Password Standard

Policy Title:
Password Standard

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This standard covers the minimum password requirements for all electronic devices owned or leased by Loyola that can be protected by a password. In addition, please note that this policy covers all IoT devices. The purpose of the Password Standard is to ensure that all electronic devices are secured by a password of a certain complexity, and to ensure that more sensitive devices require more complicated passwords.

II. Definitions

Character Classes: There are four, character classes available. The four classes are numbers, lowercase letters, uppercase letters, and special characters. Special characters are those characters that can be typed on a computer that do not fall into one of the other three classes.

LSA: The acronym for Loyola Secure Access which is the branded term for the university Virtual Private Network service (VPN).

Student Worker: A student worker is an individual who is enrolled in at least one class at Loyola, is hired in a position that is not eligible for benefits and works in a temporary capacity. This includes hourly employees and temporary part time (TPT) workers. This does not include permanent part time (PPT) workers or full-time employees (FTE).

Exception Example: If a system treats uppercase and lowercase characters as the same, and does not accept special characters, it is impossible to create a privileged password using our standards. In this case, the password would have a length of eight characters (matching the standard) and would contain both characters and numbers (2 classes being as close to the standard of 3 as possible).

Mobile Device: a small computing device, typically small enough to be handheld (does not include laptops)

Multi-Factor Authentication (MFA): a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transactions typically using a PIN, a one-time password (OTP) sent to the requester's phone or email address, a digital certificate, a fingerprint, or hardware token.

III. Policy

Change to Password Length

Beginning July 1, 2021, the minimum length for all network passwords will be 12 characters with a maximum of 20 characters.

Change to Password Expiration

Beginning January 1, 2022, passwords for general use accounts will be set to never expire. ITS reserves the right to manually expire the password for an account that appears to be compromised and will notify the user should their password be expired. The reason for this is because of NIST password guidelines. NIST says that periodic password resets have become counter-productive, as users end up setting weaker passwords to help with remembering them. This compromises the security of an organization. The NIST recommends resetting passwords only when necessary.

Network Passwords

All network passwords will be a minimum of twelve characters long with a maximum length of 20 characters. All network passwords must contain at least one lower case letter and one upper case letter. Passwords must also be a combination of letters and numbers, letters and symbols or letters, numbers, and symbols. General use passwords do not expire unless there is an indicator of compromise. All other passwords are required to be changed per the requirements below. When a network password is changed, the new password used must not be any of the passwords used based on requirements below or within the previous 500 days.

Privileged Passwords

All passwords for accounts, which have additional privileges beyond a normal user must be at least twelve characters long and contain at least three of the character classes (see Definitions section below). All privileged passwords are required to be changed every 180 days. No privileged passwords can be based on a word that is found in a dictionary. When a privileged password is changed, it cannot be set to its previous value. Privileged passwords cannot be provided to student workers.

- Examples of privileged passwords include root, super user, and administrator passwords for servers, databases, infrastructure devices, and other systems.
- All passwords used to access resources in the High Security (PCI) environment are considered above this level and are thus held to even higher standards (see High Security Accounts section of this policy).
- Privileged passwords also include application accounts that provide rights beyond those of a typical user.
- If a user is unsure if a given account is privileged, they must assume that it is.

Non-network Passwords

All devices, which do not use the network to authenticate users, must follow the same password standards as listed under network passwords. Operating systems, which store password history, must store the previous 10 passwords. Operating systems, which do not store password history, must ensure that the new password is different from the previous password.

Mobile device Passcodes

Users of mobile devices used to access Loyola email or other Loyola resources must ensure that the mobile device locks automatically and has a strong passcode.

- Acceptable mobile passwords must consist of one of the following. Passwords or passcodes that do not meet these requirements cannot be used.
  - Alphanumeric Code (minimum 6 characters)
  - Numeric Code (minimum 4 digits)
  - Fingerprint Scanner
  - Facial Recognition
- Device must be set to automatically lock out access to the mobile device after ten incorrect passwords.
- Mobile devices that cannot be configured with a password will not be allowed to access Loyola email or Loyola resources.
- If a mobile device that does not meet these standards must be connected to Loyola email or other Loyola resources, the end user must consult with the University Information Security Office to discuss the situation.
- The Information Security team will advise the end user on the type of password that should be used.

Service Passwords

All passwords used to allow servers to communicate with one another in an automated fashion require stronger passwords as they are infrequently changed. They must be at least 20 characters long and contain at least two characters from each of the four-character classes. Service passwords cannot be provided to student workers. Service account passwords must be changed whenever the administrator responsible for the account leaves the organization or changes roles.

High Security Accounts

All passwords used on systems that store, transmit or process Loyola Protected Data, per the Data Classification Policy, Protected Health Information (ePHI), and Payment Card Data (PCI) will conform to the following password requirements in addition to the Privileged Password requirements:

- Avoid using dictionary words, people's names, usernames, special dates, or number sequences that can be easily guessed.
- The password will be changed every 90 days or if there is any suspicion the password could be compromised.
- New passwords may not be the same as the last four passwords.
- Accounts will be locked out for thirty minutes after six failed login attempts.

- First time passwords will be set to a unique value for each user. Passwords will be set to change immediately after first use.
- Authentication mechanisms are assigned to an individual account and not shared among multiple accounts.
- Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.

Multi-Factor Authentication (MFA)

Increasingly, passwords are the weak link in protecting information and accounts. In addition to following the Password Standard, adding another layer of protection to accounts with 2-step/multi-Factor authentication where available provides extra protection. This is an emerging requirement for accounts that provide access to restricted data and for privileged accounts and is **required for access to the High Security Network which is only accessible using LSA (VPN).**

Password Managers and Password Sharing

Passwords managers help generate unique and strong passwords, store them in one safe (encrypted) place, and use them while only needing to remember one master password. Loyola University Chicago prohibits sharing of personal passwords with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of the University Information Security Office and must have a primary responsible contact person. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those passwords, and that person will ensure that only appropriately authorized employees have access to the passwords. Internal sharing of administrative accounts must use the password manager provided by ITS.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	• Enforcing the Password Standard at the University by setting the password requirements
All users (Employees and contractors, Students, Visitors and/or Volunteers)	• Comply with the requirements of this policy • Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible

VI. Related Policies

Please see below for additional related policies:

- Data Classification Policy
- ITS Security Policy

Approval Authority:	ITESC	**Approval Date:**	March 28th, 2019
Review Authority:	Jim Pardonek	**Review Date:**	July 31st, 2025
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu