Password Policy

End-User Policy Summary: Passwords are an important component of information security here at Canisius, and need to be handled carefully. Your passwords should have upper and lower case letters, as well as numbers and special characters. Treat your password with the same care that you would your ATM PIN or other important information. Do not share your password with anyone, or communicate it via email or telephone. If you forget your password, call the Help Desk. Accounts with special capabilities or privileges may have additional requirements and responsibilities.

1.0 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.

2.0 Scope
This policy applies to anyone who has been issued authentication credentials for an account 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. This includes both members of the Canisius community, such as faculty, staff, or students, as well as members of third party organizations granted access to College resources.

3.0 Policy
All newly generated or issued passwords will be strong passwords, as described in section 3.1 below.

3.1 Generating Passwords
All passwords should 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.

3.2 Protecting Passwords
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., Firefox, Thunderbird.)
• Don't 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 notified and required to change it.

3.3 Forgotten Passwords
In the event that a password is forgotten:

• 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 for end users 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.
• If the user cannot come to the Help Desk, then resets may be performed over the phone after alternate verification of the user's identity.
• Reset passwords will follow the guidelines for strong passwords in section 3.1 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.

3.4 Privileged Account Passwords
There are additional rules that apply to ITS personnel and vendors in the use of privileged accounts and in the initial configuration of network equipment.

• 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.

3.5 Application Development Standards
Application developers must ensure their programs contain the following security precautions.

• Applications should support authentication of individual users, not groups.
• Applications should not store passwords in clear text or in any easily reversible form.
• Applications 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.
• Applications should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

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