Marist College

Information Security Policy

February 2005

Information Security Policy

Information Security Policy

This document establishes the Information Security policy for Marist College.

Introduction

The Marist College Information Security Policy serves to support the College's mission of "…helping students develop the intellect and character required for enlightened, ethical and productive lives in the global community of the 21st century." Marist is committed to providing a computing environment that protects the community's academic freedom. Nothing in this document should be construed or is intended to limit academic freedom or any legitimate use of Marist information resources (information resources are defined below). At the same time, Marist is also committed to ensuring the integrity and confidentiality of data, meeting legal and regulatory requirements and ensuring that the use of our computing resources meets the highest ethical standards.

The Executive Vice President has overall responsibility for this policy.

Purpose of Information Security Policy

The purpose of the Marist College Information Security Policy is to:

1. Communicate to the Marist community their rights and responsibilities related to the use of information resources;
2. Establish rules to effectively protect information resources from misuse or abuse;
3. Establish information security roles and responsibilities within Marist College;
4. Ensure that Marist College complies with state and federal law and regulation regarding information security;
5. Provide assurance to our stakeholders that Marist is taking appropriate measures to meet best practices for the securing of information resources;
6. Establish mechanisms for responding to security related issues.

This policy also recognizes the evolutionary nature of information security. Therefore, this policy is established with an eye toward change recognizing the dynamic nature of the current security environment.

Information Resources – Definition

For the purpose of this policy, information resources refers to:

1. All Marist College owned computer hardware, software, communications equipment, networking equipment, networking and telecommunications protocols, associated storage and peripherals;

2. All computer hardware, software, communications equipment, networking equipment, associated storage and peripherals that are connected to any Marist College information resource;
3. All computer hardware, software, communications equipment, networking equipment, associated storage and peripherals that store or transmit information that belongs to Marist College;
4. All data, information and intellectual property that may be transmitted over or stored on any Marist College information resource;
5. Any paper reports, microfilm, microfiche, books, films or any media containing information, data or intellectual property that is the property of Marist College.

Information Security - Definition

Information Security is the protection of information resources against unintended uses. This includes, but is not limited to, protection against:

1. Inappropriate release of data (advertently or inadvertently);
2. Access of the College's data without the permission of Marist College;
3. Illegal or unethical use of Marist College's data, computing or network resources;
4. Disruption of computing and network resources at Marist College or by resources of Marist College;
5. Violations of the intellectual property rights of Marist College and members of the Marist community;
6. Violations of intellectual property rights by members of the Marist community;
7. Other activities that interfere with the education, research or service mission of the College.

Applicability

This policy applies to all Marist students, faculty and staff. This policy also applies to anyone who has access to, or uses any Marist College information resources. Contractors performing work for Marist College that involves any information resources must also meet the requirements of this policy.

This policy is meant to be consistent with all other College policies. In the event that state or federal law, regulation or local policy imposes more specific or more stringent requirements than are required by this policy, the law, regulation or policy shall take precedence.

Roles and Responsibilities

Information Security Policy

All members of the College community share in the responsibility for protecting information resources for which they have access or custodianship. Below are listed specific information security roles and responsibilities within the Marist community.

Information Security Policy Steering Committee

The Information Security Policy Steering Committee is a College-wide committee chaired by the Executive Vice President and charged with:

a) Establishing a secure and stable environment and providing leadership for the security of our information resources;
b) Developing policies relative to the security of our information resources;
c) Providing guidance to the IT Security Procedures and Practices Working Group;
d) Providing periodic reports and updates to the President, Cabinet and Technology Committee of Board of Trustees.

The membership list for this committee appears in Appendix A.

College Information Security Officer

The College Information Security Officer (CISO) will be designated in writing by the Vice President and Chief Information Officer (CIO). The CISO has primary responsibility for implementation of the College's information security policy, practices and processes. The CISO shall report to the Vice President for Information Technology and Chief Information Officer. The responsibility of the CISO shall include:

1. Staying abreast of federal and state legislation and its impact on security policy and planning;
2. Monitoring security activities and best practices at institutions of higher education;
3. Implementing and auditing College-wide information security practices as established by the Information Security Steering Committee;
4. Advising the Executive Vice President and CIO on requests for implementation of information resources that deviate from approved College information security practice or policy;
5. Disconnecting, blocking or removing from the Marist College network any information resource that violates this policy, state or federal law or regulation, other polices of Marist College;
6. Investigating all actual or potential information security incidents or violations of this policy and providing reports to the Executive Vice President and the CIO, as well as, to other Vice Presidents or unit heads as is appropriate to the incident;
7. Coordinating information security activities of Marist College with appropriate state or federal agencies as required by law;

8. Serving as the College's point of contact for any alleged copyright or intellectual property infringements;
9. Serving as or supporting existing College compliance officers for federal information security and privacy mandates;
10. Taking necessary and immediate action to prevent damage to the College's information resources in the event of an emergency (e.g., blocking ports on a border router to prevent the spread of viruses);
11. Developing a College-wide information security education program that includes:
    a) Working with the Office of Human Resources to develop information security training and education for all Marist College employees,
    b) Working with ResNet, the Student Affairs Office and School of Computer Science and Math to develop information security training and education for all Marist College students,
    c) Informing the Information Security Policy Steering Committee and the College community of security issues and safeguards,
    d) Maintaining the College's Information Security Web site,
    e) Providing information for the CIO to inform the Cabinet, Deans, Trustees and others of security issues and safeguards;
12. The CISO with the advice and consent of the Executive Vice President and CIO may permit deviations from this policy if such deviations are required for the smooth operation of the College.

IT Security Procedures and Practices Working Group

The IT Security Procedures and Practice Working group is a cross-functional team within IT chaired by the College Information Security Officer with the following responsibilities:

a) Establishes standards, procedures and guidelines to implement policies set by the Information Security Policy Steering Committee, including appointment and oversight of Marist IT internal auditors to ensure compliance with policies and standards;
b) Advises the Information Security Policy Steering Committee on existing and proposed new policies;
c) Proposes policy changes to the Steering Committee;
d) Provides the Marist community with education on security issues and practices;
e) Establishes and monitors the work of the Security Incident Response Team;
f) Manages the Central Security System.

The membership list for this group is shown in Appendix B.

Stewards

Stewards are senior supervisory personnel who work within a specific department who have primary responsibility for particular information. A steward will be appointed for all information covered under this policy. Stewards will be designated in writing by the Vice President in charge of the department responsible for the maintenance of the information in question. In addition, faculty are the stewards of their research and course materials; students are the stewards of their work.

Stewards determine who is authorized to access Marist College information resources under their management. They shall make sure that those with access have a need to know the information and know the security requirements for that information. Information may be disclosed only if disclosure is consistent with law, regulations and College policies, including those covering privacy. Except under unusual and specifically recognized circumstances, access shall be granted to individuals in such manner as to provide individual accountability.

Stewards shall keep records documenting the creation, distribution, and disposal of College information.

Stewards shall report suspected or known compromises of their information to the CISO at the following e-mail address: security@marist.edu. Incidents will be treated as confidential unless there is a need to release specific information.

Stewards must:

a) Identify the electronic information resources within areas under their control;
b) Ensure adequate backups (for data not stored on central IT resources) and other safeguards for all information under their purview;
c) Ensure all data under their purview is maintained in a manner that will provide up-to-date and accurate information for the College;
d) Define the purpose and function of the resources and ensure that the necessary education and documentation are provided to the campus as needed;
e) Establish acceptable levels of security risk for resources by assessing factors such as:

   - Legal or intellectual property requirements
   - Criticality of information for College operation, research projects or other essential activities
   - Likelihood for misuse of information resources
   - Technology programmatic, cost or staff limitations;

f) Ensure that required security measures are implemented for the information resources under the steward's purview.

IT Internal Auditor

Internal auditors are designated IT staff with cross-functional responsibilities. They must:

a) Oversee the enforcement of the Information Security Policy;
b) Identify information security risks and report them to the Information Technology Policy and Practices Working Group;
c) Identify Information Security Policy violations and report them immediately to the CISO;
d) Audit Information Technology operations, policies and practices to ensure conformance with this policy.

In accordance with College audit procedures, the Internal Auditors will conduct audits of the College's information security procedures and practices, including privacy and confidentiality procedures in individual offices on a regular, periodic basis. Internal auditors cannot supervise or work within the area for which the auditor has responsibility.

Managers

Managers are members of the College community who have management or supervisory responsibility, including deans, department chairs, directors, department heads, group leaders, supervisors, etc. Faculty who supervise teaching and research assistants are included. Managers shall provide an environment that promotes security. They shall make sure their staff has the training and tools needed to protect information.

Managers must:

a) Make sure their people have the access authorizations needed to perform their jobs. The authorizations themselves are acquired from the Stewards of the information resources;
b) Ensure that employees, including student employees, lose access when their employment is terminated or job responsibilities change;
c) Administer and retain confidentiality statements for the people they manage or supervise if confidentiality statements are required by the steward(s) of the information.

Users

Users are individuals who access and use campus electronic information resources. Without exception, all members of the College community are "Users" of Marist's information resources. Users must:

a) Become knowledgeable about relevant security requirements and guidelines;
b) Protect the information resources they have access to or control, such as access passwords, computers, and data;

c) Adhere to all College information security policies and procedures;
d) Use Marist information resources in an ethical manner consistent with College's mission.

The CISO, with the advice and consent of the IT Security Policy and Practice Working Group and the Information Security Policy Steering Committee, shall publish and enforce guidelines for users relating to physical security, logical security, passwords, software and patches, data backup, viruses, remote access and other topics critical to the information security posture of Marist College.

Information Classification

Data and information that are owned by Marist College must be protected to ensure the rights of Marist College, its students, faculty and staff are safeguarded. These safeguards are required, in some cases, by law, in some cases by College policy, and in some cases by high ethical standards. Appendix C contains the Marist College information classifications. The Information Policy Steering Committee is responsible for monitoring and maintaining these classifications.

Policy Violations

It is a violation of this policy to:

1. Interfere with the normal operation of any Marist College information resource;
2. Use Marist College information resources to interfere with the normal operation of information resources outside of Marist College;
3. Use Marist College information resources to:
    a) Violate local, state, federal or international law,
    b) Cause, encourage or facilitate others in violating local, state, federal or international law;
4. Access or cause another to access any information resource without permission of the CISO or appropriate steward. The CISO will work with the stewards to develop a consistent, document process for granting access to information resources. Permission is given generally to access publicly accessible Web pages;
5. Access or cause another to access intellectual property, copyright protected property or other legally protected property without permission from the property's owner;
6. Release information resources without the approval of the appropriate office of Marist College;
7. Use any information resource to violate any policy of Marist College;
8. Use any information resource to violate the security policy, acceptable use policy or other operational policies of organizations or institutions outside of Marist College;
9. To promulgate software, data files or other materials that can be reasonably considered as viruses, Trojans or other "malware;"

10. To use information resources to take part in, encourage or foster the development, exploitation or use of software, data files or other materials that can be reasonably considered viruses, Trojans or other ”malware;”
11. Scan any information resource of Marist College without written approval of the CISO;
12. Capture or monitor network transmissions, telecommunications transmissions, or any information resources without written approval of the CISO or, in the case of data, written permission of the appropriate steward;
13. Share userids, passwords, identity cards or other means of access to information resources. Exceptions to this may be requested of the CISO but will not generally be granted unless significant resource or operational inefficiency would occur by not granting an exception;
14. Connect or disconnect any device to an information resource without written permission of the CISO. General exceptions are given to Information Technology staff who, as part of their normally assigned duties, continually connect and disconnect equipment from information resources. In addition, a general exception is given to connect storage devices to Marist Information resources if:
    a) The person connecting the device is authorized to use the information resource they are connecting too,
    b) The device does not interfere with the normal operation of information resource,
    c) Connecting this device does not otherwise violate this policy;
15. Install or connect to any Marist College information resource any telecommunications equipment or networking equipment without the written permission of the CISO. General exceptions are given to Information Technology staff who, as part of their normally assigned duties, install or connect telecommunications and networking equipment.

Rights Reserved to Marist College

Marist College reserves the rights to:

1. Examine or monitor any information resource including, but not limited to, equipment, software, computer files, information and data. It is not the policy of the College to routinely examine or monitor these resources. However, the College may choose to do so at any time. The following is a list of situations where the College may invoke this right. This is not intended as an exhaustive list.
    a) Required by legal authority,
    b) The information resource in question may be in violation of this or other policies of the College,
    c) The CISO with the coordination, advice and consent of the Executive Vice President and Chief Information Officer deems it necessary for the efficient and effective operation of the College’s information resources,
    d) The CISO is directed to do so by the College President,
    e) It is required for IT staff to perform repair or normal operation and maintenance activity,

   f) Reasons determined by the Information Security Steering Committee;
2. Remove or block access to any information resource at any time on Marist College or elsewhere should the resource:
   a) Be in violation of this or any other policies of the College,
   b) Interfere with the operation of information resources at Marist College or elsewhere,
   c) Be in violation of state or federal law or regulation,
   d) For other reasons as determined by the Information Security Steering Committee and approved by the executive vice president and the CIO;
3. Prohibit or inhibit any information resource that the CISO with the advice of the Information Security Steering Committee and the approval of the Executive Vice President and CIO determines is:
   a) In violation of this or any policy of the College,
   b) Interfering with the operation of Information Resources at Marist College or elsewhere,
   c) In violation of state or federal law,
   d) Not in keeping with the high ethical standards of Marist College;
4. Report to local, state or federal authorities' information resource related activities that appear to violate the law or regulation.

Reporting Violations

All members of the Marist College community will report violations or suspected violations of this policy to the CISO at the following e-mail address: security@Marist.edu. Alternatively, violations or suspected violations may be reported to the Vice President and Chief Information Officer. Information Technology staff, who become aware of a potential or suspected violation of this policy through the normal course of their work, are required to inform the CISO of the event. The CISO with the advice and consent of the Executive Vice President and Chief Information Officer may, if appropriate, report violations of this policy to law enforcement.

Policy Sanctions

Anyone found to have violated this policy will be sanctioned using the processes found in existing Marist College policy and employment contracts where applicable.

Sources

In addition, the following non-Marist resources were either used in development of this policy or are good references for the Marist community following the procedures, standards and guidelines in this policy. The list is not part of the policy and the list may be amended as needed.

"IT Security for Higher Education: A Legal Perspective"
http://www.educause.edu/ir/library/pdf/csd2746.pdf

"A National Strategy To Secure Cyberspace Questions To Be Addressed"
http://www.gcn.com/cybersecurity/breakout3pgs.pdf

"A National Strategy To Secure Cyberspace" http://www.whitehouse.gov/pcipb/

"Collaborations on Internet Security (CIS) Final Report"
http://www.itrd.gov/fnc/fnc-pswc.pdf

RFC2196 – (FYI8) "Site Security Handbook"
ftp://ftp.rfc-editor.org/in-notes/rfc2196.txt

RFC3127 – "Authentication, Authorization, and Accounting: Protocol Evaluation"
http://www.rfc-editor.org/rfc/rfc3127.txt

The SANS Security Policy Project http://www.sans.org/resources/policies/

"The Information Security Forum's Standard of Good Practice"
http://www.isfsecuritystandard.com/

"OECD Guidelines for the Security of Information Systems and Networks"
http://www.oecd.org/pdf/M00033000/M00033182.pdf

Open Web Application Security Project http://www.owasp.org/

ISO17799 Newsletter http://www.iso17799-web.com/

"Why Security Policies Fail" – Control Data
http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf

Educause/Internet2 Computer and Network Security Task Force
http://www.educause.edu/security/

"Identifiers, Authentication, and Directories: Best Practices for Higher Education"
http://middleware.internet2.edu/internet2-mi-best-practices-00.html

"Libraries Put Up Patriot Act Warnings, But Are They Overreacting?" – Orin Kerr
http://volokh.blogspot.com/2003_03_09_volokh_archive.html#90481062

"Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't"
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=317501

Other higher educational institutions used as reference:

- University of Florida http://www.it.ufl.edu/policies/security
- Georgetown University http://www.Georgetown.edu/uis/security/policies.html
- University of Toronto http://www.utoronto.ca/security/policies.html
- University of California at Berkeley http://Socrates.Berkeley.edu:2002/pols.html
- Penn State http://guru.psu.edu/policies/AD20.html

Approval Process

- Information Security Policy Steering Committee Date Approved: Feb 2004
- Technology Committee of Board of Trustees Date Approved: Nov 2004

Review Cycle

This policy will be reviewed and updated as needed, at least annually, based on the recommendations of the College Information Security Officer, Vice President of Information Technology/CIO and the Executive Vice President.

Appendices

In general the appendices are not part of this policy but are incorporated through reference in the policy. Committee members may be added or replaced as needed by the Chair Standards, as described, are maintained by the IT Security Procedures and Practices Working Group and are not part of this policy. Current copies of these Standards are available on the Information Security Web pages listed in the Additional Resources section of this document.

A. Information Security Policy Steering Committee Members

Director of Physical Plant
Dean, School of Graduate and Continuing Education
Vice President for Student Affairs
Director of Library Services
Director of Safety and Security
Vice President of Information Technology/CIO
Director of the Institute for Data Center Professionals
Executive Vice President (Chair)
Dean, Computer Science and Math
Assistant Academic Vice President/Dean Academic Programs
Director of Academic Technology and eLearning
FAC Representative
Faculty Member
Director of Technology & College Information Security Officer
SGA Representative
IBM Lead Solutions Architect

B. IT Security Procedures and Practices Working Group

College Information Security Officer/Chair
Assistant Director Academic Technology
Manager Administrative Computing
Manager Help Desk
Server Administrator
Manager Operations
Systems Administrator – VM
Systems Administrator -- MVS
Systems Administrator– UNIX & LDAP
Director Telecommunications
Training and Development
Security Analyst

C. Marist College Standard for Information Classification

This Policy applies to all College information resources, including those used by the College under license or contract. "Information resources" include information in any form and recorded on any media, and all computer and communications equipment and software.

All information covered by this Policy is assigned one of three classifications depending on the level of security required. In decreasing order of sensitivity, these classifications are Confidential, Internal use only, and Unrestricted. Information that is either Confidential or Internal use only is also considered to be Restricted.

- **Confidential information**
  This classification covers sensitive information about individuals, including information identified in the Human Resources Manual, and sensitive information about the College. Information receiving this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include information about:
  - Current and former students (whose education records are protected under the Family Educational Rights and Privacy Act (FERPA) of 1974, including student academic, disciplinary, and financial records; and prospective students, including information submitted by student applicants to the College;
  - Library patrons, and donors and potential donors;
  - Current, former, and prospective employees, including employment, pay, benefits data, and other personnel information;
  - Research, including information related to a forthcoming or pending patent application, and information related to human subjects. Patent applications must be filed within one year of a public disclosure (i.e., an enabling publication or presentation, sale, or dissemination of product reduced to practice, etc.) to preserve United States patent rights. To preserve foreign patent rights, patent applications must be filed prior to public disclosure. Therefore, it is strongly recommended that prior to any public disclosure, an Invention Disclosure Form be submitted to the Office of Technology Transfer for evaluation of the technology and determination of whether to file a patent application, thereby preserving U.S. and foreign patent rights;
  - Certain College business operations, finances, legal matters, or other operations of a particularly sensitive nature;
  - Information security data, including passwords;
  - Information about security-related incidents.

- **Internal use only**

This classification covers information that requires protection against unauthorized disclosure, modification, destruction, and use, but the sensitivity of the information is less than that for confidential information. Examples of Internal use only information are internal memos, correspondence, and other documents whose distribution is limited as intended by the Steward.

- **Unrestricted information**
  This classification covers information that can be disclosed to any person inside or outside the College. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to protect against unauthorized modification and destruction of information.

- **Default classification**
  Information that is not classified explicitly is classified by default as follows: Information falling into one of the Confidentiality categories listed above is treated as Confidential. Other information is treated as Internal use only unless it is published (publicly displayed in any medium) by the Steward, in which case it is classified Unrestricted.