LOYOLA COLLEGE IN MARYLAND

Information Security Policy

March 17,2009

Contents

Loyola College in Maryland

Information Security Policy

In order to support sound College-wide information security practices, compliance with various State and Federal legislation, and with various industry standards and best practices, this *Information Security Policy* ("Security Policy") applies to all organizations within the College, and to all authorized Users of College Information Resources. Instances of non-compliance must be reported to the Information Security Office (ISO) and reviewed and approved by the Technology Services Advisory Committee Information Security Subcommittee (ISAC ISS).

College Information Resources are among the College's most valuable assets, and must be managed in a manner that supports appropriate levels of information integrity, confidentiality, and availability for lawful educational and business purposes. This document contains a high-level information security policy for use by all College faculty, staff, administrators, consultants, contractors, students and other Users of the College's information technology resources. All Users shall adhere to the requirements of this Security Policy, and to the requirements of other applicable College policies, standards, and mandatory procedures. All Users shall also comply with any applicable legal or regulatory requirements, and ethical or contractual obligations.

Note: Throughout this Security Policy the terms "data" and "information" are used interchangeably.

I. PURPOSE

The purpose of this Security Policy and associated documents is to define information security practices which will enable the College to:

1) Identify and classify the data in the College's custody, and to apply appropriate protection mechanisms to that data and to systems related to that data.

2) Protect the privacy rights of College faculty, staff, administrators, and students, as well as other Users of College Information Resources.

3) Prevent the misuse of College data, applications, networks and Computer Systems.

4) Prevent compromises of the confidentiality, integrity or availability of College Information Resources.

5) Identify any compromises or misuse that may occur, and provide organizational process and procedures to address such incidents.

6) Comply with legal, contractual and ethical responsibilities with regard to the handling of personally identifiable and other sensitive information, including the configuration of its Computer Systems and networks.

II. SCOPE

1) This Security Policy covers electronic and printed information, defined to include, but not limited to, all information created, collected, retained, processed, or distributed by the College, and all Computer Systems or any subsidiary systems that contain or process data owned or in the custody of the College, regardless of physical location.

2) This policy also applies to, but is not limited to, all faculty, staff, administrators, students, alumni, consultants, and any person or agency employed or contracted by the College or any of its auxiliary organizations, who have an authorized need to access restricted or sensitive College information.

3) This policy applies regardless of whether the Computer Systems used in conjunction with College Information Resources are owned or controlled by the College or by some other party, including Users' personally owned Computer Systems, and regardless of physical location.

III. DEFINITIONS

Data Classifications:

Restricted – Information assets that could be used to steal an individual's identity or cause harm to the individual, or for which there are legal requirements or industry standards prohibiting or imposing financial or other penalties for unauthorized disclosure or improper security measures. Data covered by the Family Educational Rights and Privacy Act (FERPA), the Maryland Personal Information Privacy Act (PIPA), and the Payment Card Industry Data Security Standard (PCI DSS) are in this class, and other data may be as well.

Sensitive -Data that the College has determined should be protected because it may expose the College to loss, or expose an individual to harm if disclosed, but which is not specifically protected by federal or state legislation or by binding contracts. For example, a User ID in combination with a password is considered to be sensitive.

Public -Although there are no restrictions on disclosure to protect public data (because the data is provided for broad viewing access), sufficient protection must be applied to preserve data integrity and prevent unauthorized modification or loss of such data.

General Definitions:

Computer Systems -All computer hardware and software systems, including but not limited to routers, switches and wireless access points, firewalls, servers, databases, workstations, and Portable Computer Systems.

Electronic Media -Any device-readable storage media, whether electronic, mechanical, magnetic, optical, or other. Electronic Media includes, but is not limited to, memory devices in computers, e.g.: hard drives and non-volatile "flash" memory, and any removable/transportable digital memory medium, such as magnetic tape or disks, optical discs, or flash memory devices such as thumb drives and flash cards.

Information Resources – An umbrella term for all data, information media, and computer and other information systems.

Portable Computer Systems -A subset of Computer Systems, these are devices that are designed to be moved from location to location as a part of their normal operation. They include laptop computers, portable digital assistants (PDA), smart phones, and other portable electronic equipment capable of accessing or storing data.

Printed Media – Any human-readable information storage media, including but not limited to information written, typed, drawn, or printed on paper or microfiche.

Privileged Connectivity -Any network connectivity to College Computer Systems or data that would provide access not publically available to a User via an arbitrary computer system on the Internet. Certain workstations and other Computer Systems on certain College networks have Privileged Connectivity. A system is not considered to have Privileged Connectivity if all Users of that system are required to go through a College security gateway which requires authentication and encryption (such as a VPN or a secure portal) to gain access to any restricted or sensitive protected data, just as a User of an arbitrary system on the Internet would.

User -All faculty, staff, administrators, students, alumni, consultants, and any person or agency employed or contracted by the College or any of its auxiliary organizations who have a legitimate need to have access to College systems or data, and who are authorized to do so.

IV. POLICY

The unauthorized addition, modification, deletion, use, or disclosure of restricted or sensitive information owned by or in the custody of the College is expressly forbidden. In certain limited circumstances, as specified in federal and state legislation, the College may disclose restricted or sensitive information.

The College will take reasonable and appropriate steps consistent with current technological developments and accepted best practices to ensure the appropriate confidentiality, integrity, and availability of all restricted and sensitive College information.

A. ACCEPTABLE USE

All Users of College Computer Systems, networks, accounts, or other Information Resources arc bound by the *Acceptable Use Policy*.

B. ACCESS CONTROL

1) Access to restricted or sensitive information and any associated systems that store College information is limited to those authorized individuals who need such access for the purpose of performing their job duties or other functions directly related to their contractual affiliation with the College.

2) While recognizing that there is a delicate balance between protecting data and permitting access to those who need to use the data for authorized purposes, systems should be configured to provide Users, Computer Systems and associated accounts with *only* those system privileges required for authorized purposes. This is the principle of least privilege.

3) Data access control measures must be sufficiently documented to support effective ongoing management of access privileges.

4) Restricted and sensitive information, whether electronic or printed, shall not be displayed in plain sight in order to prevent unauthorized viewing, and must be secured when unattended.

5) Methods of access to restricted or sensitive information, and any associated information systems, is limited to approved, secured, authenticated and centrally managed methods as defined by this Security Policy and by other College policies, configuration standards, and mandatory procedures.

6) Any computers, whether owned by the College or not, with direct connectivity to non-College networks, and which are also used to connect to College networks must comply with applicable College policies, standards, and mandatory procedures.

7) Access to Restricted, Sensitive or Public data may be monitored or logged for later review, in accordance with decisions made by the ISO or the appropriate data stewards. Where required by law or binding contracts, such monitoring and logging shall be performed.

C. ACCOUNT MANAGEMENT

1) All Users of systems that host, or have Privileged Connectivity to, restricted or sensitive data must have their own individual accounts and passwords. The sharing of accounts or passwords is forbidden.The use of group or generic accounts with access to restricted or sensitive data is forbidden.

2) User and system accounts shall be given only for those system privileges that allow them to perform their assigned job duties and functions in an efficient and effective manner.

3) Personnel who have administrative system access must use non-administrative accounts for performing non-administrative tasks.

4) The accounts of terminated, resigned or retired employees must be disabled on the effective date of the termination, resignation or retirement.

5) Employees that transfer from one position within the College to another must have their access adjusted or removed on the effective date of the transfer.

6) Accounts used by vendors or consultants for remote management of information systems must be enabled only during the time periods needed for their authorized contractual obligations.

D. PASSWORDS

1) All Users of College Computer :Systems must fully comply with the *Password Policy*.

E. NETWORK CONNECTIVITY

1) No party may connect College networks (whether wired or wireless) with each other or with non-College networks without the approval of the ISO.

2) No party may install networking equipment, including but not limited to hubs, switches, routers, or wireless access points without the approval of the ISO.

3) All College wireless networks are to be treated as untrusted public networks, isolated by firewalls from other College networks.

4) Any computer system connected to College Information Resources via a wireless network is to be treated as if it were connected via the public Internet, and no such system is to be given Privileged Connectivity to any College computer system or data.

5) Sensitive and Restricted information shall be encrypted when transmitted over any networks which are publicly accessible. Due to the open nature of college campuses this includes most College networks that are not both physically secured and protected by firewalls and other technical security measures. Encryption technologies may include secure application protocols or the use of clear-text protocols when protected within encrypted Virtual Private Networks (VPN).

6) Any connections between College networks and non-College networks must be properly secured by Technology Services to ensure that College networks, Computer Systems, and data are appropriately protected.

7) All Computer Systems that connect to College networks, or which are used to access, store, or process restricted or sensitive data must comply with this Security Policy and with other applicable College policies, configuration standards, and mandatory procedures.

8) All servers must be approved by and registered with the ISO before being connected to College networks.

9) Technology Services reserves the right to remove any computer system from the College network that does not comply with this policy.

F. DATA COLLECTION, RETENTION, AND DESTRUCTION

1) Data collection and retention must meet standards required for business, legal, or regulatory purposes, as documented in the *Data Collection, Retention and Destruction Policy.*

2) Data collection, retention, and destruction shall be performed using mechanisms that comply with this Security Policy, the *Data Collection, Retention and Destruction Policy,* with other applicable College policies, configuration standards, and mandatory procedures.

G. BACKUP AND RECOVERY

1) Data essential to the business of the College, whether or not it is sensitive or restricted, is to be stored redundantly (backed up).

2) In order to be backed up by Technology Services, data must be stored on centrally managed file servers. Technology Services is not responsible for backing up the contents of the local hard drives of desktop or Portable Computer Systems, or the contents of removable storage media.

3) Backup of data and software stored on centrally managed file servers must be sufficient to satisfy disaster recovery requirements, as negotiated between the stewards of the data and software, and the administrators of the Computer Systems.

4) Computer Systems and media used for centralized storage and backup purposes shall be housed in College approved, centrally managed, and secured facilities.

5) Backup and recovery procedures are required for all essential data and software systems.

H. PHYSICAL SECURITY

1) No computer system or other information resource, which is not sufficiently physically secured shall be used! to store or be given Privileged Connectivity to restricted or sensitive data, without sufficient compensating controls as determined by the ISO.

2) All Users of College Information Resources are responsible for the physical security of any College data and Computer Systems and data in their custody. This includes, but is not limited to, ensuring that doors and cabinets are locked when unattended, and that only authorized individuals have access to these facilities and resources. It also includes responsibility for maintaining the physical security of briefcases and other physical information storage and transport mechanisms in their custody.

3) Public Safety will provide guidance to the College and its User community regarding physical security measures, mechanisms and procedures.

4) Documentation of all Information Resources that house or have Privileged Connectivity to restricted or sensitive data, including but not limited to Computer Systems and file cabinets, shall be provided to the ISO by the Data Stewards of each division or department.

5) The ISO will provide Public Safety with documentation of areas that house or have Privileged Connectivity to restricted or sensitive data, including data centers and other locations.

6) Public Safety will provide appropriate physical security measures for College data centers, and other locations which house or have Privileged Connectivity to restricted or sensitive data.

7) Public Safety will monitor security cameras and other physical security systems, and respond appropriately to suspected breaches or attempted breaches of physical security, including forced doors and other attempts at unauthorized access to areas housing or having Privileged Connectivity to restricted or sensitive data.

8) Technology Services is responsible for determining who needs physical access to College data centers, and for logging visitors to these and other associated facilities, where such logging is required by policy, or by legislative, regulatory or contractual requirements.

I. INCIDENT RESPONSE MANAGEMENT

1) It is the responsibility of everyone involved with College data and information systems to report suspected security incidents regarding these resources to the ISO. Such suspected incidents include but are not limited to unauthorized access, exposure, loss or modification of restricted or sensitive data.

2) Various parties have additional responsibilities for security incident monitoring beyond reporting what they happen to notice. These specific responsibilities are listed in the Roles and Responsibilities section of this policy, and in other College policies.

3) The ISO must respond to any suspected security incidents to make an initial detennination of whether to begin full Incident Response Procedures, as described by the *Incident Response Plan.*

4) The *Incident Response Plan* defines roles, responsibilities and procedures for responding to a suspected incident involving the integrity, availability, or confidentiality of restricted or sensitive data and associated Computer Systems.

5) The College will report or publicize unauthorized information disclosures, as required by law or specific industry requirements. All such reporting and or publication is to be handled exclusively by the appropriate appointed members of the Incident Response Team as described by the *Incident Response Plan.*

J. TRAINING AND AWARENESS

I) All College employees shall be trained on this Security Policy, the *Acceptable Ue Policy,* and other appropriate College policies, configuration standards, and procedures as they relate to their individual job responsibilities. Such training will include information regarding controls and procedures to prevent employees from providing unauthorized access to restricted and sensitive information.

2) Employees shall be presented with this Security Policy upon hire and at least annually, and be informed of their responsibilities regarding information security. The College will also make available educational material such as guidelines for safe computing, and for the safe handling of information.

3) Employees are required to acknowledge in writing that they understand their responsibilities, by signing the Confidentiality/FERPA agreement before being granted access to restricted or sensitive information.

K NEW HIRE EMPLOYEE SCREENING

All employee hiring, including the hiring of student-employees, must be done in compliance with the *Background Check Policy.*

L. SERVICE PROVIDERS

Any outside parties who, in order to fulfill their contractual obligations to the College, require access to restricted or sensitive College information, must comply with all applicable College Policies, including this Security Policy. Contracts involving access to restricted or sensitive College data shall be written in accordance with the *Information Security Policy for Contracts.*

M. ROLES AND RESPONSIBILITIES

I) Technology Services Advisory Committee Information Security Subcommittee (TSAC ISS) -This is a group of individuals appointed by the Chief Information

Officer (CIO), the President's Cabinet, the Faculty Senate, and the Loyola Conference to:

a. Review current and proposed College practices to investigate their impact on information security.

b. Review College policies, standards or procedures intended to address risks to information security, and identify necessary changes.

c. Identify additional policies, standards or procedures that arc needed to address risks to information security.

d. Deliver new or modified policies, standards, and procedures to the Technology Services Advisory Committee (TSAC) for approval.

e. Support the efforts of the College Compliance Officer, Information Security Office, and the department of Public Safety in promoting secure and compliant practices surrounding College Information Resources.

2) **Information Security Office** - This office, within Technology Services will:

a. Perform Risk Management, including a formal Risk Assessment at least once per year, assisting the College in identifying and mitigating internal and external risks to the confidentiality, integrity and availability of College data, including but not limited to restricted and sensitive information.

b. Provide guidance and assistance to Data Stewards, Data Managers, and Users for handling restricted and sensitive information and associated information systems.

c. Contribute to the development of College information security policies, standards, and procedures, including this Information Security Policy.

d. Identify and promote good security strategics and practices, based on industry-accepted best practices.

c. Provide guidance regarding information security to Users of College Information Resources.

f. Implement and provide support for appropriate security mechanisms and procedures for controlling access to, transmitting, storing, and destroying restricted or sensitive data.

g. Perform vulnerability scans and penetrations tests on College Computer Systems regularly and after significant changes or upgrades to these systems.

h. Employ, encourage and support the use of, secure software and hardware technologies that meet the requirements of this Security Policy.

i. Take measures to detect, and take appropriate actions in response to any suspected information security compromises, as described *Incident Response Plan.*

3) **Incident Response Team -** This group, designated by the CIO in consultation with the TSAC ISS, has responsibility to:

   a. Develop the *Incident Response Plan.*

   b. Execute the *Incident Response Plan* if prompted to do so by a suspected compromise to the availability, security, integrity, or confidentiality of College information or related Computer Systems.

   c. Coordinate the efforts of the ISO, the College Compliance Officer, Public Relations, Public Safety, and other College functions as appropriate and specified in the *Incident Response Plan.*

4) **External Auditors - This** group, engaged by the Division of Business and Finance will:

   a. Regularly evaluate the effectiveness of current information security safeguards.

   b. Provide recommendations for additions and revisions to College computing policies and associated documents.

   c. Conduct regularly scheduled audits of individual and departmental access to restricted and sensitive College information and associated systems to verify compliance with associated requirements.

5) **Data Stewards** -The Steward of a given collection of data is the individual, department, or organization that has ultimate authority to authorize access to it, and which is responsible for its collection, retention, and destruction. Any given collection of data may be under the shared stewardship of multiple parties. Data Stewards have responsibilities to:

   a. Determine what data they have collected or retained, where it is stored, and who has an authorized business need for privileges to access, modify, or destroy that data.

   b. In coordination with the College Compliance Officer and the TSAC ISS, and in compliance with relevant statutes and contractual obligations, determine if their data is restricted, sensitive, or public.

   c. Regularly review and document User access requirements to their restricted and sensitive data, and provide this documentation to the ISO, so that this information can be included in the *Software and Data Inventory*.

d. Work with ISO and the College Compliance Officer to ensure that any restricted or sensitive data is handled in compliance with this Security Policy, and with any other applicable policies, standards, or mandatory procedures, and with any applicable legislative, regulatory, or contractual requirements.

6) **Data Managers** – The managers of a given collection of data are the individuals, departments, or organizations that are responsible for storing, handling, or managing systems related to that data, and any Users, including but not limited to employees, agents, or affiliates of the College, who handle or have access to that data. Data Managers shall:

   a. Implement necessary security requirements should such data be considered restricted or sensitive.

   b. Work with ISO and the College Compliance Officer to ensure that any restricted or sensitive data is handled in compliance with this Security Policy, and with any other applicable policies, standards, or mandatory procedures, and with any applicable legislative, regulatory, or contractual requirements.

7) **Systems Administrators –** These individuals are responsible for the technical administration of various Computer Systems. In addition to their responsibilities under this Security Policy and other policies and related documents, they must also comply with the *Secure Systems Administration Policy*.

8) **Supervisors -** These individuals, who have managerial or oversight responsibility for others employed by, or contracted to the College, are responsible to:

   a. Ensure that their subordinates' access to restricted and sensitive data is appropriate to their job duties.

   b. Conduct periodic reviews of the access requirements of their subordinates to restricted or sensitive data.

   c. Notify the Human Resources Office of employee reassignments and changes in employment status.

   d. Notify the ISO of changes in employee responsibilities that impact employee access requirements to restricted or sensitive data.

   e. Ensure that their subordinates adhere to College policies, standards, and procedures related to information security.

   f. Ensure that their subordinates receive appropriate training as directed by the department of Technology Services and the Human Resources Office.

   g. Provide their subordinates with approved and sufficient resources and methods to properly handle restricted or sensitive information and associated information systems.

h. Identify any data their departments own or are in custody of, and work with the ISO to determine which if any of that data is restricted or sensitive.

9) **Human Resources Office** -The Human Resources Office has a responsibility to:

a. Notify the ISO of employee reassignments and changes in employment status that impact employee access requirements to restricted or sensitive data.

b. Collect, maintain, and regularly audit signed acknowledgments of employee responsibilities and employee receipt of security awareness training.

10) **College Compliance Officer** -The Assistant Vice President for Human Resources is the College's Compliance Officer. The Compliance Officer receives complaints or notices of policy violations, initiates investigations, and involves appropriate managers and outside counsel in evaluating violations and imposing penalties. The Compliance Officers may also hear appeals and manage the appeal process.

V. PENALTIES AND ENFORCEMENT

Enforcement of this policy will be in accordance with University policies;

Staff & Administrators Policy Handbook: Section 1.26 Discipline
http://www.loyola.edu/HR/Policies/Emplovment%20Polices%20and%20Procedures /Discipline

Student Community Standards Handbook: Pages 13, 27, 31
http://www.loyola.edu/campuslifc /studentlife/judicialaffairs/2008%202009%20Loyola%20Community%20Standards.pdf

Faculty Handbook: Appendix C - Employee Grievance Policy And Hearing Procedures
http://www.loyola.edu/academics/academicaffairs/documents/FH 08.pdf

VI. EFFECTIVE DATE, REVIEW AND REVISION OF POLICY

This Security Policy will be effective as of the date of signature by the approving authority and will be subject to review and revision at least yearly and as updates are needed. In cases where immediate compliance with this policy is not reasonably feasible, a detailed plan must be developed for becoming compliant, and that compliance plan must be registered with and approved by the ISO and the TSACSS.

VII. APPROVALS:

Prepared by the Technology Services Advisory Committee Information Security Subcommittee and the Information Security Office

Preparer Name and Title: **Jason Youngers** **Sr. Information Security Engineer**

Preparer Signature: ***Jason Youngers***

Reviewed and approved by the Technology Services Advisory Committee

Reviewer Name and Title: **Louise Finn** **Chief Information Officer**

Reviewer Signature: ***Louise Finn***

Reviewed and approved by the Loyola Conference

Final Approval Name and Title: **Brian Linnane, S.J.** **President**

Final Approval Signature: ***Brian Linnane, S.J.***

APPENDIX A: LEGISLATIVE CONTEXT

The ISO and TSAC ISS supports the efforts of the College Compliance Officer to determine what legislation, contracts and other standards are binding on the College, what other requirements the College will choose to comply with even if not binding, and what must be done to comply.

The following is a partial list of federal and state legislation, and industry standards which may or may not be binding or applicable to the College.

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Privacy Act (HIPAA)
- Maryland Personal Information Privacy Act (PIPA)
- Payment Card Industry Data Security Standard (PCI DSS)

APPENDIX B: ASSOCIATED DOCUMENTS

The following is a partial list of College policies, configuration standards, and procedures documents which together contribute to the College's information security objectives. Some of these documents are under development. All of them will be available from the Human Resources Office at www.loyola.edu/HR/policies or from the ISO.

- **Acceptable** Use **Policy –** A concise set of rules describing types of activities that are permitted and prohibited for Users of College Information Resources.
- **Data Classification Guidelines -**These are a collection of non-binding guideline documents that Data Stewards can use, with the assistance of the ISO, to determine appropriate classification for various data. These non-binding guidelines may be usurped by various legal and regulatory compliance documents that require specific treatment of certain types of data, as determined by the Compliance Officer.
- **Data Collection, Retention and Destruction Policy –** A policy that delineates what types of data can be collected and retained, for how long, and on what systems. This policy also details procedures for the destruction of data.
- **Incident Response Plan –** A detailed plan with roles, responsibilities and step-by-step procedures for dealing with any real or perceived compromises to the availability, integrity, or confidentiality of College Information Resources.

- Information Security Policy for Contracts – A policy listing required language that must be included in any contracts the College takes part in, regarding the handling of restricted or sensitive information by third parties.

- Information Systems Configuration Standards – A collection of documents with detailed and specific technical and configuration requirements for various types of Computer Systems.

- Employee Background Check Policy – A notice to current and future employees as to what steps the College will take to verify their employment and criminal histories, among other information.

- Password Policy – A policy containing detailed and specific requirements for the creation, storage, use and retirement of passwords and encryption keys for use with College Computer Systems.

- Privacy Policy – A legal notice addressed to Users of College Information Resources, setting expectations of what information is being collected from them, how that information will be used, and to whom that information will be disclosed.

- Procedures - Detailed step-by-step procedures for completing various business or technical processes. Some procedures are mandatory and shall be followed, while others are provided as guidelines or for informational purposes.

- Secure Information Systems Administration Policy - An additional and supplementary information security policy that provides extended and more detailed requirements and responsibilities for the administration Information Resources. Though the scope ofthis additional policy is College-wide, the responsibilities it delineates are generally those of technology managers and systems administrators.

- Software and Data and Inventory - A comprehensive accounting of all software and data owned by or in the custody of the College, including but not limited to who owns it, who has stewardship over it, who has management responsibilities concerning it, where and how it is stored, who needs access to it, what if any legislative or other obligations apply to it, and whether it is to be treated as restricted, sensitive, or public information.