Policy Title:	Password Policy
Document Reference #:	
Major Functional Area:	University Technology Services
Executive Sponsor:	Manny Rodriguez
Sponsoring Organization:	University Technology Services
Effective Date:	August 1, 2018
Revised Date:	January 8, 2020

Purpose

All computer accounts must be password protected to help maintain the confidentiality and integrity of electronic data as well as to help protect the University's computing resources and infrastructure. This policy establishes a minimum standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Audience

All Saint Leo University employees, consultants, contractors, and sub-contractors, have a personal responsibility to protect Saint Leo University's Applications and Data from intentional or accidental misuse and unauthorized disclosure.

Policy Exceptions

Exceptions to this policy must be formally documented and approved by the Vice President of Business Affairs.

Policy Violations

Violating this policy will result in disciplinary action, up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company reserves the right to report such activities to the applicable authorities.

Policy Information

Policy #	**Policy Statement**	**Reference**
General		
1.1	Passwords to University accounts and devices must be kept confidential. The Password Policy is reviewed on at least an annual basis to determine if policies and procedures are in place to maintain effective support of the IT operations of Saint Leo University.	N/A
1.2	To preserve account integrity, the owner of the account should be the only person with knowledge of the password.	N/A
1.3	Saint Leo personnel will not share a University account password with another individual; including but not limited to managers, co-workers, or University Technology Services personnel.	N/A
1.4	Notification of password expiration will be provided upon University system sign on attempt.	N/A

1.5	The support staff and system administrators must verify the identity of users when assigning or resetting passwords.	N/A
Password Requirements		
2.1	Passwords will expire every 90 days.	N/A
2.2	Password history will be archived up to 4 old passwords.	N/A
2.3	Passwords to systems containing sensitive information must be at least 8-12 characters in length.	N/A
2.4	Strong passwords should be used. A strong password will include a combination of: At least one upper case: A to Z At least one lower case: a to z At least one Numeric: 0 to 9 Spaces are not permitted May not contain part of the User Name Special Characters are optional and include: !, #, $, ^, _, %, -	N/A
2.5	Account lockout duration will occur after five invalid login attempts, and you must wait 30 minutes before you can login again.	N/A
2.6	Passwords should not consist solely of personal information or words found in a dictionary (any language). The use of at least three of the four types of strong password characters noted above as part of the password is required.	N/A
Illegal Activities		
3.1	If an account or password is suspected to have been compromised, report the incident to University Technology Services and immediately change all of the associated passwords.	https://helpdesk.saintleo.edu
3.2	In the event that someone request your password, refer them to this document or have them contact University Technology Services.	https://helpdesk.saintleo.edu

Contact Information

If you have any questions about this policy, you can contact us:

Saint Leo University
University Technology Services
Web: https://helpdesk.saintleo.edu
Phone: (352)588-8888