

IMMACULATA UNIVERSITY PASSWORD POLICY

Effective Date:

Authority This Program was approved by the President of Immaculata University (hereinafter "IU").

Program Statement This IU Password Policy (the "Policy") defines standard methods for using passwords on IU information technology systems and applications.

Program Purpose The purpose of this Policy is to prevent damage and/or loss to Institutional Data, including Private Information, to prevent damage to IU Information Technology and to place IU in compliance with its legal obligations.

Section headings are:

1. PURPOSE
2. SCOPE
3. POLICY

I. PURPOSE

Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of IU's entire network. The purpose of having a password policy is to ensure a more consistent measure of security for IU's network and the information it contains. The implementation of this Policy will better safeguard the personal and confidential information of all individuals and organizations affiliated, associated, or employed by IU. Additionally, this Policy establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

II. SCOPE

The Policy applies to all persons accessing the IU network regardless of their capacity, role or function. Such persons include students, faculty, staff, third party contractors, visitors (guests), consultants and employees fulfilling temporary or part-time roles.

III. POLICY

All IU owned electronic devices must, if possible, have password protection enabled.

All passwords (e.g., email, web, voice mail, computer, PDA, BlackBerry, etc.) must be changed at least every semester.

Passwords must not be inserted into email messages or other forms of electronic communication and should not be shared with anyone, including via email or phone conversations.

Passwords should not be written down and stored in unsecure locations or stored electronically without encryption.

All passwords must be at least 8 characters long, contain at least 2 numbers or special characters, not be a word in the dictionary, and not be part of your name or user name. If the device or application does not permit a password to meet these criteria, the password should satisfy as many of these criteria as possible.