CALIFORNIA STATE UNIVERSITY
BAKERSFIELD

Campus Password Policy

CSU Bakersfield Policy

Document Number:	ITS-90.020	**Last Revision Date:**	2/1/2022
Responsible Office:	Information Technology Services	**Effective Date:**	2/5/2021
Primary Author:	CIO & AVP of Information Technology		

General Description

Purpose:

Establish a password standard for all CSUB system accounts including students, alumni, staff and facility based upon the most current NIST, and California State University Office of the Chancellor best practices.

Definition:

A password is a memorized secret authenticator. It is a secret value intended to be chosen and memorized by the user. Passwords need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorized secret is something you alone know. Users are responsible for safeguarding passwords for their accounts.

Scope:

This policy applies to all CSUB students, alumni, staff and facility

Policy/Procedure

Policy

Passwords must:

- Not contain the user's account name or parts of the name that exceed two consecutive characters
- Be at least eleven (11) characters in length
- Contain characters from three of the following four categories:
  - Uppercase characters (A through Z)
  - Lowercase characters (a through z)
  - Numbers (0 through 9)
  - Non-alphanumeric characters (for example, !, $, #, %)
- No reuse, passwords will not be allowed to be set to any of the users last 12 previous passwords
- Will be checked against a known password compromised list before accepted

Controls

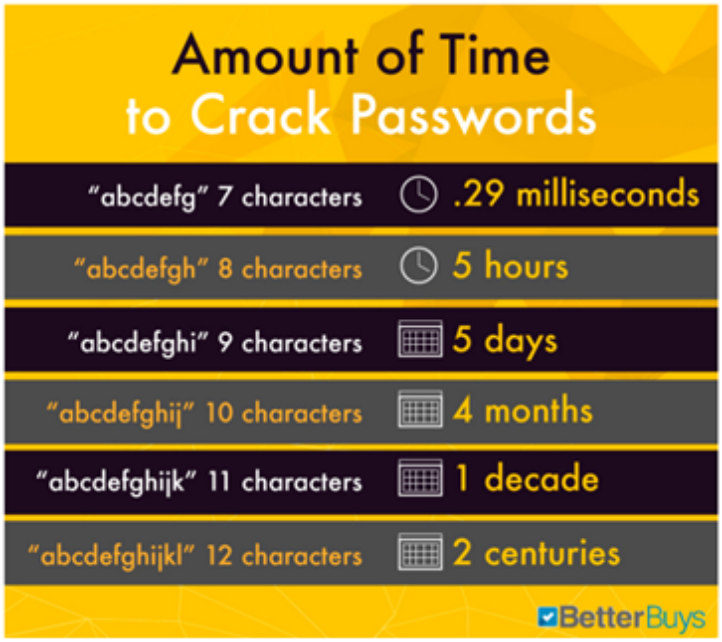
Passwords will be periodically audited to identify weak or compromised passwords. Any passwords that fails this audit will require an immediate change.

Periodic password changes will no longer be required. However, the administrators may force a change of any password if there is evidence of compromise.

Systems incapable of enforcing compliant passwords shall have user enforced compliant passwords. If compliant passwords are not permitted then other mitigating controls, determined on a case by case basis, shall be user enforced; e.g. shorter password lifetimes, longer passwords, or inactivity screen locks.

Additional Information

When it comes to passwords, one thing is certain: Size matters. Adding a single character to a password boosts its security exponentially. In a so-called “dictionary attack,” a password cracker will utilize a word list of common passwords to discern the right one. The list below shows the difference that adding characters can make when it comes to security.



Source: https://www.betterbuys.com/estimating-password-cracking-times/

Review (Frequency and Process)

This policy shall be reviewed annually by the Associate Vice President & CIO or a designate and provided to the Vice President Business and Administrative Services for approval and then to Cabinet for final approval.