Setting Strong Passwords Fac/Staff

Date of Last Revision:	February 2019
Responsible Department:	Information Technology
Security Framework References:	NIST: PR.AC-1; PR.AC-2; PR.AC-3; PR.AC4; PR.AC-5; PR.AT-2; PR.AT-5 CSC: 5.1; 5.6; 5.7; 5.8; 5.9

A strong password is one that considers the following attributes:

- Length. GVSU systems allow for varying lengths for passwords. Your password should be a minimum of 12 or more characters in length when allowed.
- Combination of characters. Use numbers, letters, and symbols, where allowed. Some applications may not accept spaces at this time.
- Use words or phrases that are easy for you to remember, but difficult for others to guess.

Password Creation Do's:

- Minimum of 12 characters long.
- Is a series of words that create a phrase.
- Is significantly different from previous passphrases.
- Strong passwords and passphrases may contain characters from each of the following four categories: uppercase letters, lowercase letters, numbers and symbols.
- Protect passwords that are written down or electronically stored.

Password Creation Don'ts:

- Avoid names.
- Avoid birthdays.
- Avoid common phrases.
- Avoid using your user name, real name or company name.
- Avoid using the same password for all accounts.
- Do not give your password to anyone.
- Do not send passwords via email.
- Do not type passwords on computers you do not control. Public computers can be loaded with keystroke logging applications to capture what others have typed.

What do you do if your password is stolen:

1. Contact the Helpdesk immediately for all GVSU accounts
2. Change your password
3. Monitor your accounts if it is a home account

Example of strong passphrase:

What makes a passphrase stronger today is length. The longer the passphrase, the longer it takes hackers to crack it. Strong passphrases using multiple words put together are much stronger than the old philosophy of shorter, more complicate passwords using different character sets.

The previous password rules that were considered strong at one point were:

- Old example using uppercase, lowercase, numbers and special characters:
- Tr0ub4dor&3 - which can be cracked in 3 days by a computer and is hard to remember for the user

New example using passphrase or multiple words put together:

- New example using a longer passphrase:
- Correcthorsebatterystaple - which takes 553 years to crack by a computer but is easier for the user to remember
- Note: GVSU currently requires 3 out of the 4 characters sets to be used in the password creation. This will change in the near future. However, you can still take advantage of the passphrase method while using uppercase, lowercase, numbers and special characters.