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 and changes to passwords and Multi-Factor Authentication (MFA) use.

II. DEFINITIONS

"Agency Business" shall mean carrying out the responsibilities and duties of the office or position held by the employee.

"Employee" or "Staff" shall mean those individuals who are employed for a salary or wage by Pioneer, not including members of the Board of Directors or individuals working under a contract for services unless specifically identified in said contract.

"Information Systems" shall mean an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products..

"Sensitive Information" shall mean data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization.

III. Background

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

IV. Scope

Adopted: July 15, 2021
Resolution 2021-29

This policy applies to all staff that utilize Information Systems with IDs and passwords (credentials). This policy applies whether staff is using Pioneer Information Systems, staff owned devices for Executive Director approved work, or staff use of Information Systems of third-party service providers for work related activities.

V. POLICY

The IT department shall ensure:

- Policies and procedures manage the process of creating, changing, and safeguarding passwords/phrases and Multi-Factor Authentication.
- Policies and procedures prevent staff from sharing passwords/phrases with others.
- Procedures advise staff to commit their passwords/phrases to memory and not allow them to be written down. However, in the event a password needs to be written down in place of memorization, it should be stored digitally and saved with password protection.
- Policies and procedures dictate when passwords/phrases must be supplemented with additional access controls.

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

- Administrator accounts.
- User accounts.
- Network infrastructure devices (e.g. firewalls, routers, wireless access points, etc.).
- Third party service providers.
- Web applications.
- Screen savers.
- Mobile devices.

A. 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.
- The user will be required to setup Multi-Factor Authentication.

B. SELECTING PASSWORDS/PHRASES

When selecting a new password/phase, system administrators and users must 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. and either a password or phrase.
- 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 common words such as those found in a dictionary.
- 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.

C. 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 must not be:

- Revealed to anyone.
- Stored, written down, or transmitted in clear (unencrypted) text.
- Inserted into unencrypted e-mail messages or other forms of electronic communications.

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 the IT department.

If someone demands a password, refer them to this policy or have them contact the IT Department.

D. Password/Phrase Changes

Passwords/phrases must be changed on a regular basis according to the following schedule:

- Pioneer User Account. Pioneer requires all staff to use Multi-Factor Authentication (MFA) on these accounts, which is setup

during employment orientation. Based on the MFA requirement, Pioneer does not require these passwords to be updated, which aligns with Microsoft recommendations and industry standards.
- Third-party software. Follow the recommended password update requirements.

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

E. Software Applications

Staff must ensure programs contain the following security precautions:

- Each user should have their own unique ID (e.g. not shared, no user groups).
- 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.

VI. ENFORCEMENT

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

VII. DISTRIBUTION

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