IT2

Category: Information Technology

PASSWORD POLICY

I. PURPOSE

Identification and authentication access controls play an important role in helping to protect Information Systems. The purpose of this policy is to protect Information Systems by defining requirements for new passwords, changes to passwords, Multi-Factor Authentication (MFA), and Single Sign-on.

II. Background

Computer accounts are used to grant access to Pioneer's Information Systems. The process of creating, controlling, and monitoring computer accounts is extremely important to the overall security program.

III. Scope

This policy applies to all Pioneer Staff that have access to the organization's Information Resources.

IV. POLICY

Pioneer's IT support shall ensure:

- Policies and procedures manage the process of creating, changing, and safeguarding passwords/phrases and Multi-Factor Authentication.
- Policies to prevent staff from sharing passwords/phrases with unauthorized persons.
- Procedures advise staff to commit their passwords/phrases to memory rather than having them written down.
- Policies and procedures govern the password/phrase change frequency.
- Policies and procedures dictate when passwords/phrases must be supplemented with additional access controls.

Adopted: October 16, 2025
Resolution: 2025-39

This Policy applies to all Pioneer related authentication activities including, but not limited to, the following:

- Administrative accounts
- User accounts
- Network infrastructure devices (e.g. firewalls, routers, wireless access points, etc.)
- Third party service providers
- Web applications
- Workstations, Laptops, Servers
- Mobile devices

New User Accounts

When granting access for a new user/account:

- System administrators will establish a unique ID and unique password/phrase.
- The user password will be conveyed to the user in a secure manner.
- When the user logs on for the first time, the user will be required to change their initial password/phrase to something that meets the requirements of this policy.

Selecting Passwords/Phrases

When selecting a new password/phase, system administrators and users should select passwords/phrases that are long, strong, and complex. Where possible, Staff shall choose passwords/phrases that meet the following requirements:

- Contain both upper- and lower-case characters (e.g., a-z, A-Z).
- Include both numbers (0-9) and special characters (e.g. @, #, $, *).
- Have a minimum of at least 12 characters and preferably 16 characters long.

- Where possible, use different passwords/phrases for general office activities (e.g. e-mail, file access) vs. systems that store sensitive or confidential data.

Staff should not choose passwords/phrases that:

- Include single common words (e.g., "password", "secure")
- Common or predictable phrases
- Are the same as passwords/phrases used on Staff personal accounts (e.g. personal e-mail, on-line banking, or social media).
- Contain personal information such as a spouse or pet's name, social security number, driver's license number, street address, phone number, etc.
- Contain sequences or repeated characters. For example, 1234, 3333, etc.

Staff with special system privileges, assigned by a transaction, program, process, or group membership, should select a unique password/phrase from other accounts held by that individual.

Password/Phrase Guidelines

Staff shall follow security guidelines to ensure passwords/phrases are not compromised. Security training and awareness programs shall ensure Staff is:

- Educated on security related risks.
- Reminded of security requirements when selecting and protecting passwords/phrases.
- Reminded to be careful when using social media so the password/phrase are not compromised.

Passwords/phrases should be kept secure. To help with that:

- Avoid sharing with any unauthorized persons.
- Try not to store/write down in plaintext.
- Avoid transmitting in clear (unencrypted) text.

- Avoid inserting into unencrypted e-mail messages or other forms of electronic communications.

Passwords shall only be stored in a manner approved by Pioneer's IT support:

- Service Accounts and Shared Administrative accounts shall be recorded in the organization's information management system
- Corporate, personal logins (email, etc.) shall be stored in the organization's private Password Manager software when implemented.

If a Staff member believes that their password/phrase has been compromised or made available to others, the Staff member must immediately change their password and reach out to IT support.

If Pioneer staff demands a password to be shared, refer them to this policy or have them contact IT support.

It's good practice to update passwords/phrases regularly. As a general guideline:

- Try to change user passwords or phrases at least every 90 days, unless the application or service you're using recommends a different schedule.

When selecting a new password/phrase, Staff should not repeat any of their prior passwords/phrases.

Software Applications

IT support should ensure programs contain the following security precautions:

- Applications should require each user to have their own unique ID (e.g. not shared, no user groups) unless there's a

clear operational need or it's more practical to use a shared account for specific use cases.

- Passwords/phrases and Sensitive Information must be protected using strong encryption.
- Passwords/phrases and Sensitive Information must not be transmitted or stored in clear text.
- Ensure applications timeout and require the user to enter a password/phrase after a period of inactivity.
- Where possible, single sign-on (SSO) should be configured to the organization's IdP to ensure all data access is secure and managed.

V. ENFORCEMENT

Any staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. DISTRIBUTION

This policy is to be distributed to all Pioneer staff who use Information Resources.

VII. Policy Revisions

The Chief Executive Officer is authorized to make minor modifications, clarifications, or administrative updates to this policy, provided that such changes do not alter the policy's intent, scope, or underlying principles.

VIII. HISTORY

Version	Date	Description	Approved By
2021.1	7/15/2021	Initial policy release	Board of Directors
2025.1	10/16/2025	Policy Update	Board of Directors