partners who are involved in the software/product development lifecycle.

2 System Development Lifecycle Policy and Procedures: Acquisition, Development, and Maintenance *(ISO 27001 Control: A.14)*

2.1 Security requirements of information systems *(ISO 27001 Control: 14.1)*

1) Information security requirements shall be identified when introducing new applications/systems or making enhancements to existing applications/systems.

2) When developing Information Systems, the requirements specification shall consider the automated controls to be incorporated into the information system and the need for supporting manual controls.

3) The evaluation of software packages shall also take into consideration automated controls as well as their capabilities to support manual controls.

4) System requirements shall be taken from business users based on their needs and information security requirements shall be identified, documented, and approved by Project Managers / Delivery Managers.

5) Information Security requirements shall be integrated throughout the system development or integration project lifecycle from initiation to completion.

6) Adequate security controls as per applicable laws and regulations shall be put in place to ensure the confidentiality, integrity, and availability of the information contained in the publicly available systems of the Organization.

7) Before to deployment, all publicly available systems shall be tested by Research and Development Teams for threats such as denial of service, etc. and it shall be ensured that the identified vulnerabilities are fixed before deployment. A review of all publicly available systems shall be carried out at a specified frequency; and

8) Where additional functionality supplied with a product causes additional security risks, these additional functionalities shall be disabled, or the proposed control structure shall be re-evaluated to determine if advantages can be gained from the enhanced functionality.

2.2 Security in development and support processes *(ISO 27001 Control: 14.2)*

2.2.1 Secure Development Policy *(ISO 27001 Control: 14.2.1)*

Secure development shall be carried out to build up a secure service, architecture, software, and system. The Secure Development Policy shall include:

1) Security of the development environment.

2) Guidance on the security in the system development lifecycle:

   - Security in the system development methodology; and

   - Secure code development principles *(Refer – SDLC)*.

3) Identification of security requirements in early phases of software development.

4) Security checkpoints within the project milestones (as applicable).

5) Secure repositories and security in the version control.

6) Secure coding standards shall be considered and where relevant mandated for use; and

7) Trackon Canada Pvt Ltd shall obtain assurance that the external party complies with these rules for secure development (wherever applicable).

Other than the Secure Development Policy mentioned above, the following practices shall be part of security in development and support processes:

1) System change control procedures for changes to existing systems or introduction of new systems shall be followed and strictly enforced.

2) Changes shall be appropriately authorized, tested, and approved before being implemented in the production environment.

3) New releases/patches about the operating system shall be tested before being implemented in the production environment to ensure that there is no adverse impact on operation, application controls, or security. In case of any exceptions due to technical limitations, approval shall be taken from the respective Project Manager / Delivery Manager.

4) The application controls shall be reviewed to ensure that they have not been compromised by the operating system changes (as applicable).

5) It shall be ensured that notification of operating system changes is provided in time so that appropriate tests and reviews are performed before implementation.

6) Previous version(s) of the software shall be retained as a contingency measure in case a roll-back is required.

7) Secure system engineering principles shall be identified when obtaining security requirements for new systems or making enhancements to existing systems. These principles shall entail the use of secret authentication, data validation, encryption, etc. to ensure appropriate security levels are maintained. Based on the identified requirements, the security shall be designed and implemented in all architecture layers including business, data, applications, and technology for new systems balancing with the need for information security requirements and accessibility.

8) Access to the development environment shall be restricted and controlled.

9) Adequate and appropriate backups shall be taken to ensure availability in case of a disruption.

10) Appropriate version control shall be managed through Source Control Software (as applicable).

11) For vulnerability assessment conducted by third parties, arrangements about intellectual property rights shall be documented in the contract between the Organization and the third-party vendor.

12) System Security Testing shall be conducted during the development phase. Tests shall be conducted against the security requirements identified. Appropriate documentation shall be maintained of the test results and approval; and

13) Any new internally developed information processing system shall be tested before accepting for implementation in the production environment. Acceptance criteria shall be defined, and tests shall be conducted to validate the criteria. System acceptance testing shall include the following phases:

- Setting up acceptance criteria.
- Prepare for system acceptance.
- Validate the acceptance criteria and claims; and
- Testing and acceptance.

2.3 Test data *(ISO 27001 Control: 14.3)*

1) Test data used shall be very much similar to the operational data. Dummy data shall be used for testing purposes.

2) Access to the test environment shall be given to only those personnel who are involved in testing the entire application and not to individual developers based on the approval of the Project Manager / Delivery Manager.

3) Operational information shall be erased from a test environment immediately after the testing is complete; and

4) Audit trails/logs shall be enabled to track the copying and use of operational information