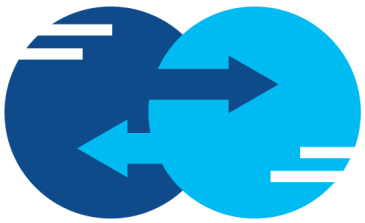

Trackon Canada Private Limited

Password Management Policy

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

CONFIDENTIALITY CLAUSE 3

CONTACT INFORMATION 3

INTRODUCTION 3

PURPOSE OF THE DOCUMENT 3

SCOPE AND APPLICABILITY 3

POLICY 4

- USER MANAGEMENT 4
- PASSWORD COMPROMISE 4
- PASSWORDS OF PRIVILEGED USERS 4
- EXCEPTIONS TO PASSWORD POLICY 5
- PASSWORD PARAMETERS 5

1.0 CONFIDENTIALITY CLAUSE

This document is the property of Trackon Canada Private Limited. All ideas and information contained within the document are the intellectual property of Trackon Canada Pvt Ltd. These

documents are not for general distribution and are meant for use solely by the person/persons to whom it is specifically issued or shared. Trackon Canada Pvt Ltd does not share this document with any third party or vendor unless specifically exempted by the competent authority. Copying or unauthorized distribution of these documents, in any form or means including electronic, mechanical, photocopying, or otherwise is illegal.

2.0 CONTACT INFORMATION

For any questions regarding this policy, please contact -

Email: rk@paypenny.io

3.0 INTRODUCTION

The purpose of the document is to establish a password policy that applies to Trackon Canada Pvt Ltd. The relevant system comprises IT infrastructure which handles important data, information systems, and processes for transmission. It is pertinent for the organization to ensure minimal risk to the Confidentiality, Integrity, and Availability (CIA) of the data/information collected, stored, and processed. The perceived risk is both from an external and internal perspective.

Passwords are an important aspect of system security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of the entire network. As such, all employees (including contractors and vendors with access to the systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

4.0 PURPOSE OF THE DOCUMENT

The purpose of this policy is to establish a standard for the creation of strong passwords, and the protection of those passwords, and to define the frequency of change.

5.0 SCOPE AND APPLICABILITY

Password policy applies to all information assets, IT, and OT systems, for Trackon Canada Pvt Ltd. across all locations.

Trackon Canada Pvt Ltd. employees, contractors, third-party staff, or any other partners who are directly or indirectly a part of Trackon Canada Pvt Ltd. ecosystem and have access to Trackon Canada Pvt Ltd. systems, processing facilities shall adhere to blow stated password policy and ensure compliance.

6.0 POLICY

6.1 USER MANAGEMENT

All User passwords (Individual as well as Administrator) must remain confidential and must not be shared, posted, or otherwise divulged in any manner. An initial password must be provided to the users securely during the user creation process & the system must be configured to force the users to change the initial password immediately after the first login.

- Once the user is created the username should be shared in emails and initial passwords should be communicated to the user through a phone call.
- Appropriate procedures must be put in place for storing and management of administrative passwords for critical information systems or assets.
- Two-factor authentication mechanism must be used to provide access to all critical information systems or assets.
- Critical Information Systems or critical assets are the assets that are determined as highly critical based on confidentiality, integrity, and availability rating in the asset register. The password and account policy should be enforced for all user and administrative accounts on operating systems, applications, databases, and all other information protected by password controls.
- Due to system limitations or organizational necessity if any policy parameters are not followed, then approvals shall be taken from the respective authority, and implement countermeasures to mitigate the risk of not following the password policy.

6.2 PASSWORD COMPROMISE

The incident of a password compromise should be immediately reported to the information security manager. A user must ensure to log off before leaving a computer unattended and the password should be changed immediately whenever there is suspicion of compromise. Systems should be configured to log off automatically after 5 minutes of idle time or inactivity.

6.3 PASSWORDS OF PRIVILEGED USERS

The passwords of privileged users (such as network technicians, technicians, and network operators) should be most secure and be changed as per defined frequency i.e., after 60 days. The operating system and application running in the system should have different passwords and online password generation tools should be avoided to generate passwords.

Passwords should not be sent across any network unless protected by some form of encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network securely. Account credentials should not be shared with anyone in any circumstance.

6.4 EXCEPTIONS TO PASSWORD POLICY

The exceptions to password policy can be approved by authorities on a case-to-case basis by understanding the limitations and issues of the systems. These exceptions can be approved only for a limited period.

6.5 PASSWORD PARAMETERS

Passwords provide a means of authenticating an employee's identity and thus establish access rights to information and information processing assets. Password parameters in business applications, tools, servers, network devices, etc. should be configured as follows:

Sr. No.	Description	Values (for normal users)	Values (for privileged users)
1.	Password History	The last 5 passwords remembered	The last 5 passwords remembered
2.	Minimum Password Length	08 characters	12 characters
3.	Password Complexity	Minimum 1 Upper Case, 1 Lower Case, 1 Digit and1 Special Character	Minimum 1 Upper Case, 1 Lower Case, 1 Digit and1 Special Character
4.	Maximum Password Age	90 days	90 days
5.	Account Lockout Threshold	5 invalid login attempts	3 invalid login attempts
6.	Reset Account Lockout Counter	15 minutes	15 minutes

Poor passwords not satisfying the password standard shall not be allowed to create. All passwords must be changed at least every 90 days. The system automatically asks the user to change the password before completing this duration.

6.6 REMOTE ACCESSIBILITY OF SYSTEMS AND SERVERS

Remote accessibility of systems and servers preferably should be avoided. In an emergency, the remote accessibility of the servers and systems may be allowed using passwords and/or passphrases under a remote accessibility setup.

TIPTAP shall enforce a password history policy that will set how often an old password can be reused. It should be implemented with a minimum of 5 previous passwords remembered. This policy will discourage users from reusing a previous password, thus preventing them from alternating between several common passwords.

6.7 IF ANY USER FORGETS A PASSWORD

If any user forgets the password, he/she should request mail to admins or super users of the systems and request them to reset the passwords. Reset passwords should be communicated to the user through a phone call and users should be forced to change the reset password at first login after resetting the password.

6.8 SHARED USER ACCOUNTS

Shared user accounts shall not be permitted to be used by employees or subcontractors. Where it is not possible to implement individual user ids and passwords, alternative solutions for restricting and auditing access privileges must be evaluated for feasibility and must be implemented. All users should use strong passwords so that they are not guessed and compromised easily.

Poor passwords not satisfying the password standard shall not be allowed to create. All electronics Devices, industrial devices, network devices, and cyber security devices used in the network must be password protected. There shall not be any provision to access the system by using its default password. Simultaneous login from different places on behalf of the same user shall be avoided.

6.9 OTHER NECESSARY GUIDELINES

- Do not reveal a password over the phone, email, or massages to anyone
- Do not share/type the passwords in front of others, family members, and friends
- Do not hint at the format of a password (e.g., “my family name”)
- Do not reveal a password on questionnaires or security forms
- Do not reveal a password to a co-worker while on vacation
- Do not reveal the "Old Passwords" to anyone

- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file or post on a computer system unencrypted