



Information Technology Services Standards

Title: Password Standards

Created: April 20, 2007

Author: J. Bazeley

Version: 1.0

Scope:

These standards cover the minimum password requirements for all electronic devices owned or leased by Loyola that can be protected by a password.

Purpose:

To ensure that all electronic devices are secured by a password of a certain complexity. And to ensure that more sensitive devices have more complicated passwords.

Standards:

Network passwords

All network passwords will be at least 8 characters long. All network passwords are required to contain at least 2 characters and at least 2 numbers. All network passwords are required to be changed every 180 days. When a network password is changed, it cannot be set to any of its previous 10 values.

Privileged passwords

All passwords for accounts which have additional privileges beyond a normal user must be at least 8 characters long and contain at least 3 character classes (definition in appendix). All privileged passwords are required to be changed every 180 days. All privileged passwords cannot 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, superuser, and administrator passwords for servers, databases, infrastructure devices and other systems. This also includes 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 than the previous password.

Mobile device passwords

All mobile devices used to access Loyola email or other Loyola resources must follow the same password standards as listed under network passwords. If the mobile device cannot be configured to confirm that the password meets those standards, then the user of the mobile device is responsible for choosing an appropriate password. Mobile devices must be configured to automatically erase themselves if an incorrect password is entered 10 times in a row.

Mobile devices that cannot be configured with a password and cannot be configured to automatically erase themselves after a certain number of failed password attempts cannot be used to access Loyola email or Loyola resources.

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 2 characters from each of the 4 character classes. Service passwords cannot be provided to student workers.

Non-compliance

If a mobile device that does not meet these standards is connected to Loyola email or other Loyola resources, the end user must consult with the Information Security team at DataSecurity@luc.edu to discuss the situation. The Information Security team will advise the end user on the type of password that should be used.

Exceptions:

Certain systems are unable to support the above listed requirements. In those cases, the password chosen must be as close to the appropriate standard as possible. Certain systems are unable to confirm that a password meets the appropriate standards. In those cases, the requirements associated with an appropriate password must be communicated to the end user. The end user is then responsible for choosing an appropriate password.

An administrator may apply to be exempt from the password standards. To do so, they must receive approval from the ITS director responsible for the application as well as the ITS director overseeing the Information Security team. This approval must detail why the application should not be subject to the standard, what password standards it will be subject to, and any additional controls that will help mitigate the risk. This password must be obtained in writing, and must be obtained every 12 months.

Appendix

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.

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 8 characters (matching the standard) and would contain both characters and numbers (2 classes being as close to the standard of 3 as possible).

Known systems that require exceptions

Blackberry mobile devices – Minimum length can be checked, password complexity cannot. Password requirements will be communicated to the end user.