Trackon Canada Private Limited

Authentication & Identity Management Policy

Version Number: 1.1

Last Updated: July 2022

Next Update: January 2023

Approved By:

Senior Officer Approval for Program:

TABLE OF CONTENT

Policy Statement 3

Our Commitment 3

Purpose 3

Scope 3

Authentication & Identity Management Policy (ISO 27001 Control: A.9) 4

Business requirements of Authentication & Identity Management (ISO 27001 Control: 9.1) 4

User access management (ISO 27001 Control: 9.2) 5

User responsibilities (ISO 27001 Control: 9.3) 8

System and application access control (ISO 27001 Control: 9.4) 8

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 Policy is to ensure that only authorized personnel are provided access to information and information processing facilities (including operating systems, networks, and applications). Thus, helps ensure the protection of confidentiality, integrity, and availability of information from unauthorized access, malicious intent, compromise, and theft.

1.3 Scope

The Authentication & Identity Management Policy applies to, but is not limited to:

1) Internally hosted business applications (Pulse, MS Dynamics AX, Tally, Jenkins, Bugzilla, etc.).

2) External Vendor hosted business applications (Salesforce, Jira, Support Portal, Concur, Alsek, Excelled Global, OpenAir, Jive, Market, Factiva, etc.).

3) Tools (Helpdesk, Trak, Office 360, screener, Messenger, VPN, etc.).

4) Database.

5) Network and Security devices.

6) Domain Server (AD, DNS, DHCP, SMTP).

7) Application servers; and Secure Tokens, Key Fobs, etc.

2 Authentication & Identity Management Policy *(ISO 27001 Control: A.9)*

2.1 Business requirements of Authentication & Identity Management *(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 the 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/guestlist access to Trackon Canada Pvt Ltd’s networks shall not be provided.

2.2 User access management *(ISO 27001 Control: 9.2)*

The main objective is to ensure authorized user access and prevent unauthorized access to systems and services.

1) Access to the information assets and services for all users (employees, sub-contractors, or partners) shall be granted, modified, or revoked through a formal user access provisioning process. Access for new joiners shall be granted only after background verification/ screening confirmation from authorized personnel from the respective Department/ Function.

2) Access revocation of separating users shall be performed on a timely basis based on the intimation from the HR Team.

3) Privileges/ privilege access to users shall be given based on the requirements of their job function and role, on authorization from CE Head / CE Function Manager / Cloud Function Manager (as applicable).

4) Allocation of additional privileges, more than what is required for the job function, shall be granted after getting approval from the user's Functional Head / CE Function Manager / Cloud Function Manager (as applicable).

5) Privilege Job Function Matrix shall be developed and documented and sent to CE Head / Cloud Function Manager (as applicable) for approval.

6) Review of the list of users with key privileged rights, to determine if each user's access rights are appropriate based on their job description/role and responsibilities, shall be performed periodically by the Functional Head / CE Head / Product Manager Cloud Engineering, as applicable.

7) All user secret authentication information (individual as well as Administrator) shall remain confidential and shall not be shared, posted, or otherwise divulged in any manner.

8) Initial secret authentication information (initial password) shall be provided to the user securely over email during the user access provisioning process and the system shall be configured to force the users to change the initial password immediately after the first login.

9) Default vendor (wherever applicable) secret authentication information shall be altered following the installation of systems or software; and

10) User access review shall be conducted annually to ensure access is commensurate with the user's job roles and responsibilities.

- The System Administrators shall review the individual workstations including laptops and desktops on a bi-annual basis to ensure that unauthorized software is not downloaded or installed on these systems.

- The CE Head / CE Function Manager (as applicable) / Cloud Function Manager (as applicable) shall review the access logs for servers (with Asset Value as High and Medium) on a bi-annual basis to detect any suspicious access to the Trackon Canada Pvt Ltd servers.

- Project Managers/Delivery Managers shall review the access logs for respective team folders on SVN on a half-yearly basis to detect any suspicious access to the source code libraries, etc.

- The CE Head / CE Function Manager / Cloud Function Manager (as applicable) shall review the access logs for intranet applications periodically to detect any suspicious access to the intranet applications.

- Any identified discrepancy, if required, shall be treated as Information Security Incident and shall follow the “Trackon Canada Pvt Ltd_ Information Security Incident Management Procedure” for the remediation/closure of the incident.

- The review shall also include a review of privileged user access rights, to determine if each user’s access rights are appropriate based on their job description/role and responsibilities. The review shall be performed bi-annually by CE Function Manager and IT Security Head based on the following scenarios:

    - When Business Applications, Tools, Servers, Domain Controlled, or Network Devices / Systems undergo a major change requiring a change in the existing roles or when a new module or functionality is added.

    - A new job function is created.

    - The existing job function or role has changed; and

    - Resource change is required.

- Modified Privileged Job Function matrix shall be sent to CE Head / Cloud Function Manager (as applicable) for approval before implementation.

2.3 User responsibilities *(ISO 27001 Control: 9.3)*

All users with access to information assets are required to understand their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of systems. Users shall ensure that secret authentication information, is not to be transmitted in clear text. Similarly, displaying secret authentication information shall be masked, suppressed, or otherwise obscured such that unauthorized parties may not be able to observe and/ or subsequently recover them. Acceptable Use of Assets Policy defines the steps to be followed for passwords.

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

1) 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, controlling the access rights like reading, writing, deleting, etc.

2) 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).

3) 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 the initial password after the first log-on.
- Inactive system lockout: 15 minutes.
- Account Lockout Threshold: 5 invalid logon attempts; and
- Account Lockout Duration: 15 minutes.

4) 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.

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

6) 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

7) 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. Track shall follow appropriate version management processes to ensure the integrity of the program source codes.