SAINT MARY'S COLLEGE OF CALIFORNIA PASSWORD POLICY

Revision Approved May 2018

1.0 General

Shared accounts and passwords shall not be used. The issuance of a User password or other means of authenticated access to College systems is intended to ensure the appropriate security of College data. It does not guarantee complete privacy for users' personal information or sanction improper use of College equipment, facilities or data, and is intended to prevent unauthorized third party access to any account information. User should be aware that passwords or other means of authenticated access does not prevent Saint Mary's from viewing account content

2.0 Password Minimum Requirements

In order to protect the security of the College's systems and data, all Users are required to use strong passwords. Strong passwords are those which are at least sixteen characters long (passphrases are recommended for better security) and can contain a mix of both alphanumeric and non-alphanumeric characters (e.g. #, %, ^, &, etc.). Obvious or predictable words that can be guessed, like the names of people, places or commonly used words, or information that can be easily found out, like the name of a pet, or an address or birthday, should be avoided.

2.1 Password Maintenance

Password change is currently required of all Faculty and Staff Users, and for all organizational (fictitious) accounts, once every year for all systems. Students are encouraged to do the same, but are not required at this time. Any password used for access to Saint Mary's IT resources should be unique and not used for access to any other site or application.

3.0 Security

Passwords used for access to Saint Mary's IT resources should never be revealed to anyone (i.e. leaving a written password in plain sight). Appropriate measures must be taken by all Users to protect their Saint Mary's password. If a User suspects that his or her password has been revealed to an unauthorized person, the User should change it immediately. Violations of this provision may result in appropriate disciplinary action.

3.1 Exceptions

Passwords may be revealed under certain circumstances to:

- Law-enforcement agencies and courts requesting information under court orders and rules of evidence that require disclosure.
- Supervisors (Employees only)

4.0 Enforcement

This password policy may be enforced by automated systems that will not accept weak passwords or allow users to log in without changing their passwords if they have not done so within the stated time intervals.