Wireless Communications policy
Frequently Asked Questions
April 2016

To assist the St. Lawrence University community to better understand the Wireless Security Policy , the following FAQ document was developed by IT in collaboration with the Information Technology Committee (ITC). The University is required to have this policy to document the practices associated with making wireless data network available across the SLU campus.

Q. Why do we need to limit individual people from setting up WiFi access points?

A. Personal access points represent an institutional and individual security risk because they can be configured to bypass any authentication requirements. Additionally, individual access points can cause wireless interference with institutional access points and can disrupt wireless networking for those in the vicinity of a personal access point.

Q. I have a friend visiting campus, can he/she login to SLU-WiFi?

A. Visitors should use the "guest" wireless network because it does not require an institutional account to connect and provides access to the Internet and limits institutional network resources. Guests of campus who are visiting from another institution that is part of the eduroam network can connect to the "eduroam" wireless network with the username and password from their home institution. More information about eduroam can be found at https://www.eduroam.org.

Q. Why do we have multiple wireless network names available and which should I use?

A. Having multiple networks allows us to better align network access for different constituents or different device types. Each network supports different capabilities. Please see https://www.stlawu.edu/it/service/network-wireless/wireless for details on which wireless network you should use.

Q. What information is logged by the wireless system and why?

A. Authentication information (usernames that connect to the WiFi network along with time/date, and device identifier) is collected and retained for 6 months which is both an industry standard and also required to be part of the eduroam community. When necessary, network and computer information is used to troubleshoot network, account, or device problems as well as identify the source of potential malicious network activity in accordance with the privacy section of the technology Acceptable Use Policy found at https://www.stlawu.edu/it/acceptable-use-policy-aup.

Q. Who do I contact for questions regarding this policy?

A. Please contact the Information Technology Helpdesk at helpdesk@stlawu.edu or 315-229-5770 and they will put you in touch with the most appropriate person for whatever policy or technical question you may have.

POLICY:
WIRELESS COMMUNICATION

DOCUMENT #: POL-000X
EFFECTIVE: XX-XXX-2016
CARETAKER: VICE PRESIDENT FOR LIBRARIES AND INFORMATION TECHNOLOGY

1.0 PURPOSE

The purpose of this policy is to ensure the availability and security of the St. Lawrence University wireless communications infrastructure as well as the security and protection of information assets transmitted through this network.

2.0 SCOPE

All employees, students, contractors, consultants, and guests must adhere to this policy. This policy applies to all wireless infrastructure devices, such as wireless network access points, that connect to a University data network or reside on a St. Lawrence University location that provide wireless connectivity to endpoint devices.

3.0 POLICY

St. Lawrence University has established the following requirements for use of its wireless infrastructure based on ISO/IEC and NIST documented standards*.

3.1 GENERAL REQUIREMENTS

All wireless infrastructure devices at St. Lawrence University that connect to the University data network and/or provide access to information assets must comply with the following:

i. Abide by the standards for communication specified in the Wireless Communication Standard.
ii. Wireless infrastructure resources will be installed, supported, and maintained by St. Lawrence University Information Technology.
iii. Users and devices must not interfere with university wireless access deployments.

4.0 ENFORCEMENT

The institution may temporarily suspend or block access to any individual or device when it appears necessary to do so in order to protect the integrity, security, or functionality of the institution's **communications network.**

Violations of this policy may result in penalties and disciplinary action in accordance with the Student Handbook, Faculty Handbook and/or rules governing employment at St. Lawrence University.

5.0 EXCEPTIONS

Exceptions to the policy may be granted by the Vice President for Library and Information Technology, and/or his/her designee in accordance with the St. Lawrence University Wireless Communication Standard.

6.0 REFERENCES

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) – Joint Technical Committee 1 (JTC 1) / Standardization subcommittee 27 (SC27): IT Security Techniques
- National Institute of Standards and Technology (NIST) – Computer Security Resource Center
- St. Lawrence University Acceptable Use Policy
- St. Lawrence University Asset Inventory
- St. Lawrence University Data Classification Policy
- St. Lawrence University Wireless Communication Standard

STANDARD:
WIRELESS COMMUNICATION

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.

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.

STANDARD

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.

ENDPOINT CONNECTIVITY AND USER ACCESS

Internal (+Internet):

"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

"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

Internet Only

"guest": Provides access to the internet

- Authentication: Open

"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.

"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

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

Rouge Access Points

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

ADMINISTRATION OF WIRELESS NETWORK

Remote access via encrypted communications

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

Default configurations and accounts

All Vendor/default configurations will be removed.

All Vendor/default accounts will be removed or disabled.

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.

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

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.

RELATED STANDARDS, POLICIES AND PROCESSES

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