Password Protection Policy

Purpose

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of VWPLD's resources. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all staff, contractors, and affiliates who have or are responsible for an account or any form of access that requires a password on any system that resides at VWPLD, has access to the library staff network, or stores any nonpublic library information.

Policy

All staff and contractors who have access to library accounts or the library staff network must follow "Password Requirements," as outlined below, to select, secure, and change their passwords.

Password Requirements:

Password Creation

1 The password cannot contain all or part of your user account name or login ID.

2 Users must not use the same password for VWPLD accounts as for other non-library accounts (for example, personal ISP account, personal email account, benefits, and so on).

3 The password must be at least eight (8) characters in length.

4 The password must contain characters from three of the following categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numbers (0 through9)
- Nonalphabetic characters (for example, !, $, #, %)

5 The following are examples of passwords that follow the necessary criteria. Do not use these examples.

- &Ez2do, Suce$$ful, 2S!ncere, Etc&etc,

Password Change

1. Passwords must be changed every 180 days (January 1^{st} and July 1^{st}).

2. The three previous passwords cannot be used.

3. The password cannot be changed again until a period of 24 hours has passed.

Password Protection

1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive and confidential information.

2. Passwords must not be inserted into email messages or other forms of electronic communication.

3. Passwords must not be revealed over the phone to anyone.

4. Do not reveal a password on questionnaires or security forms.

5. Do not hint at the format of a password (for example, "my family name").

6. Do not share passwords with any member of the public, including family members.

7. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

8. Do not use the "Remember Password" feature of applications (for example, web browsers).

9. Any user suspecting that his/her password may have been compromised must report the incident to the director and change all passwords. If a user suspects his/her password to SHARE has been compromised, the director will report the incident to IHLS.