Research Affairs User Account Password Policy

Last updated February 25, 2013

x:\rait policies\research affairs ad user account password expiry policy v3.docx

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of UCSD's resources. All users, including contractors and vendors with access to UCSD systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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.

Scope

The scope of this policy includes all employees or affiliates 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 UCSD's Research Affairs maintained equipment, has access to Research Affairs maintained network, or stores any non-public Research Affairs information.

Research Affairs AD User Account Policy

1. Passwords must be changed at least every 120 days
    a. Passwords on accounts that have access to sensitive data (PII, FERPA, etc.) must be changed every 90 days
2. Accounts that have not been used for 180 days will be automatically disabled
3. Accounts that have been disabled for more than 365 days may be deleted
4. All passwords must conform to the following guidelines

General Password Construction Guidelines

All users supported by the Research Affairs Information Technology unit (RAIT) should be aware of how to select strong passwords. Strong passwords have the following characteristics:

- Contain at least 7 alphanumeric characters.
- Contain at least three of the five following character classes:
    - o Lower case characters
    - o Upper case characters
    - o Numbers
    - o Punctuation
    - o "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

PassPhrases: Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

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

Avoid Using Weak Passwords. Weak passwords have the following characteristics:

- The password contains too few characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - o Names of family, pets, friends, co-workers, fantasy characters, etc.
    - o Computer terms and names, commands, sites, companies, hardware, software.
    - o The words "<Company Name>", "sanjose", "sanfran" or any derivation.
    - o Birthdays and other personal information such as addresses and phone numbers.
    - o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - o Any of the above spelled backwards.
    - o Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Password Protection Standards

- Use different passwords for UCSD accounts from other non-UCSD access (e.g., personal ISP account, option trading, benefits, etc.).
- When possible, use different passwords for different UCSD systems. For example, select one password for Active Directory) and use a different password for Single Sign On
- Do not share UCSD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential UCSD information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the UCSD Security Team (security@ucsd.edu).
- Always decline the use of the "Remember Password" feature of applications (e.g., Eudora, Outlook, Internet Explorer, etc).

If an account or password compromise is suspected, report the incident to Research Affairs IT Support (raitsupport@ucsd.edu) or the UCSD security team (security@ucsd.edu).

==========

Password Expiration Email Notification

As a courtesy, the message below will be sent to AD users email accounts letting them know they will need to change their password:

- 15 days prior to expiration
- 6 days prior to expiration
- 2 day prior to expiration
- 1 day prior to expiration

==========

Subject: Active Directory (AD) account password expiration

Dear <first name> <last name>,

Your Active Directory (AD) account password will expire in < > days. If you do not change your password prior to this date, your account will be locked.

Instructions to change your password before the deadline are available on the UCSD Blink portal, and are searchable using the phrase "Campus-wide Password Reset". Note--we are deliberately not providing a link to that page so this message does not appear to be phishing email.

If you have questions, please contact Research Affairs IT Support Team at raitsupport@ucsd.edu or 858-534-9499.

Research Affairs IT Support Team