California University of Pennsylvania
Pennsylvania State System of Higher Education

Technology Policy Number 2013-03
Password Policy

Approved by: Cabinet

History: Issued – 1/29/2013

Revised

Additional History

Related Policies:

Additional References:

I. Introduction

Appropriate password security is necessary to protect the University's academic interactions, business and research. Passwords are often the first, and sometimes the only, defense against unauthorized access or intrusion of a specific computing system. Creating and maintaining secure passwords is an important step to protect against unauthorized use of computing resources.

This policy describes the requirements necessary for creating and maintaining password security on all California University of Pennsylvania Accounts.

II. Purpose:

The purpose of this policy is to require a standard set of rules regarding the length, complexity and expiration time period for passwords and storage of passwords.

III. Statement of Policy

Employee and Contractor Passwords:

California University of Pennsylvania Accounts created for faculty, staff and contractors must use the following password policy. This standard does not apply to system administrator type accounts or administrative type accounts for network devices. The password complexity for administrative accounts and network devices should exceed those listed in this procedure.

- Password must be at least 8 characters in length.

- Password must be different than the previous 4 passwords.
- Password must consist of 3 out of 4 of the following:
    - Uppercase character.
    - Lowercase character.
    - Numeric characters.
    - Symbol characters.
- Password must have a minimum age of 1 day.
- Password must have a maximum age of 90 days.

Student Passwords

California University of Pennsylvania Accounts created for students must have passwords that comply with the following:

- Password must be at least 8 characters in length.
- Password must be different than the previous 4 passwords.
- Password must consist of 3 out of 4 of the following:
    - Uppercase character.
    - Lowercase character.
    - Numeric characters.
    - Symbol characters.
- Password must have a minimum age of 1 day.
- Password must have a maximum age of 180 days.

Storage of Passwords

- Passwords must be stored in a strongly encrypted format.
- Passwords must be stored in a non-reversible format.

Transmission of Passwords

- For any new systems, passwords MUST be encrypted when transmitted on ANY type of network. For existing systems, passwords should be encrypted when transmitted on ANY type of network whenever possible.

Account lock out provision

- The University will disable user accounts for a period of time if there are repeated attempts to login with an invalid password.
    - Accounts will be locked out after 6 invalid login attempts.
    - Lockout duration must be at least 10 minutes.
        - For users in the CDE (Cardholder Data Environment) for PCI, this value will be 30 minutes.
        - Users in the CDE are also required to re-authenticate after 15 minutes of inactivity.
    - Account lockout counter will be reset after 5 minutes.

IV. Definitions

- CDE (Cardholder Data Environment) - This includes all processes and technology as well as the people that store, process or transmit customer cardholder data or authentication data, including connected system components and any virtualization components (i.e., servers, applications, etc.)

- Non-reversible format – A reversible format stores a user name in a list with an associated password. When the user logs on this password is decrypted. The decrypted password is then compared to the password the user typed. A non-reversible format eliminates this weakness by performing a transformation on the password that makes it practically impossible to turn it back into the original password.

- PCI (Payment Card Industry) - Security procedures from the PCI Security Standards Council for merchants that accept credit cards online.