INFORMATION TECHNOLOGY
ST. LAWRENCE UNIVERSITY

POLICY:
INFORMATION SECURITY POLICY

EFFECTIVE: 03-2016

CONTENTS

1.0 Introduction 3
2.0 Purpose 3
3.0 Scope 3
4.0 Implementation 4
5.0 Roles and Responsibilities 4
6.0 Information and System Classification 5
7.0 Provisions for Information Security Standards 5
- 7.1 Access Control (AC) 5
- 7.2 Awareness and Training (AT) 6
- 7.3 Audit and Accountability (AU) 6
- 7.4 Assessment and Authorization (CA) 6
- 7.5 Configuration Management (CM) 6
- 7.6 Contingency Planning (CP) 7
- 7.7 Identification and Authentication (IA) 7
- 7.8 Incident Response (IR) 7
- 7.9 Maintenance (MA) 7
- 7.10 Media Protection (MP) 7
- 7.11 Physical and Environmental Protection (PE) 8
- 7.12 Planning (PL) 8
- 7.13 Personnel Security (PS) 8
- 7.14 Risk Assessment (RA) 8

7.15 System and Services Acquisition (SA) 8
7.16 System and Communications Protection (SC) 9
7.17 System and Information Integrity (SI) 9
7.18 Program management (PM) 9
8.0 Enforcement 9
9.0 Privacy 10
10.0 Exceptions 10
11.0 Disclaimer 10
12.0 References 10
13.0 Related Policies 11
14.0 Policy Authority 11
15.0 Revision History 12
16.0 Approvals 12

1.0 INTRODUCTION

The purpose of this Policy is to assist the University in its efforts to fulfill its responsibilities relating to the protection of information assets, and comply with regulatory and contractual requirements involving information security and privacy. This Policy framework consists of eighteen (18) separate Policy statements, with supporting Standards documents, based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-53.

Although no set of policies can address every possible scenario, this framework, taken as a whole, provides a comprehensive governance structure that addresses key controls in all known areas needed to provide for the confidentiality, integrity and availability of the institution's information assets. This framework also provides administrators guidance necessary for making prioritized decisions, as well as justification for implementing organizational change.

2.0 PURPOSE

The purpose of this Information Security Policy is to clearly establish the University's role in protecting its information assets, and communicate minimum expectations for meeting these requirements. Fulfilling these objectives enables St. Lawrence University to implement a comprehensive system-wide Information Security Program (See "*New York Six Information System Management System (ISMS) guidelines*" document).

3.0 SCOPE

The scope of this policy includes all information assets governed by the University. All personnel and service providers who have access to or utilize information assets of the Institution, including data at rest, in transit or in process shall be subject to these requirements. This Policy applies to all information assets operated by the University; All information assets provided by University through contracts, subject to the provisions and restrictions of the contracts; and all authenticated users of St. Lawrence University information assets.

All third parties with access to the Institutions' non-public information must operate in accordance with a service provider contract containing security provisions consistent with the requirements promulgated under, but not limited to the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), New York State Information Security Breach and Notification Act, and the Payment Card Industry Data Security Standard (PCI-DSS).

4.0 IMPLEMENTATION

St. Lawrence University needs to protect the availability, integrity and confidentiality of data while providing information resources to fulfill our academic mission. The Information Security Program must be risk-based. Implementation decisions must be made based on addressing the highest risk first.

The University's administration recognizes that fully implementing all controls within the NIST Standards is not possible due to organizational limitations and resource constraints. Administration must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practicable.

5.0 ROLES AND RESPONSIBILITIES

The university has identified the following roles and responsibilities:

1) University President: The President is accountable for the implementation of the Information Security Program including:

   a) Security Policies, Standards, and procedures

   b) Security Compliance including managerial, administrative and technical controls.

   The President is to be informed of Information security implementations and ongoing development of the Information Security Program design

2) University Senior Staff: The group is responsible for the oversight and compliance functions of the Information Security Program for St. Lawrence University. The group consists of individuals who report directly to the University President who have specific operational responsibilities.

3) Information Security Committee: The group is responsible for the design, implementation, and operations functions of the Information Security Program for all St. Lawrence University constituent units as identified in the Information Security Committee charter. The committee reports to University Senior Staff and their charter is defined in the Information Security Committee Charter.

4) Information Security Officer: This role is responsible for the development, implementation and maintenance of a comprehensive Information Security Program for the St. Lawrence University. This includes security policies, standards and procedures which reflect best practices in information security. (See *"St. Lawrence Policy – Information Security Policy – Appendix"* for details regarding the ISO role)

6.0 INFORMATION AND SYSTEM CLASSIFICATION

St. Lawrence University must establish and maintain security categories for both information and information systems. For more information, reference the Data Classification Policy.

7.0 PROVISIONS FOR INFORMATION SECURITY STANDARDS

The Information Security Program is framed on National Institute of Standards and Technology (NIST) and controls implemented based on SANS Critical Security Controls priorities. St. Lawrence University must develop appropriate control standards and procedures required to support the University's Information Security Policy. This policy is further defined by control standards, procedures, control metrics and control tests to assure functional verification.

The Information Security Program is based on NIST Special Publication 800-53; this publication is structured into 18 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements, including but not limited to the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), New York State Information Security Breach and Notification Act, and the Payment Card Industry Data Security Standard (PCI-DSS).

7.1 ACCESS CONTROL (AC)

The University must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

7.2 AWARENESS AND TRAINING (AT)

The University must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of University information systems; and (ii) ensure that University personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

7.3 AUDIT AND ACCOUNTABILITY (AU)

The University must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

7.4 ASSESSMENT AND AUTHORIZATION (CA)

The University must: (i) periodically assess the security controls in University information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in University information systems; (iii) authorize the operation of the University's information systems and any associated information system connections; And (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

7.5 CONFIGURATION MANAGEMENT (CM)

The University must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

7.6 CONTINGENCY PLANNING (CP)

The University must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the University's information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

7.7 IDENTIFICATION AND AUTHENTICATION (IA)

The University must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to St. Lawrence University information systems.

7.8 INCIDENT RESPONSE (IR)

The University must: (i) establish an operational incident handling capability for University information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate University officials and/or authorities.

7.9 MAINTENANCE (MA)

The University must: (i) perform periodic and timely maintenance on University information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

7.10 MEDIA PROTECTION (MP)

The University must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) encryption, where applicable, (iiii) sanitize or destroy information system media before disposal or release for reuse.

7.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

The University must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems;

(iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

7.12 PLANNING (PL)

The University must develop, document, periodically update, and implement security plans for University information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

7.13 PERSONNEL SECURITY (PS)

The University must: (i) ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions; (ii) ensure that University information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with information security policies and procedures.

7.14 RISK ASSESSMENT (RA)

The University must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

7.15 SYSTEM AND SERVICES ACQUISITION (SA)

The University must: (i) allocate sufficient resources to adequately protect University information systems; (ii) employ system development life cycle processes that

incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third- party providers employ adequate security measures, through federal and New York state law and contract, to protect information, applications, and/or services outsourced from the organization.

7.16 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

The University must: (i) monitor, control, and protect University communications (i.e., information transmitted or received by University information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within University information systems.

7.17 SYSTEM AND INFORMATION INTEGRITY (SI)

The University must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within University information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

7.18 PROGRAM MANAGEMENT (PM)

The University must implement security controls to provide a foundation for the organizational information security program.

8.0 ENFORCEMENT

The University 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.

9.0 PRIVACY

The University will make every reasonable effort to respect a user's privacy. However, faculty, staff and students do not acquire a right of privacy for communications transmitted or stored on University resources.

In addition, in response to a judicial order or any other action required by law or permitted by official University policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the University and the University community, the President may authorize the Vice President for Library and Information Technology, or an authorized agent, to access, review, monitor and/or disclose computer files associated with an individual's account.

10.0 EXCEPTIONS

Exceptions to the policy may be granted by the Information Security Committee. All exceptions must be documented properly and reviewed no less than annually.

11.0 DISCLAIMER

St. Lawrence University disclaims any responsibility for and does not warrant information and materials residing on non- St. Lawrence University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of St. Lawrence University, its faculty, staff or students.

12.0 REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- New York State Information Security Breach and Notification Act (*Section 208 of the State Technology Law and Section 899-aa of the General Business Law*)
- NIST 800-53,
- FIPS-199
- PCI DSS 3.1

13.0 RELATED POLICIES

- St. Lawrence Charter - Information Security Committee
- St. Lawrence Policy - Data Classification, Procedure and Quick Reference Guide
- St. Lawrence University Acceptable Use Policy
- New York Six Information System Management System (ISMS) guidelines
-

14.0 POLICY AUTHORITY

This policy is issued by the University President for St. Lawrence University.

15.0 REVISION HISTORY

Version	Date	Author	Revisions
D1.0		GreyCastle Security	Initial Draft
D1.01	3/31/2016	GreCastle Security	Changes requested by SLU
D05	4/11/2016	Sean Cunningham	Updates
D05.01	7/14/2016	Sean Cunningham	Updates – ISC
D05.02	10/31/2016	Sean Cunningham	Updates – JS review
1.0	03/31/2017	Sean Cunningham	Approved version

16.0 APPROVALS

University President	Vice President for Libraries and Information Technologies
Name William Fox	Name Justin Sipher
Date	Date
Signature	Signature