INFORMATION SECURITY STANDARD

Passwords

Effective Date: 11/16/2020
Last Updated: New
Responsible University Officer:
VP Technology/CIO
Owner:
Chief Information Security Officer
Contact:
Todd Brown

RELATED POLICY: Information Security and Appropriate Use

Purpose

Passwords are the primary control for protecting university information systems from unauthorized access that could result in compromise of personal or institutional data, or disruption of critical services. Weak passwords that are easily guessed represent a serious security risk since they can be easily cracked by malicious persons desiring to gain access university systems. By the same token, constructing strong passwords provides a key defense against malicious users being able to guess or crack passwords.

University information security standards are intended to reflect the minimum level of care necessary to protect sensitive BYU information and IT resources from unauthorized access and misuse. Nevertheless, there may be may be other standards imposed by law, regulation, or contract the university must comply with.

Applicability

This standard applies to all university information systems containing non-public institutional information and extends to all university departments, employees, partners, consultants, and vendors. University information systems should be configured to only allow passwords that comply with these password rules.

For additional information or questions, contact the CES Security Operations Center.

Password Rules

Password rules are based on password length, i.e., the longer the password, the less need for complexity with mixed case letter, numbers, and symbols. Password rules are as follows:

Length	Required Characters
8-11	mixed case letters, numbers, & symbols
12-15	mixed case letters & numbers
16-19	mixed case letters
20+	no restrictions

Additional Requirements:

- It *must not* be equal to your current password, previous passwords, BYU Netid ID, or password reset answer
- It *must not* be a single word that appears in the dictionary (English or non-English)
- It *must* be composed only of characters in the Roman alphabet, numbers, or symbols on the US keyboard. Examples include characters such as # $ % ! @.

Tips for Creating Good Passwords or Pass Phrases

Consider using four or more unrelated words with mixed capitalization, separated by punctuation or spaces. If you have trouble remembering a longer password, write it down on a piece of paper, put the paper in your wallet, and use the same caution with it as you would with a credit card.

Using a Pass Phrase

A pass phrase is basically a series of words, including the use of spaces if desired, that can be used instead of a single pass "word." Pass phrases are easier to remember than complex passwords. Pass phrases should be at least 16 characters in length (spaces count as characters). Longer is better because, though pass phrases look simple, the increased length provides so many possible permutations that a standard password-cracking program will not be effective. Disguising simplicity by throwing in elements of weirdness, nonsense, or randomness, will help make it more secure. For example

pizza home cosmo spaniels
foggy tooth jazz pants

Adding punctuation and capitalization to your phrase and adding in a few numbers or symbols from the top row of the keyboard, plus using some deliberately misspelled words will create an almost unguessable password. For example

Pizza Home Cosmo Spaniels?
P1zza 4 Hom3 Cosmo Spaniels!

Foggy Tooth Jazz Pants!
Foggy Tooth J4zz P@nts?

Related Information

- How To Make a Strong Password
- Minimum Security Controls for IT Resources
- DUO Security