Marist College

Information Security Policy

February 2005

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, character, and skills 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

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.

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.

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

9. To promulgate software, data files or other materials that can be reasonably considered a 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)

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.

"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
- 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.

Reviewed: May 2014

Appendices

In general the appendices are not part of this policy but are incorporate 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.

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.