Mary Immaculate College

Password Policy

Introduction

Username and passwords are utilized in Mary Immaculate College to facilitate access to College IT resources. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of MIC's entire network.

As such, all MIC students and employees including contractors, vendors and third parties with access to MIC 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

This policy applies to all College Staff, Students, or Third parties who are issued with usernames and passwords for any College IT System or device.

This policy applies to all system administrators who issue usernames and passwords.

This policy applies to all username and password pairs on all devices, systems and applications that are part of the College network that provide access to College owned information.

Policy

General

- A valid password must consist of at least 8 characters and must comply to 3 of the 4 complexity rules:
    1) Password contains English uppercase character(s) (A to Z)
    2) Password contains English lowercase character(s) (a to z)
    3) Password contains Numeral(s) (0 to 9)
    4) Password contains non alphabetic character(s) (i.e. # $ % !)
- Passwords maximum age is 120 days, and you will be prompted to change at this time.
- Password minimum age will be at least 1 day
- Password history maintains a history of the last 3 passwords.
- User accounts will be locked out after 5 consecutive failed login attempts.
- User accounts will be locked out for a period of 60 minutes.
- Passwords set for new and locked accounts may not be standard and must be changed on first use.
- User Accounts that are not logged on for a period of 120 days will be disabled pending further investigation.
- Passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorised user to responsibility for actions that the other party may take.

- Passwords must not be written down and left in a place where unauthorised persons might discover them.
- If an account or password is suspected to have been compromised, report the incident to the MIC Helpdesk immediately.
- Whenever an unauthorised party has compromised a system, the IT Department must immediately change every password on the involved system. Even suspicion of a compromise likewise requires that all passwords be changed immediately.
- All vendor-supplied default passwords e.g. default passwords supplied with routers, switches or software such as operating systems and databases must be changed before any computer or communications system is used.
- Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over communications system
- Change passwords at least once every four months on all applications.