Policy Title:	Client Computer Security Policy
Document Reference #:	
Major Functional Area:	Business Affairs
Executive Sponsor:	Manny Rodriguez, CTO
Sponsoring Organization:	University Technology Services
Effective Date:	2/23/2016
Revised Date:	4/27/2020

Purpose

The purpose of the Client Computing Security Policy (CCSP) is to (a) help protect each user's device from harm, (b) to protect other users' devices from harm, and (c) to protect the Saint Leo University (SLU) data, network and its allied resources from misuse. The CCSP consists of four requirements, all of which must be met before using a device on SLU's network.

Audience

All members of the Saint Leo University Community full-time employees; part-time employees; contractors; etc. – 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

Section No.	Policy Statement	Reference
Standard		
1.1	The CCSP 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	Supported operating system and application software with current security patches will be installed.	N/A
1.3	The device must use firewall software if technically possible.	N/A
1.4	The device must be protected against malicious or undesired software such as viruses, spyware or adware and this protection must be kept up-to-date per industry standards.	N/A

1.5	The device must have a user name and password or other sign-on mechanism that helps prevent its use by unauthorized individuals.	N/A
1.6	Portable storage devices with University data must be encrypted.	N/A
1.7	Laptops that belong to the University and that contain institutional data must be encrypted with a University of Technology Services approved encryption software.	N/A
Compliance		
2.1	Passwords may not be shared with others and must be changed periodically not to exceed a 90 day cycle. All university owned/managed devices must meet or exceed the university password requirements including complexity and password life-cycle qualities as defined in the Password Policy.	N/A
2.2	Generic and "Guest" accounts are to be limited and must be disabled where appropriate. Any manufacturer delivered accounts must be deactivated when technically possible and those with well-known passwords must be changed.	N/A
2.3	In some cases, it may not be possible to bring a device into compliance. For example, older laboratory equipment and/or software may not operate with current operating systems or security patches. In these special cases, units must employ compensating controls to meet the requirements of this standard. Departments must document compensating controls and must retain this documentation for audit so long as the device is in operation.	N/A
2.4	Compliance with the policy can be accomplished using a variety of technological or practical tools.	N/A
2.5	Devices found not to be in compliance must be quarantined from SLU's network and the compliance issue must be addressed before it may be reconnected to SLU's network.	N/A
2.6	UTS reserves the right to install software on any University device, this can include security, productivity software, or software that is requested for business purposes. This software can and will be installed remotely when possible with proper notification to the user community. Interfering with the delivery of any software without approval, that device will be considered out of compliance and can be removed from the SLU network until the device is brought into compliance.	N/A
Roles of Departments, and IT Staff		
3.1	The user is responsible for compliance on personally owned devices.	N/A
3.2	Users granted responsibility for administration on university equipment would share responsibility for compliance with IT staff.	N/A
3.3	The UTS department is responsible for ensuring compliance with this policy.	N/A

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