



Where leaders are made

Library & Information Services

Help Desk | phone 716-888-2299 | fax 716-888-2516 | email helpdesk@canisius.edu

Canisius College Password Policy

1 Overview

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 Canisius College's entire network. As such, all Canisius College students and employees (including contractors and vendors with access to Canisius College systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, the frequency of change, and the policy for resetting passwords.

3 Scope

The scope of this policy includes all personnel and students who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Canisius College facility, has access to the Canisius College network, or stores any non-public Canisius College information.

4 Policy

4.1 General

- All newly issued passwords will be strong passwords.
- Passwords must not be inserted into email messages or other forms of electronic communication.

4.2 Guidelines

All passwords must conform to the guidelines described below.

4.2.1 General Password Construction Guidelines

Passwords are used for various purposes at Canisius College. Some of the more common uses include: network authentication, electronic mail, Banner web access, and BlackBoard accounts. Everyone should be aware of how to select strong passwords that would be difficult to guess or crack, even by a computer.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.

Canisius College Password Policy

- The words "Canisius College", "buffalo", "mainst" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., @\$&"(),<>`=;=#
- Are at least eight characters in length.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be stored on-line. When you write your passwords down, keep them with other secure items such as with your credit cards. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

4.2.2 Password Protection Standards

All passwords are to be treated as sensitive, confidential Canisius College information. Here is a list of "don'ts":

- Do not use the same password for Canisius College accounts as for other non-Canisius College access (e.g., personal ISP account, option trading, benefits, etc.)
- Do not share Canisius College passwords with anyone, including administrative assistants or secretaries
- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to ITS and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by ITS or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4.2.3 Forgotten Passwords and Resets

- Only authorized, full time employees of the Canisius College may reset passwords. A log of authorized users will be kept by the Chair of the CIMS Security Steering Committee.
- A self service password reset program is available at <http://www.canisius.edu/passwordreset>.
- No passwords will be changed on behalf of a computer user without positive identification such as a Canisius College ID card. Other proof may be acceptable, but will always consist of a picture ID and proof of current employment, enrollment, or other authorized association at Canisius College.
- Facsimile transmission of identification is permissible, if it is followed with written confirmation of the password transaction mailed (campus or USPS) to the address of record.
- Reset passwords will follow the guidelines for strong passwords in section 4.2.1, above.
- If technically possible, the new password that is reset on behalf of a computer user will be set to expire upon first use by the user, who will then be prompted to choose a new password.

5 Additional policy items for Information Technology Services employees

In addition to the above, special rules apply to the practices of Information Technology.

5.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least an annual basis. The recommended change interval is every three months.
- All production system-level passwords must be part of the Information Technology Services (ITS) administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- Under no circumstances will the ITS person who changes a user password attempt to access any data and/or applications of that user beyond simple verification of the password reset. Violation of this provision will result in the most serious disciplinary consequences, up to termination of employment.

5.1.1 Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Canisius College Password Policy

5.1.2 Passphrases

Passphrases are generally used for public/private key authentication. Only those with access to Virtual Private Networks need to be concerned with this section. Virtual Private Networks are used for highly secure transactions over the public (e.g. ISP) network.

A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

6 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

7 Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

8 Revision History

November 23, 2004 Adopted by Presidents Cabinet

May 16, 2005 Revised to eliminate expiration of strong passwords

May 16, 2007 Minor updates; changed password reset URL.

Changing Your Novell, Griffmail and Banner Self Service Password

Your Canisius College password for several applications, including Novell, email, Banner Self Service, and network registration may be found at <http://www.canisius.edu/passwordreset> .

Additional documentation on changing passwords may be found at <http://www2.canisius.edu/its/documents.html>