Mobile Device policy
Frequently Asked Questions
April 2016

In an attempt to help the St. Lawrence University community understand this policy, the following FAQ document was developed by IT in collaboration with the Information Technology Committee (ITC). This policy is required for SLU to inform and protect individuals and the institution since the growth in use of mobile technology is so significant. The requirements of the policy are in line with general best practices for mobile technology. Even though many members of the SLU community will not fall under the scope of the policy, because of how they do and do not use this technology, we encourage everyone to properly protect their information stored and accessed on smartphones and tablets.

Q. Do I have to comply with this policy?

A. If you need or choose to access or store St. Lawrence University sensitive or protected information on a smartphone or tablet device, that device must comply with this policy. Protected information is that which is outlined in numerous government and industry regulations such as FERPA (Family Educational Rights and Privacy Act), GLBA (Gramm-Leach-Bliley Act), and PCI DSS (Payment Card Industry Data Security Standard). Sensitive information is that which can cause institutional or individual harm but isn't formally protected by law. Common examples of St. Lawrence University protected or sensitive information could include the following: bank information, credit card numbers, social security numbers, and student grades.

Q. How do I enable what is needed (mobile wipe, encryption, etc..) for different operating systems?

A. The technical aspects of this policy are all capabilities native to the major operating systems used on smartphones and tablets today. If you configure your smartphone or tablet to connect to SLU email then remote wipe and passcode security features are already automatically enabled. Please visit the website for your device's operating system or contact the IT Helpdesk at helpdesk@stlawu.edu or 315-229-5770 for assistance.

Q. Could these configuration settings affect any personal content on my device?

A. Generally settings like this apply across the device and all data stored on it. So if you ever have to "remote wipe" the device then any information stored on it is removed including apps, contacts, photos, non SLU email, etc. Making sure to have a data backup mechanism for your device is always wise even if you do not have SLU sensitive or protected data on it.

Q. If I have a St. Lawrence University provided tablet have these settings been configured already?

A. Not necessarily. You are responsible for ensuring your device complies with this policy if you access or store St. Lawrence University sensitive or protected information on that device.

Q. If my device falls within the policy and I get a new phone or tablet, what should I do to make sure the previous phone is cleaned of data?

A. You must wipe or factory reset the device before you trade-in, sell, or give away. You can find out how to do this at the website of your device manufacturer or contact the IT Helpdesk at helpdesk@stlawu.edu or 315-229-5770.

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:
MOBILE DEVICES

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 secure and protect St. Lawrence University information assets that may be accessed and stored on mobile devices. Mobile devices offer great flexibility and improved productivity for employees, but they can also create added risk and potential targets for data loss. This document describes St. Lawrence University's requirements for securing the institution's information on mobile devices.

2.0 SCOPE

All employees, students, contractors and consultants must adhere to this policy. This policy applies to all university owned and personal mobile devices with access to St. Lawrence University's information assets classified as sensitive or protected. St. Lawrence University considers mobile devices to be smart phones, tablets, or other types of highly mobile devices. Laptops are specifically excluded from the scope due to significant differences in security control options.

3.0 POLICY

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

3.1 USER AND TECHNICAL REQUIREMENTS

Individuals and their devices accessing St. Lawrence University's information assets classified as sensitive or protected are subject to the St. Lawrence University Mobile Device Standard.

The user is responsible for the backup of their own personal data and St. Lawrence University is not responsible for the loss of data.

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 institution and computer resources.

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 Mobile Device Standard.

6.0 REFERENCES

- St. Lawrence University Mobile Device Standard
- 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 Data Classification Quick Reference Guide

STANDARD:
MOBILE DEVICES

PURPOSE

This standard specifies the technical requirements related to mobile devices that utilize the infrastructure and access Sensitive or Protected St. Lawrence University data.

SCOPE

St. Lawrence University considers mobile devices to be smart phones, tablets, or other types of highly mobile devices. Laptops are specifically excluded from the scope due to significant differences in security control options. There are two general types of mobile device categories that will impact the applicability of the Standard – University owned and BYOD (Bring Your Own Device)/personal devices.

Users include any mobile device that is able to connect and make use of the University's sensitive or protected information assets that include, but is not limited to all employees, faculty members, students, contractors, consultants, and approved guests.

STANDARD

LOST OR STOLEN DEVICES

Contact the IT Help Desk (315.229.5770) and University Safety & Security (315.229.5555) if a device is lost or stolen.

ADMINISTRATION OF MOBILE DEVICES

Users of BYOD and university owned devices are responsible for the administration of the devices that they utilize.

The IT department will implement the ability to manage university owned devices as the technology is developed and deployed in our institutional infrastructure.

REMOTE DEVICE WIPE

Users of BYOD and university owned devices are responsible for ensuring that remote wipe of their device is enabled.

Remote wipe of specific university protected and sensitive information will be deployed as the technology becomes available.

"JAILBROKEN", "ROOTED", ETC. DEVICES

Devices that have been modified to bypass security, sideload applications, and/or provide privileged control are prohibited.

DEVICE ACCESS SECURITY

All devices must enable security measures (PIN, passcode, Biometrics, etc.) that protected the device from unauthorized used.

ENCRYPTION

All protected and sensitive data assets accessed on the mobile device must be encrypted. Refer to the St. Lawrence University Data Classification Policy.

VULNERABILITY MANAGEMENT

Mobile devices must be maintained with the most recent versions of operating system and software/apps as available from carriers, manufacturers, or software vendors.

IT will deploy patches and updates to University owned devices as the technology is developed and deployed in our infrastructure.

COMPLIANCE WITH STATE AND FEDERAL LAWS

Employees who use mobile devices to conduct University business must comply with all State and Federal laws related to those devices.

CAMERA-ENABLED DEVICES

Capturing, recording, or transmitting images on a mobile device that may contain sensitive or protected university data is prohibited.

OWNERSHIP OF UNIVERSITY PROVIDED MOBILE DEVICES

University provided mobile devices are institutional assets and are intended for business use.

All institution-provided mobile devices and associated telephone numbers are the property of St. Lawrence University.

Personal use of university provided mobile devices is not encouraged and use is restricted to the assigned employee with approval from their supervisor. Expenses associated with personal use are the responsibility of the assigned employee.

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 Mobile Device Policy
- St. Lawrence University Acceptable Use Policy
- St. Lawrence University Data Classification Policy