STANDARD: WIRELESS COMMUNICATION

Contents

1 Purpose

This standard specifies the technical requirements related to wireless communications and infrastructure at St. Lawrence University. The majority of restrictions for wireless communications is related to sensitive and protected university information, which is defined in the University Data Classification Policy.

2 Scope

The Wireless network at St. Lawrence University comprises a subsection of the institution's network infrastructure. The scope of this standard includes infrastructure, user & endpoint access, and management related to these elements.

Wireless infrastructure devices include, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points and must be installed, supported, and maintained by St. Lawrence University Information Technology.

Wireless endpoints are devices that connect to and make use of the wireless infrastructure. Wireless endpoints include, but are not limited to desktop and laptop computers, mobile devices, and any other devices that is capable of connecting to a wireless network.

Users include any person who attempts to, or is able to connect and make use of the University's wireless communication infrastructure that include, but is not limited to all employees, students, contractors, consultants, and guests.

3 Standard

3.1 General Infrastructure:

The St. Lawrence University wireless communication infrastructure shall be centrally managed exclusively by the University Information Technology department.

The communication infrastructure and allows for the publishing of multiple authentication options through many of the single access points deployed across the campus and remote sites. These access points provide gateways to two different networks: Internal (includes Internet access) or Internet only.

3.2 Endpoint Connectivity and user access

3.2.1 Internal (+Internet):

3.2.1.1 "slu-wifi": Provides Direct access to internal university resources and the internet

- WPA2-AES: Use Wi-Fi Protected Access II with Advanced Encryption System protocols.
- Authentication: Clearpass

3.2.1.2 "eduroam" (with St. Lawrence University account): Provides direct access to internal university resources and the internet

- WPA2-AES: Use Wi-Fi Protected Access II with Advanced Encryption System protocols.
- Authentication: Clearpass

3.2.2 Internet Only

3.2.2.1 "guest": Provides access to the internet

- Authentication: Open

3.2.2.2 "slu-gamer": Provides access to the internet

- WPA-PSK-AES: Use Wi-Fi Protected Access with Advanced Encryption System protocols and a Pre-Shared Key.
- WPA2-PSK-AES: Use Wi-Fi Protected Access II with Advanced Encryption System protocols and a Pre-Shared Key.

3.2.2.3 "eduroam" (without St. Lawrence University account): provides access to the internet

- WPA2-AES: Use Wi-Fi Protected Access II with Advanced Encryption System protocols.
- Authentication: Clearpass

3.2.3 Remote Access Points

All Remote Access Point (RAP) devices that provide direct access to a St. Lawrence University network must be provided and managed by Information Technology and will meet the general requirements identified in 4.1.2.1.1

3.2.4 Rouge Access Points

Unauthorized/Rogue wireless access points are not allowed. See the Acceptable Use Policy, section "Acceptable Use of Computers"

3.3 Administration of Wireless Network

3.3.1 Remote access via encrypted communications

Access limited to select members of the IT Network and Server Group

3.3.2 Default configurations and accounts

All Vendor/default configurations will be removed.

All Vendor/default accounts will be removed or disabled.

3.3.3 Log Management

All SLU infrastructure that provide wireless network access will retain logs related to their health, functionality, and configuration for 30 days.

All SLU infrastructure that provide wireless network access will retail logs related to user authentication to the wireless network for 6 months.

All SLU infrastructure that provide wireless network access will deliver logs related to user authentication to the University enterprise log management system for information security risk analysis.

3.3.4 Wireless Testing

Device configuration reviews will occur annually to ensure that configuration are appropriate and compliant.

Penetration (Pen) tests will occur annually to ensure system integrity

4 Standard review

This document will be reviewed on an annual basis and the results will be documented in the Revision History below. St. Lawrence University reserves the right to update this standard as necessary and all changes will be presented to the Information Technology Committee (ITC) for review.

Requests for changes to this policy may be made through the IT HelpDesk and will be directed to the appropriate group for review and inclusion as appropriate.

5 Related Standards, Policies and Processes

- St. Lawrence University Wireless Communication Policy
- Acceptable Use Policy

6 Revision History

Version	Date	Author	Revisions/Reviews
1.01.00	2015-12-08	Sean Cunningham	Original
1.01.01	2015-12-18	Sean Cunningham	Edits
1.01.02	2015-12-21	Sean Cunningham	Phil edits
1.01.03	2016-02-03	Sean Cunningham	Standard review update based on ITC review.
1.01.04	2016-03-09	Sean Cunningham	Additional updates from ITC
1.01.04	2016-07-01	Sean Cunningham	Effective date

7 Approvals

VP for Library and Information Technology	Sponsor/Caretaker
Name	Name
Title	Title
Date	Date