

Information Systems Password Policy

1. Overview and Purpose:

The purpose of this policy is to establish a standard for creation of strong passwords, for the protection of those passwords, and for the frequency of change of passwords. Passwords are a critical aspect of computer security. They are the first line of protection for user accounts. A poorly chosen password may result in a compromise of the entire Loyola University network. Therefore, all members of the Loyola University community are responsible for taking the appropriate steps to safeguarding computer systems by selecting and securing passwords as outlined in the following guidelines.

2. Scope

This policy applies to all faculty members, staff, administrators, students, alumni and any other person affiliated with the University who either (1) has an account, or any form of access that supports or requires a password, on any system that resides at any Loyola University, or (2) has access to the Loyola University network, or (3) stores any non-public Loyola University information in digital format.

3. Policy and Guidelines

3.1 General Guidelines

All user-level passwords (e.g., e-mail, desktop login, Blackboard, etc.) <u>must</u> be changed at least every six months. This simple guideline ensures that in the rare case that a password is revealed, the access vulnerability from the disclosure will have a limited lifespan (otherwise, unauthorized access could continue indefinitely if not detected). A user should not reuse old passwords. Furthermore, all users should choose strong passwords to avoid threats due to password guessing and password cracking.

3.2 Password Construction Guidelines

A strong password has the potential to prevent your computer, accounts, and the entire network from unauthorized access to the system and the information residing on the system. Strong passwords are difficult to guess and nearly impossible to crack using password cracking programs. Here are some characteristics of strong passwords, several of which are enforced by the systems when users are setting or changing account passwords:

The following are attributes of user passwords which are enforced by the systems:

- The password chosen is at least eight (8) characters long
- The password contains at least one number
- The password contains both upper and lower case characters (e.g., "Rv78#56A")

The following are desirable attributes of a password:

- The use of special digits (like these "!@#\$%^&*()_+|~-=\`{}[]:";'<>?,./") in addition to the use of letters and numbers is highly desirable.
- The password contains strings of characters that are not words in any language, including slang, dialect, jargon, etc. (partially enforced)
- The passwords are not based on personal information, names of family, etc.
- The password is easy to remember (because passwords should never be written down or stored on-line). One way to do this is create a password based on a song title or phrase that you can easily remember. (i.e., a strong password could be created and easily remembered based on the song title "This little light of mine" and the password could be "TILOmi9~")

Users should not use weak passwords. The following are some characteristics of weak passwords:

- 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
 - The words "loyola", "baltimore", "sellinger" or any derivation such as "loy12345" or "selli325"
 - Birthdays and other personal information such as addresses and phone numbers (e.g. "90271sbr" where the numbers represent the user's birthdate)
 - Word or number patterns like "aaabbb", "qwerty", "zyxwvuts", "123321", etc.
 - Any of the above examples spelled backwards (e.g. "ytrewq" password cracking programs easily check combinations and reversals of strings of characters)
 - Any of the above preceded or followed by a digit (e.g., "qwerty1" or "1ytrewq")

In order to decrease the likelihood that a previously compromised password is guessed after it is changed, it is an excellent policy to change the password enough as to avoid guessing. (e.g. Suppose that the password "TlL0mi9~" is compromised unbeknownst to

the user, and the user is prompted by the system to change the password after several months. A change to "TlL0mi9~1" may be easy to guess by someone who knows the original password. A change to "tLl0MI9!" would be harder to guess.)

Also, common sense goes a long way when choosing passwords. For example, while the above gives examples of strong passwords, do not use these examples as passwords (they are part of published guidelines about passwords and would be very easy to guess by anyone having access to this policy).

3.3 Password Protection Guidelines

Do not use the same password for Loyola University accounts as for other non-Loyola access accounts (e.g., your banking account password, other e-mail account passwords, Internet chat room passwords, etc.). Whenever possible, try not to use the same password for various Loyola University accounts. If single sign-on is available for a number of accounts allowing you to login to several systems simultaneously with a single username and password, consider the single sign-on to be a single account although you are accessing multiple systems. For example, select one password for single sign-on perhaps allowing you to access E-mail, Blackboard and Web Advisor systems and different passwords to access other systems such as Colleague.

Do not share your Loyola University passwords with anyone, including administrative assistants. All passwords are to be treated as sensitive.

When it comes to revealing and sharing passwords, here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE. (Hackers are notorious for creating emergency situations via phone to induce individuals to reveal passwords over the phone.)
- Don't reveal a password in an email message or Internet chat.
- Don't reveal a password to your supervisor.
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., it's "my family name" followed by...)
- Don't reveal a password on questionnaires or security forms, especially online as this is a common approach used in "fishing" attacks
- Don't share a password with family members
- Don't reveal a password to co-workers before going on vacation
- Don't type your password in plain view of potential "shoulder surfers" (sometimes the easiest way for a hacker to obtain a password is by looking over your shoulder as you type it, shielding the keyboard with your body and strong passwords requiring the use of the shift key make shoulder surfing much more difficult!)

If someone demands a password, refer them to this document or have them call someone at the Office of Technology Services (x5555).

Do not to use the "Remember Password" feature of applications (e.g., MS Internet Explorer, MS Outlook, etc...). Again, do not write passwords down and store them anywhere in your office. 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 Technology Services and change all passwords.

Note that many systems have a built in capability to require periodic password changes and to require strong password choices (including not allowing the choice of previous passwords as new passwords, or trivial changes to passwords). These system features are used to assist you in creating and maintaining strong passwords in order to protect you, your accounts, and the networks you are connected to from threats of unauthorized access and abuse. Also, Technology Services may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4. Enforcement

Individuals are responsible for ensuring that their passwords are in accordance with these guidelines. These policies and guidelines are intended to protect you and others who use Loyola University systems, the integrity of the systems, and the integrity and confidentiality of information stored in connected systems. Any member of the Loyola University community who is found in violation of these guidelines may lose access privileges.

5. Glossary of Terms Used in this Policy

Dictionary Attack -	A method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password.
Encryption -	An algorithm used to scramble data which makes it unreadable to everyone except the recipient. This is often used by e-commerce sites to secure credit card data. Secure

sites use encryption.

Hacker -	The term often refers to any programmer, but its true meaning is someone with a strong technical background who is "hacking away" at the bits and bytes.
Obfuscated Password -	a password that is intentionally made harder to guess
Password -	A secret series of characters that enables a user to access a file, computer, or program. The password helps ensure that unauthorized users do not access the computer.
Password Cracking -	Password cracking is the process of recovering secret passwords stored in a computer system. The purpose of password cracking might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk), to gain unauthorized access to a system, or as a preventive measure by the system administrator to check for easily crackable passwords.
Phishing -	The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Shoulder Surfer -	someone watching you type the password.
Special Characters -	Non-alphabetic or non-numeric character, such as @, #, \$, %, &, * and +.
Strong Password -	A password that is hard to detect both by humans and by the computer. Two things make a password stronger: (1) a larger number of characters, and (2) mixing numeric digits, upper and lower case letters and special characters.
Username -	A unique name used to gain access to a computer system. Usernames, and often passwords, are required in multi-user systems.
Weak Password -	A password that is easy to detect both by humans and by computer. People often use obvious passwords such as the names of their children or their house number in order not to forget them. However, the simpler the password, the easier it is to detect.