INFORMATION SECURITY STANDARDS FRAMEWORK

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) 6

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) 7

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) 8

7.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE) 8

7.12 PLANNING (PL) 8

7.13 PERSONNEL SECURITY (PS) 8

7.14 RISK ASSESSMENT (RA) 9

7.15 SYSTEM AND SERVICES ACQUISITION (SA) 9

7.16 System and Communications Protection (SC) 9

7.17 System and Information Integrity (SI) 9

7.18 Program management (PM) 10

8.0 Enforcement 10

9.0 Privacy 10

10.0 Exceptions 10

11.0 Disclaimer 10

12.0 References 10

13.0 Revision History 11

14.0 Approvals 11

1.0 Introduction

An Information Security Framework assists in the protection of information assets. This framework consists of eighteen (18) separate statements, with supporting Standards documents, based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-53 r4.

Although no set of standards can address every possible scenario, this framework, taken as a whole, provides a comprehensive 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 Framework is to clearly establish Hamilton College's role in protecting its information assets, and communicate minimum expectations for meeting these requirements. Fulfilling these objectives enables Hamilton College to implement a comprehensive system-wide Information Security Program.

3.0 Scope

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

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

Hamilton College recognizes that fully implementing all controls within the NIST Standards is not possible due to institutional limitations and resource constraints. The College must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practicable.

5.0 Roles and Responsibilities

Hamilton College has identified the following roles and responsibilities:

1) **Hamilton College President:** The President is ultimately accountable for the implementation of the Information Security Program. Executive oversight of the information security program is delegated to the VP for Libraries and Information Technology, including security policies, standards, and procedures; security compliance including managerial, administrative and technical controls.

2) **Hamilton College Senior Staff**: The senior staff consists of the heads of the divisions of the college, each of whom reports to the President. The senior staff generally meets weekly and is advisory to the President on matters of strategic direction and institutional policy. The Senior Staff recommends institutional policy to the president who approves these recommendations on behalf of, and in consultation with, the Board of Trustees. The Senior Staff is to be informed of Information security implementations and ongoing development of the information security program design.

3) **Information Security Board of Review (ISBR)**: The ISBR advises the VP for Libraries and IT on ways to protect the security of confidential and sensitive information through the efforts of the Information Security Program. The ISBR oversees the development, implementation, and maintenance of a college-wide information security plan and related policies and procedures and recommends policies for approval to the Senior Staff. The ISBR includes representatives from all major administrative offices and the faculty.

4) **Advisory Group for Information Security (AGIS):** The Advisory Group for

Information Security (AGIS) is responsible for the drafting of information security policies, procedures, standards and guidelines and overseeing the implementation of the approved policies, procedures, standards and guidelines. AGIS is responsible for communicating the information security program to the Hamilton community and is accountable for the maintenance of Information Security Program documentation.

AGIS includes information security subject matter experts from on campus and reports monthly AGIS efforts to the ISBR. The AGIS has a chaired position nominated annually to detail AGIS efforts and present policies for approval to the ISBR. A backup chair will also attend ISBR meetings in the event the AGIS Chair is unavailable.

AGIS works closely with existing Hamilton committees and department leaders while drafting Information Security policies and practices. This collaboration leads to the effective development and implementation of Information Security efforts serving to minimize the college's exposed risk.

5) **GreyCastle Security:** GreyCastle Security, through a contractual arrangement with Hamilton College and the other NY 6 colleges, performs as the Chief Security Officer for Hamilton College. GreyCastle is responsible for the development, implementation and maintenance of a comprehensive Information Security Program for Hamilton College. This includes security policies, standards and procedures which reflect best practices in information security.

6.0 Information and System Classification

Hamilton College establishes and maintains security categories for both information and information systems.

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. Hamilton College must develop appropriate control standards and procedures required to support the Information Security Policy Framework. This framework 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 revision 4; 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)

Hamilton College 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)

Hamilton College 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 Hamilton College information systems; and (ii) ensure that Hamilton College personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

7.3 Audit and Accountability (AU)

Hamilton College 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)

Hamilton College must: (i) periodically assess the security controls in Hamilton College 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 Hamilton College information

systems; (iii) authorize the operation of Hamilton College'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)

Hamilton College 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)

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

7.7 Identification and Authentication (IA)

Hamilton College 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 Hamilton College information systems.

7.8 Incident Response (IR)

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

7.9 Maintenance (MA)

Hamilton College must: (i) perform periodic and timely maintenance on Hamilton

College 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)

Hamilton College 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, (iv) sanitize or destroy information system media before disposal or release for reuse.

7.11 Physical and Environmental Protection (PE)

Hamilton College 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)

Hamilton College must develop, document, periodically update, and implement security plans for Hamilton College 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)

Hamilton College must: (i) ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions; (ii) ensure that Hamilton College 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)

Hamilton College 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)

Hamilton College must: (i) allocate sufficient resources to adequately protect Hamilton College 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)

Hamilton College must: (i) monitor, control, and protect Hamilton College communications (i.e., information transmitted or received by Hamilton College 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 Hamilton College information systems.

7.17 System and Information Integrity (SI)

Hamilton College 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 Hamilton College information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

7.18 Program management (PM)

Hamilton College must implement security controls to provide a foundation for the organizational information security program.

8.0 Enforcement

Hamilton College 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 Framework, or the specific policies that go with it, may result in penalties and disciplinary action in accordance with the Student Handbook, Faculty Handbook and/or rules governing employment at Hamilton College.

9.0 Privacy

Hamilton College will make every reasonable effort to respect a user's privacy as indicated in the Appropriate Use of Information Technology Resources Policy (https://www.hamilton.edu/offices/lits/rc/policies-responsible-use-of-networks-and-computer-facilities).

10.0 Exceptions

Exceptions to these standards may be recommended by the AGIS and approved by the VP for Libraries and IT. All exceptions must be documented properly and reviewed no less than annually.

11.0 Disclaimer

Hamilton College disclaims any responsibility for and does not warrant information and materials residing on non-Hamilton College systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of Hamilton College, 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
- NIST 800-53 r4,
- FIPS-199
- PCI DSS 3.1

13.0 Revision History

Version	Date	Author	Revisions
1.0		GreyCastle Security	Initial Draft
1.01	3/31/2016	GreCastle Security	Changes requested by SLU
1.05	06/17/2016	Dave Smallen	Updates
1.06	02/28/2017	AGIS	Updates

14.0 Approvals

Executive	Campus Security Officer
Name	Name
Title	Title
Date	Date
Signature	Signature