Pacific University
Password Management Policy

Pacific University reserves the right to amend or otherwise revise this document as may be necessary to reflect future changes made to the Information Technology (IT) environment. You are responsible for reviewing this Policy periodically to ensure your continued compliance with all Pacific University IT policies. By accepting and using a Pacific University user account, the user agrees to this policy.

This document has been reviewed and endorsed by the University Technology Committee, while enacted and enforced by the Chief Information Officer (CIO) and the staff of University Information Services.

1.0 Overview

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

2.0 Purpose

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.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Pacific University facility, has access to the Pacific University network, or accesses or stores any non-public Pacific University information, including protected health information (PHI).

4.0 Policy

4.1 General

- Accounts will not be shared. Each user or administrator must have his/her own unique account.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every twelve months. The recommended change interval is every six months.

- Passwords may not be reused for a period of two years.
- User or System Level passwords must not be inserted into email messages or other forms of electronic communication.
- Pacific staff will never ask for you to provide your password or other personal information via email.
- All PUNet ID password changes should be made using the University's myAccount page.
    - Other applications which may not use the PUNet ID for authentication may have separate password change protocols.
- All user-level and system-level passwords (PUNet ID and others) must conform to the standards described below.

5.0 Information Technology Password Standards

It is expected all systems connecting to the Pacific network with the purpose of accessing information or services must do so using secure credentials and will meet 'General Password Construction Standards' as outlined if technically feasible.

A. General Password Construction Standard

User Level Account Passwords are used for various purposes at Pacific University. Some of the more common uses include: access to websites, email accounts, university applications, and local workstation logins. Everyone should be aware of how to select strong passwords and use them.

User level accounts must meet the following minimum criteria when technically feasible:

- Passwords will be at least eight characters.
- Passwords will be alphanumeric.
- Passwords must be changed every 12 months.
- Accounts will be either disabled or temporarily locked for at least 15 minutes after five failed login attempts.
- Passwords must be changed upon first system use or after a password reset by UIS.
- Accounts which have not been used in twelve months will be locked.
- The following are **not** permitted as passwords:
    - The word *password*

    - The PUNet ID
    - Passwords beginning or ending with spaces
    - Passwords that contain only numbers at the beginning or end of the password such as *secret1234 or 1234secret.*
- Users should consider creating and using a passphrase so that passwords are both complex and also easy to remember. Examples include:
    - *Ohmy1stubbedmyt0e*
    - *ILik3MyD0g*
    - *EyeAm@w1nner*
    - *Y3ll0wSubm@r1ne*

NOTE: Do not use any of these examples as actual passwords!

In addition to the standard password requirements noted above, Administrator or System Level accounts with special elevated privileges used for administering network equipment, servers, databases, etc. may be subject to additional password requirements. Please contact UIS for these additional password standards. Administrator accounts are not to be used for standard computing activities.

B. Password Management Standards
Passwords are the virtual keys to Pacific University systems and information resources. They must be protected. Users must adhere to the following standards to help ensure passwords are not compromised.

- Do not use the same password for Pacific University accounts as for other non-Pacific University access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Pacific University access needs.
- All passwords are to be treated as sensitive, confidential Pacific University information.
- Never share a password over email, over the phone, or in front of others. This includes questionnaires and security forms.
- Never share your password with anyone, including friends and family members, a manager or supervisor, or an administrative assistant or secretary. Treat your password like you would an ATM PIN. You are responsible for any misuse of your account.

- Never share your password with co-workers before or while on a vacation.
- Never give access to your computer, or any private information, to anyone claiming to work for University Information Services unless you know them personally or they show you proper picture ID.
- Nobody in the university is authorized to demand your password. If someone demands a password, refer them to this document or have them call someone in University Information Services.
- Do not use the "Remember Password" feature of applications (e.g., Internet Explorer, Outlook, Firefox).
- Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smartphones or similar devices) without encryption.
- Mobile devices containing University data, owned by the University or not, must also be password/PIN/pattern protected.
- If an account or password is suspected to have been compromised, report the incident to University Information Services and change all passwords. Reports should be made to the Technology Information Center at 503.352.1500.
- Password cracking or guessing may be performed on a periodic or random basis by University Information Services or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Students in violation may be subject to actions as described in the Student Handbook.

7.0 Definitions

Terms

User Level Account – A user account used by most members of the Pacific community to carry out normal computer usage activities such as logging into computers, sending email, accessing applications, performing standard functions, etc.

Administrator or System Level Account – A user account that has the ability to make computer system changes that cannot be made by the majority of users. Such accounts will include, for example, the system administrator(s) and Network administrator(s) who

are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

8.0 Revision history
Approved: by University Technology Committee
Reviewed:
Revised:
Version 1.0 Approved 08/12/2010
Version 1.1 Approved 11/01/2012
Version 1.2 Approved 12/18/2013
Version 1.3 Approved 08/25/2015 HIPAA Taskforce
Owner: Information Security Officer

Attachment:

References: