These guidelines describe how Hamilton College approaches the development, measurement and management of information security.

Version 3.03

1. Introduction

1.1 Overview

Information is a key resource for all enterprises, and from the time that information is created to the moment that it is destroyed, information security plays a significant role in assuring the confidentiality, integrity and availability of these resources.

Today, organizations use information to increase efficiencies, reduce costs and generate competitive advantages. Information is instrumental in diagnosing illness, understanding financial markets and stabilizing geo-political relationships. Information is at the core of our critical infrastructure, commerce, banking, entertainment and nearly every other system on Earth. Yet the relationship between information and security is not well understood.

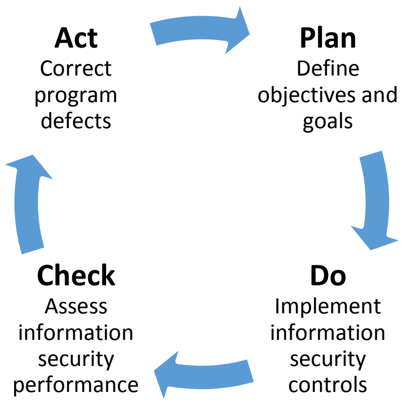
As a result, today, more than ever, enterprises and their executives strive to:

1. Generate value from information security investments,
2. Reduce information security risks to an acceptable level,
3. Optimize the costs of information security initiatives, and
4. Comply with ever-increasing regulatory and legal mandates.

Together, these activities comprise the governance activities referred to as an Information Security Management System (ISMS). This document describes the ISMS for Hamilton College.

1.2 The Information Security Management System

Utilizing the familiar Plan > Do > Check > Act process, the ISMS will help ensure that Hamilton College considers the many non-technical aspects of information security, all of which are critical to its success.


Act
Correct program defects
Plan
Define objectives and goals
Check
Assess information security performance
Do
Implement information security controls

Successful organizations deploy security controls to reduce risk for information assets, as defined by specific goals. Achieving these goals requires that organizations:

1. Align information security initiatives with business strategy,
2. Assign ownership and accountability for information security initiatives,
3. Identify critical information assets and assess risks to these assets.
4. Monitor the status and efficacy of information security initiatives, and
5. Institute a process of continuous assessment and improvement.

1.3 Scope

The ISMS defines the Information Security Strategy, roles and responsibilities, policies, Risk Management processes and Information Security Road Map for Hamilton College.

2. Strategy

2.1 Overview

The result of an effective Information Security Strategy is a program where risks and resources are in balance. To reach this equilibrium, Information Security Strategy must incorporate all of the elements that will ultimately define its implementation, set its direction or drive its priorities.

In many cases, Information Security Strategy is influenced by factors outside of the Information Security team. In fact, in many ways the Information Security team is a service provider, where Hamilton College sets security objectives, thresholds and tolerances and the Security team is implementing controls necessary to meet the requirements. The ISMS ensures that this relationship between information security and the business objectives of the Hamilton College exists, and is effective.

2.2 Business Alignment

Information security exists for one reason: to support the business strategy by appropriately protecting the information assets of the Institution. To do this effectively, the ISMS must consider the organization's business strategy. Rather than implementing security for security's sake, the goals of information security should directly or indirectly support those of the Institution.

This initiative will consider the following business initiatives as information security drivers:

1. Enabling world-class instruction and education at Hamilton College;
2. Protecting the reputation Hamilton College; and
3. Reducing institutional risk through the safe and secure handling of student, alumni, employee and other sensitive data.

2.3 Standards Implementation

Information security, like most areas of technology, has become a sophisticated web of technologies, processes, metrics and paradigms. Identifying, architecting, implementing and assessing security controls from scratch would be both a monumental undertaking and an inefficient use of resources.

First, we know from experience that many information security "wheels" have already been invented. We can save resources by not repeating this task. Second, we recognize that the organization is expected to operate under specific regulatory and legal mandates which makes inventing a "better mousetrap" unwise. Third and last, our goal from a security perspective is to reduce risk to *an acceptable level*, not eliminate all risk.

To accomplish this, Hamilton College has developed appropriate control standards, herein referred to as Information Security Standards, to support the Institution's Information Security policies. These standards are based on NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" which is implemented using the SANS Critical Security Controls priorities. The Information Security Standards define the

Hamilton College directives for safeguarding information and ensuring compliance with applicable laws, regulations, and commercial standards. Appropriate procedures have been documented that describe the tools, processes, and resources used to implement the Information Security Standards. The Hamilton College Information Security Standards are structured into eighteen (18) control groups (see Information Security Standards Framework).

Wherever appropriate, information security controls will comply with, reference and implement the above standards. This position will be stated and reinforced in the Security policy.

2.4 Regulatory and Security Best Practice Compliance

Hamilton College is subject to various regulations and mandates. Along with the minimum controls for information security put forth by various commercial mandates, Hamilton College is subject to other State and Federal regulations. Hamilton College has mapped the following security best practices and regulations to the Hamilton College Information Security Standards:

1. ISO 27002:2013 – The ISO 27002 standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the Institution's overall business risks. It specifies requirements for the implementation of security controls, customized to the needs of individual Institution, or parts thereof.
2. Payment Card Industry Data Security Standards (PCI DSS) v3.1 - Contractual obligations addressing the administrative, technical and physical standards required by payment brands (Visa, AMEX, MasterCard, Discover) for organizations processing payment card transactions.
3. Gramm-Leach-Bliley Act (GLB Act or GLBA) - Federal law enacted in 1999 which requires organizations that loan money to take measures to protect the financial information of individuals.
4. Family Educational Rights and Privacy Act (FERPA) - Federal law enacted in 1974 requiring any school receiving federal funds to protect the privacy of educational records.

It is the goal and intent of the ISMS to ensure compliance with all known regulations and mandates as they are understood, and to make them an appropriate priority.

2.5 Risk Tolerance Identification

Hamilton College, determines its own unique appetite for risk. This self-assigned designation defines the level at which confidentiality, integrity and availability of information assets will be pursued, or from the opposite perspective, the tolerance level at which Hamilton College will accept compromise of these attributes. Defining Hamilton College as risk-tolerant, risk-averse or somewhere in between will help drive resources, culture and Risk Management.

The determination of Global Risk Tolerance, a number between 1 and 100 (where 1 is entirely risk-averse and 100 is entirely risk-tolerant), will be performed by GreyCastle through an informal survey of organization executives and stakeholders. This will be done using qualitative means, as a quantitative measurement would require significant time and resources. The Global Risk Tolerance will be used as a suggested remediation threshold during Risk Management – any risk that exceeds this level will, and should be considered for the Security Road Map.

2.6 Resource Optimization

Hamilton College dedicates resources to Information Security initiatives in an effort to reduce risk, and subsequently meet business objectives. It is understood that these resources are finite and specific, and of the following types:

1. Budget – The information security effort is allocated funds on an annual basis. Allocated funds are determined by business need, which will be determined by organizational risk.
2. Personnel – The information security effort utilizes of both physical and virtual members, full-time employees, partners and subcontractors. The number of personnel allocated to information security initiatives is determined by business need, which will be determined by organizational risk. These are allocated and leveraged optimally based on capabilities and availability.
3. Time – The information security effort requires time to complete security initiatives. Schedules for security initiatives are determined by business need, which will be determined by organizational risk.

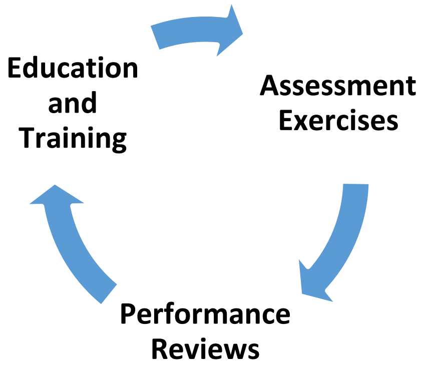
2.7 Cultural Adjustment

It has been proven repeatedly that creating a risk-conscious and security-aware culture within the organization can provide far more protection for information assets than implementing any technology or information security control. This kind of capability can be a game-changing force multiplier if leveraged effectively.

Adjustments in security awareness can be performed utilizing various tactics, techniques and procedures (TTPs), each designed to fill a specific need. These techniques include:

1. Assessment exercises – Understanding the organization's current awareness level, and demonstrating its improvements over time, are keystones of the security awareness program. Through various testing and assessment exercises, personnel awareness levels will be tracked, measured and compared to goals.
2. Classroom instruction – When content is relevant, engaging, interactive, and consumable, classroom instruction is the best way to deliver information security messages. Personnel awareness will be elevated through face-to-face interactions with experienced, engaging educators.
3. Educational reinforcement – According to research, human beings are most open to learning during "teachable moments" – those moments when they have accidentally violated company policy. Through a combination of technology and process, these "teachable moments" will be captured and capitalized on.
4. Awareness promotion – Awareness is best achieved through regular communications. E-mail, verbal and other reminders, presentations, posters, alerts and other methods and mediums will make education a continuous, immersive process.
5. Executive support – Studies continue to prove that effective leadership drives awareness and results. Executives must set examples for personnel. As role models "walking the walk", employees understand what is expected of them and their peers.

Security awareness development is a recurring cycle consisting of the following three (3) steps:



Performed effectively, this system will dramatically reduce risk for the organization and its information assets.

This position on security awareness will be stated and reinforced in the policy statements.

2.8 Risk Reduction

Like all organizations, Hamilton College has a mission. In this digital era, as organizations use automated information technology systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk.

An effective risk management process is an important component of a successful Security program. The principal goal of the risk management process is to protect Hamilton College and its ability to perform its mission, not just its information technology assets. Therefore, the risk management process should not be treated as a technical function carried out by security experts, but as an essential management function of the organization.

3. Roles and Responsibilities

3.1 Overview

Threats to information and information systems can include purposeful attacks, environmental disruptions, and human errors, which result in great harm or loss. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk – that is, the risk associated with the operation and use of information that support the missions and business functions of their organizations.

3.2 Information Security Leadership

To successfully manage risk at Hamilton College, Senior Staff and all employees of the College are committed to making information security a fundamental goal. This top-level, executive commitment ensures that sufficient resources are available to develop and implement an effective, organization-wide Security program. Effectively managing information security risk organization-wide requires the following key elements:

- Assignment of risk management responsibilities to senior leaders and executives;
- Ongoing recognition and understanding by senior leaders and executives of the information security risks to organizational information assets, operations and personnel;
- Establishment of the tolerance for risk and communicating the risk tolerance throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities; and
- Providing accountability for senior leaders and executives for their Risk Management decisions.

3.2.1. Board of Trustees

Primary responsibility for the governance of the College rests with the Board of Trustees.

3.2.2 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 recommends institutional policy to the president who approves these recommendations on behalf of, and in consultation with, the Board of Trustees.

The overall executive responsibility for information security is delegated by the President to the Vice President for Libraries and Information Technology. The VP for Libraries and IT provides executive oversight of Hamilton’s information security efforts and is responsible for approving the overall goals of our work with GreyCastle in coordination with other NY6 colleges, reporting on information security to Senior Staff, and assessing our progress towards meeting goals.

3.2.3 Information Security Board of Review (ISBR)

The ISBR’s role is to provide advice and direction for our efforts to protect the security of confidential and sensitive information.

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.

3.2.4 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.

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.

3.2.5 GreyCastle Security

GreyCastle Security is a provider of cybersecurity services. In October 2014, the NY6 consortium contracted with GreyCastle to provide information security services equivalent to those of an information security officer (ISO) including: risk assessment; development of security policies; evaluation of information security infrastructure; classification of information assets; training; incident management; and regulatory compliance.

4. Security Policy

4.1 Overview

Information Security policy forms the backbone and rulebook for information protection at the Hamilton College. A Security policy should fulfill many purposes. Among other things it should protect personnel and information, define rules for expected behavior by users, system administrators, management, and security personnel, authorize security personnel to monitor, probe, and investigate, define and authorize the consequences of policy violations and help enforce compliance with regulations and legislation.

Above all, Security policy should illustrate the intent and position of the Hamilton College to protect its assets. Hamilton College has the following three Security Policies formalized or in development stages:

- Acceptable Use Policy – Advises all members of the Campus community on acceptable and unacceptable behavior involving the institution's resources. Hamilton's policy can be found at (https://www.hamilton.edu/offices/lits/rc/policies-responsible-use-of-networks-and-computer-facilities)

- Data Classification Policy – Describes the process for classification and handling controls for the institution's data. Hamilton's policy can be found at: (https://www.hamilton.edu/offices/lits/rc/policies-data-classification)
- Information Security Standards Framework – Creates provisional compliance requirements for the Hamilton College Information Security Standards. Requires that all Hamilton College administrative and business functions meet minimum requirements for security.

4.2 Security Policy as Change Agent

In addition to the purposes described above, a Security policy can be useful in ways that go beyond the immediate protection of assets and policing of behavior. It can be a useful compliance tool, demonstrating Hamilton College's stance on best practices and ensuring that they have controls in place to comply with current and forthcoming legislation and regulations.

It is also possible to use policy to drive forward new security initiatives, with policy acting as the catalyst for future projects which move towards better security and general practices. For example, a policy stating that a certain type of encryption is required for sensitive information sent by email may help to promote the need to develop such a capacity in the future. The presence of this requirement in policy helps to ensure impetus to develop the email encryption project has remained strong.

In short, the Security policy is a useful tool for protecting the security of Hamilton College, something that all personnel can turn to in their day-to-day work as a guide and reference.

4.3 Developing Practical Security Policy

The key to ensuring that Hamilton College's Security policies are useful and useable is to develop a suite of policy documents that match the intended audience's business goals and culture. Policies must be practical and realistic. In order to achieve this, it is essential to involve and get buy-in from senior management and other stakeholders, as well as from the people who will use the policy as part of their daily work.

In order to achieve this, one important element is to communicate the importance and usefulness of policies to those who have to live by them. Often, users seem to think that policy is something that is going to stand in the way of their work. An important element of policy development, and to ensure policies are put into practice and not rejected by the users, is to convey the message that policies are useful to users: to provide a framework within which they can work, a reference for best practice and to ensure the organization complies with legal requirements.

Once users realize that policy is something that may actually help them, they are much more likely to be receptive to both assisting in its development and complying with its statutes. Similarly, once senior management realizes that policy is a tool they can leverage to help ensure adherence to legislative requirements and to move forward much needed new initiatives, they are much more likely to be supportive of policy in terms of financial and resourcing support as well as becoming policy champions themselves.

5. Risk Management

5.1 Overview

Information systems can include diverse entities ranging from high-end supercomputers, workstations, personal computers, smartphones and tablets to very specialized systems, including telecommunications systems, industrial control systems, and environmental control systems. Information systems are subject to serious threats that can have adverse effects on organizational operations, reputation, organizational assets, individuals, other organizations, and Hamilton College by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems.

All organizations are subject and vulnerable to threats. Risks to critical information assets may be intentional or negligent, they may come from seasoned criminals or careless employees, they may cause minor inconveniences or extended service disruption, and they may result in severe financial penalties, loss of public trust and damage to corporate reputation.

Identifying risks is the single-most important step an organization can take to ensure the confidentiality, integrity and availability of information assets. It is also an important component for achieving regulatory, commercial and legal compliance.

Lastly, it is important to prioritize the actions that will be taken to mitigate risks, based on the organizations vulnerabilities, the motivation of existing threat-sources, the costs of remediation, the probability that existing vulnerabilities will be exploited, and other factors. This recurring analysis is called Risk Management.

The ISMS will incorporate all of the elements required to successfully execute Risk Management on a recurring basis, comprised of the following three (3) phases:

1. Risk Assessment – This involves identifying the risks to system security and determining the probability of occurrence, the resulting impact and additional safeguards that mitigate this impact.
2. Risk Mitigation – This involves prioritizing, evaluating and implementing the appropriate risk-reducing controls recommended from the Risk Assessment process.
3. Evaluation and Assessment – This involves emphasizing the good practice and need for ongoing risk evaluation and assessment and the factors that will lead to a successful Risk Management program.

This position on Risk Management will be stated and reinforced in the information security policies.

6. Exception Process

Compliance with the Hamilton College ISMS, along with related policies, standards and procedures are necessary to ensure the confidentiality, integrity and availability of institutional information assets. The Hamilton College leadership recognizes, however, that full compliance with portions of the ISMS not be possible, due to operational constraints. As such, a process for addressing exceptions to the ISMS has been developed.

Exceptions to the ISMS are made through the following process:

1. A Request for Exception (RFE) is completed and submitted to AGIS.
2. The RFE is reviewed by committee members. Risks and Corrective Action plans must be evaluated and may be approved, provided that the exception:
   - Is based on a legitimate need,
   - Does not disrupt or compromise other portions of the Hamilton College service delivery capability, and
   - A corrective action plan has been developed for resolving the non-compliance issue that has been assigned an owner who can produce status updates, upon request.
3. Depending on the nature of risk involved, AGIS may make a recommendation to the Vice-

President for Libraries and IT, who will approve the RFE.

7. Information Security Road Map

7.1 Overview

The Information Security Road Map describes the current and planned security priorities of the organization.

During normal operations, Hamilton College's information security priorities and schedule will be determined through a rigorous risk management process. The IS Road Map will be reviewed annually by AGIS in a meeting with GreyCastle.

8. Related Documentation

- Information Security Standards Framework

9. Revision History

Version	Date	Author	Revisions
1.0			Initial draft.
1.1	3/1/2017	Jerry Tylutki (AGIS)	Updated to include Revision History and Approvals section.

10. Approvals

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