THE OFFICE OF INFORMATION TECHNOLOGY

POLICIES & PROCEDURES

2.4 INFORMATION SECURITY POLICY
2.6 TECHNOLOGY ACCEPTABLE USE POLICY

Version: 3.0 March 2013

2.4 INFORMATION SECURITY POLICY

2.4.1 Policy Statement

Maintaining the integrity of information stored in college systems is a responsibility shared by all users of those systems. All Information Technology (IT) computing resource users are responsible for protecting college information, and are expected to be familiar with and comply with this policy. Violations of this policy may result in disciplinary action up to and including dismissal or expulsion.

2.4.2 Reason for Policy/Purpose

Information is a vital College asset and requires protection from unauthorized access, modification, disclosure or destruction. This policy sets forth requirements and guidelines for incorporation of information security practices into daily usage of College IT computing resources.

2.4.3 Who Needs to Know This Policy

Faculty, staff and students

2.4.4 Table of Contents

2.4.1 Policy Statement
2.4.2 Reason for Policy/Purpose
2.4.3 Who Needs to Know This Policy
2.4.4 Table of Contents
2.4.5 Policy/Procedures
- 2.4.5.1 Physical Security of IT Computing Resources
- 2.4.5.2 Passwords
- 2.4.5.3 Securing Resources
- 2.4.5.4 Confidentiality
- 2.4.5.5 Availability
- 2.4.5.6 Integrity
- 2.4.5.7 Passwords
- 2.4.5.8 Access
- 2.4.5.9 Reporting a Security Related Event
- 2.4.5.10 Proper Evidence Handling and Chain of Custody
- 2.4.5.11 Reporting, Escalation, and Tracking

2.4.5 Policy/Procedures

Users of Mount Saint Mary IT computing resources are responsible for protecting the information processed, stored, or transmitted over or on those resources, and for incorporating the following practices into their daily usage of such resources.

2.4.5.1 Physical Security of IT Computing Resources

College technology assets require physical security measures to protect theft and loss of information. A computer, if stolen, can result in the compromise of sensitive data, passwords, and personally identifiable data (PII). It may be impossible to full know what was lost with the loss of a laptop, especially, if the laptop belonged to someone who works with sensitive data. So, it is the data on the laptop that is significantly more of a liability to the college than the computer itself. Users of IT resources should:

- Always use a security cable or locking device with laptop computers
- Lock office doors when leaving
- Never remove asset tags from equipment
- Lock away laptops, PDAs or computer peripherals overnight
- Configure a password-protected screen saver
- Logout of the system when finished working
- Utilize a power-on password.

2.4.5.2 Passwords

Passwords are an integral part of overall security. To minimize the risk of a password being compromised and data being lost due to unauthorized access, employ the following:

- Do not use familiar names
- Avoid using commonly known facts about yourself
- Do not use words found in the dictionary
- Use at least seven (7) characters
- Utilize both letters and numbers
- Use special characters if possible
- Use upper-case and lower-case letters if possible
- Combine misspelled words
- Do not share your password with anyone
- Never write down your password in an area where it can be linked to your specific computer or account
- Do not store your password in a computer file
- If you ever receive a solicitation from someone claiming to need your password, report it immediately

NOTE – No one from MSMC IT will ever request the password from a user (student, faculty, staff or administrator). IT makes every attempt to develop systems where the password is encrypted and therefore

not “knowable”. Any attempt to obtain a password, even if politely asked, should be reported to the CIO. The CIO will then determine if the attempt to obtain the password was innocent or malicious.

2.4.5.3 Securing Resources

Virus and malware prevention software is provided by IT.

It is IT’s responsibility to keep College computers up-to-date with the latest electronic security measures to prevent viruses and worms from spreading from one machine to another, and to minimize the opportunity for hackers to damage or steal data. IT should employ the following:

- Keep anti-virus software up to date.
- Keep systems patched.

2.4.5.4 Confidentiality

All members of the College community are obligated to respect and in many cases to protect confidential data, and to follow the **Data Classification Security Policy – Section 2.8.** The College strongly discourages storage of any confidential or sensitive data on any computer or network-attached device that has not been explicitly approved by IT. As such, IT computing resource users shall adhere to the following:

- Employ adequate encryption technology for sensitive or critical information such as educational records, social security numbers, student identification numbers, and credit card. For guidance protecting your data, notify the IT Helpdesk at it.support@msmc.edu. (See ITC 2.3.5.1)
- Notify the IT Helpdesk at it.support@msmc.edu if sensitive or critical College information is lost or disclosed to unauthorized parties, if any unauthorized use of College systems has taken place, or if there is suspicion of such loss, disclosure or unauthorized use.
- DO NOT post College material such as software, internal memos, or other non-public information on any publicly-accessible computer unless first approved by the appropriate authority.
- DO NOT place College sensitive or critical information in any computer unless the persons who have access to that computer have a legitimate need-to-know the information involved.
- DO NOT save fixed passwords in web browsers or e-mail clients when using a College system. This may allow unauthorized users to access critical or sensitive information such that contained in Jenzabar.
- DO NOT distribute internal critical or sensitive College communications to external entities that are not affiliated with the College. Only distribute to internal entities on a need to know basis.
- DO NOT establish Internet or other external network connections that could allow non-College users to gain access to College systems with critical or sensitive information unless prior approval has been received by the appropriate authority.
- DO NOT discuss information security-related incidents with individuals outside of the College, or with those inside the College who do not have a need-to-know.

2.4.5.5 Availability

College systems and IT computing resources are expected to be available and ready for usage. Accordingly, resource users are expected to limit usage of these resources to reasonable levels and should assist in making resources available as follows:

- Update system patches for IT computing resources that transmit, process or store critical or sensitive information.
- DO NOT probe security mechanisms at either the College or other sites unless authorized to do so by IT.
- DO NOT cause intentional harm to College-owned IT computing resources. (See ITC 2.6)

2.4.5.6 Integrity

Integrity means ensuring the soundness or completeness of information during its transmission, storage, generation, and/or handling. Information that is modified may be erroneous and could lead to poor business decisions. In order to maximize integrity, IT computing resource users shall adhere to the following:

- Screen all non-text files downloaded from the Internet with anti-virus software prior to usage to minimize the risk of corruption, modification or loss of data.
- Notify IT immediately if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed.
- Forward information pertaining to security-related problems to IT immediately. DO NOT personally redistribute system vulnerability information.
- Review information obtained from the Internet with caution. Before using free Internet-supplied information for business decision-making purposes, corroborate and confirm the information by consulting other reliable sources.
- Secure personal computers via a locking feature such as a password- protected screen saver when walking away. Public computers with no critical or sensitive information, such as those in the library or in labs, are excluded.

2.4.5.7 Passwords

For most applications, the College enforces a maximum password “lifetime” of 180 days, after which the password must be changed. System administrators may set the maximum password lifetime to less than one year for critical or sensitive applications. (**See ITC 2.4.5.2**)

2.4.5.8 Access

Access guidelines define access rights and privileges and protect assets and data from loss or inappropriate disclosure by specifying acceptable use guidelines for users, operations staff and management. Access to

College enterprise business applications is permitted on the condition that the user observes the **INFORMATION SECURITY POLICY (2.4)**. Access may be revoked if this policy is violated; other actions up to and including termination of College employment may also be taken, depending on the particular violation.

- When a user is initially granted an account for a College enterprise business application, access rights are based on legitimate need to access/change data.
- Enterprise business data categories have "owners" (stewards) who are ultimately responsible for the integrity of the data. An application security administrator (ITC 1.3) grants access to specific College Data only after such access is approved by the appropriate data owner.
- For employees and contractors, department managers with knowledge of the individuals' legitimate need to view and change data initiate requests for access to an application as well as requests to change access. Department managers have responsibility for monitoring their employees' job responsibilities and access rights to ensure appropriate access levels.
- When a user's relationship with the College changes, or specific duties change (if an employee or contractor), access rights should be changed to reflect the new relationship/responsibilities.
- The termination of a relationship with the College (e.g., resignation, graduation) results in termination of the user's access rights.
- The College restricts ability to perform changes to security access levels in a production instance of an application to the application's Security Administrator(s)(See ITC 1.3).

2.4.5.9 Reporting a Security Related Event

The IT Helpdesk should be contacted via e-mail i.e. it.support@msmc.edu, via telephone (569-3491), or via the helpdesk ticket system (helpdesk.msmc.edu). When contacting the Incident Response leader, please include the following information if possible:

- The time and date of the event
- A detailed description of the event
- Information pertaining to how the event was discovered
- Business processes affected by the event
- System(s) affected by the event including trusted relationships
- Subnets or other IT computing resources affected by the event
- The physical address where event occurred
- Witness statements of event
- System program information that detected event
- Operating System version including patch information
- Application version information
- System and Event Logs
- Security protection tools currently used by the affected system(s)
- If applicable, a vulnerability and port scan report of the affected system(s)

2.4.5.10 Proper Evidence Handling and Chain of Custody

Evidence must be relevant, material, and competent for admissibility in a court of law. Evidence must be collected and preserved. Evidence must not be altered. After an incident occurs that impacts a critical system, the machine must be unplugged from the network and left undisturbed until or other designee advises that it is safe to repair the machine and reconnect the machine to the network. The Information Security Office should be immediately contacted after the discovery of an incident.

2.4.5.11 Reporting, Escalation, and Tracking

IT shall provide a high-level status report to senior management and the affected business unit manager advising of the computer or information security related event/incident.

Legal/Public Relation Considerations

Oftentimes there are legal and public relations concerns to consider. In order to take these into account IT computing resource users:

- Shall not perform activities over the Internet that are considered libelous or that defame the character of another person or entity
- Shall not speak to or communicate publicly with news reporters or similar entities on behalf of the College unless authorized
- Shall not misrepresent, obscure, suppress, or replace a user's identity on the Internet or any College electronic communications system
- Shall not make threats against another user or organization over the Internet
- Shall not use the Internet to harass, annoy, or alarm another person
- Shall not use the Internet as a means to facilitate criminal or other illegal activity
- Shall not violate the intellectual property rights of any owner of intellectual property

2.6 TECHNOLOGY ACCEPTABLE USE POLICY

2.6.1 Purpose for This Policy

The purpose of this policy is to provide guidelines to the acceptable and ethical behavior that guides use of information and learning technology resources at Mount Saint Mary College. Information and learning technology includes, but is not limited to laptops, desktop computers, workstations, network servers, software, digital information, voice, video/data networks, classroom media and instructional technology. This policy is supplemented by all other college policies and by the policies of those networks to which Mount Saint Mary College is affiliated. All existing laws (federal, state, and local) and College regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

2.6.2 Who Needs To Know This Policy

Faculty, staff and students

2.6.3 Table of Contents

2.6.1 Reason for Policy/Purpose
2.6.2 Who Needs to Know This Policy
2.6.3 Table of Contents
2.6.4 Policy Statement
2.6.5 Responsibilities
2.6.6 Guiding Principles
- **2.6.6.1** Sexual, Racial and other Forms of Harassment
- **2.6.6.2** Authorized Use of Information Resources
- **2.6.6.3** Copyright and Lawful Use of Information Resources
- **2.6.6.4** Social Networking
- **2.6.6.5** Integrity of Information Resources
- **2.6.6.6** End User Back-up Responsibilities
- **2.6.6.7** Document Security
- **2.6.6.8** Hoaxes and Chain Letters
- **2.6.6.9** Identity Theft
- **2.6.6.10** Passwords
- **2.6.6.11** Device Security
- **2.6.6.12** Physical Security
- **2.6.6.13** Securing your Device
- **2.6.6.14** Social Engineering
- **2.6.6.15** Data Classification Security
- **2.6.6.16** Records Management

2.6.7 Consequences of Misuse
2.6.8 Access and/or Ownership

2.6.4 POLICY STATEMENT

Mount Saint Mary College provides access to information resources to students, faculty, staff, and certain other users to support the mission of learning and to conduct business. Every authorized user of information and learning technology resources at Mount Saint Mary is responsible for utilizing these resources in an efficient, ethical, and legal manner and in ways consistent with college policies and code of conduct. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific departments of the college or to uses within specific departments.

Given the inherent openness of computers and networks which facilitate the ability to communicate to a worldwide audience, users must understand that such access is a privilege requiring users to act responsibly.

All users must respect the rights of others, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

All equipment purchased by the College, gifted to the college or acquired through grants is the property of the College and not the property of the individual to whom it may be issued. Therefore, the College has the right to control the equipment and can choose not to provide access to the equipment or the resources (files, data, services) related to the equipment. Any work, files or data attached to the asset is to be considered as part of the asset and property of the College. For guidance on how to handle access or ownership issues, refer to **ITP 2.6.8.**

2.6.5 RESPONSIBILITIES

You are responsible to ensure the integrity and safe keeping of your Mount Saint Mary assigned account. As a condition of receiving access to the Mount Saint Mary network services, you must observe the following guidelines:

- Access to the Mount Saint Mary College network(s) may be used for personal purposes provided such does not interfere with College operation of information technologies or electronic mail services, burden the College with incremental costs, or interfere with any academic and/or business pursuit of the college.
- Use of the facility must be conducted in accordance with established policies and procedures. All Mount Saint Mary assigned network accounts are intended to be used for academic and/or college business purposes.
- Respect the rights of others, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.
- Make economical and prudent use of the facility resources that are shared with others, thus enabling access to those resources by the greatest possible number of users.
- Respect rights to privacy of others.
- Protect judiciously your assigned network access account information by preventing others from learning your password.
- Report suspected unauthorized use of facility resources and/or any circumstance where you perceive that your assigned access account may have been compromised to the Mount Saint Mary Help Desk (Aquinas Room 13 / 845-569-3491) or e-mail it.support@msmc.edu
- You are responsible for backing up your data and programs that are stored on your local hard drives. Mount Saint Mary provides a personal storage network folder for each student, faculty, and staff member facilitating a backup and recovery strategy. If you elect to save data on your local hard drive, it is important to note that this data remains your exclusive responsibility to backup for data loss protection.
- No information should be stored on your local hard drive that can be classified as Personal Identifiable Information (PII) or is a violation of other federal and state statutes designed to protect the identity and confidential information of individuals. All computers which require use of this data for college academic and/or business purposes should store this information on their personal storage network

folder in all cases possible. Otherwise, the laptop hard drive(s) must be encrypted to afford maximum protection where this data must reside on the local machine.

- If your local computer has Personal Identifiable Information (PII) or other confidential information that is protected by federal and state statutes and/or college policy, you are responsible to ensure that the computer is encrypted and that the information is periodically reviewed to ensure that only relevant data is stored on the computer hard drives and that all other protected information is removed in a timely manner. No protected information should be saved on any external device, such as a flash drive or CD-ROM/DVD disk that is not otherwise encrypted and not expressly approved by the CIO.
- Mount Saint Mary Electronic mail services may not be used for unlawful activities, commercial purposes not under the auspices of the College, and not for personal financial gain.

2.6.6 GUIDING PRINCIPLES

The following principles serve to guide the acceptable use of information and learning technology for all Mount Saint Mary users:

2.6.6.1 Sexual, Racial and other forms of Harassment

Respect the rights of others by complying with all college policies regarding sexual, racial and other forms of harassment, and by preserving the privacy of individuals. For example, you should not send harassing messages via e-mail or transmit/reveal personal/private information about individuals. Spoofing, or misrepresenting your identity or giving false or misleading e-mail addresses, is strictly forbidden.

2.6.6.2 Authorized Use of Information Resources

Use of computing facilities, accounts, data, hardware and software is exclusively designed to support the academic and administrative functions of the college and should be employed only when you have appropriate authorization. For example, you should not use Mount Saint Mary information resources to breach the college's network or any other network's security, access another individual's computer account, access or download any copyrighted or illegally obtained materials. In addition, no commercial use shall be made of network resources without express permission of the Mount Saint Mary Administrative Council to include, but not limited to, sales, advertising, and solicitation.

Hacking, spamming, spoofing, attempting to break in, or breaking into any workstation, server, mass storage device, or ancillary hardware owned by or connected to the Mount Saint Mary College network or any external network connected to the Internet is a violation of Mount Saint Mary College policy and may result in disciplinary action. Mount Saint Mary does not condone, sponsor or support such activity and holds no liability for any possible legal action brought against any student, faculty or staff found to be in violation of this policy by Mount Saint Mary College, outside agency or party.

2.6.6.3 Copyright and Lawful Use of Information Resources

Respect all pertinent licenses, contractual agreements, and copyrights. Use only legal versions of copyrighted software in compliance with vendor license agreements and requirements. For example, you should not post another individual's copyrighted material on your webpage or any Mount Saint Mary server without express permission of the holder of the copyright. Installation or copying software with a single user license on multiple computers or distribute via data devices is strictly prohibited. Mount Saint Mary College respects and adheres to all applicable federal, state, and local laws.

Reference: http://library.msmc.edu/copyright/copyright_home.php

2.6.6.4 Social Networking

Social networking (eg.Facebook, Twitter, LinkedIn, and other digital platforms for staying connected to friends and family and communicating/networking among people with similar interest world-wide) has grown significantly. Just as in the use of other Mount Saint Mary provided technology, users of these services should be aware of the policies and laws that apply to social networking, including relative College policies.

Information posted online, including pictures and text, may become virtually impossible to remove from the Internet even after deleting the material. Additionally, pictures and text posted within these on-line services can become the property of these sites once posted. Therefore, do not post information that you do not want available to a world-wide audience at the time of posting and in the future. Today, many potential employers, scholarship committees, graduate school admissions committees, or even potential roommates perform "background checks" by searching the Internet. Careful consideration should be given before posting any information. Posting information that may appear harmless such as your full name, address, birthday, hometown, and pictures can help someone to steal your identity.

Federal and state laws apply in using social networking sites. Copyright infringement, defamation, invasion of privacy, obscenity, pornography, sexually explicit materials, sexual harassment, and stalking are common legal concerns. Users violating theses laws could be subject to civil and criminal fines and/or imprisonment.

2.6.6.5 Integrity of Information Resources

Preserve the integrity of computing systems, electronic data, and communication networks. For example, you should not modify any hardware or software on laptop computers or any settings on desktop computers. The primary purpose of information resources is to facilitate the academic mission at Mount Saint Mary and to grant an equal teaching and learning environment to faculty and students. Therefore, you should not use Mount Saint Mary information resources to attack computers on the college's or another network by launching viruses, worms, or other forms of destructible attacks, publish online or distribute via e-mail or web copyrighted or illegal materials.

2.6.6.6 End User Back-up Responsibilities

The frequency of backups should depend on the importance of the information, how often it is modified and the impact that its loss would have to our organization.

- Perform a FULL backup whenever possible.
- Do not backup over your most recent backup media.
- Use a cycle of at least three backups to avoid losing data if a tape or other backup media goes bad.
- Frequency of backups should be appropriate for the importance of the data on your computer.
- Properly label your backups to ensure correct rotation and identification.
- Store backup media in a safe and secure location.
- Password protect your backups, if possible.

2.6.6.7 Document Security

One of the most overlooked areas of security often involves physical documents. These are also information resources and require the same level of protection as their electronic counterparts. Follow these guidelines to make sure your files are where you need them, when you need them:

- Maintain a "clean desk" and keep your work space secured; i.e., lock up any sensitive files and removable media.
- Don’t leave documents unattended on the copier or fax machine.
- Shred any confidential documents when you are discarding them.
- Remove papers and wipe boards clean when finished using conference rooms.
- Lock filing cabinets when you leave.

2.6.6.8 Hoaxes and Chain Letters

E-mail chain letters and hoaxes ask the receiver to forward the message on to a specified number of people, or as many as possible. However, if you forward a message to just ten people and they each do the same, and this cycle continues ten times, this would result in 10,000,000,000 (that's 10 billion) messages. If that sounds unbelievable, check for yourself - the calculation is 10 to the 10th power.

You can easily see how this can become a burden on e-mail systems in both traffic and storage capacity.

What makes this even worse is that most e-mail chain letters are based on falsehoods or urban legends. They may reference some reputable source but do not provide any contact information for verification.

- Learn how to recognize hoaxes and chain letters
- Discourage others from forwarding them
- If you’re not sure it’s a hoax, report it to the IT helpdesk
- Report persistent senders of inappropriate e-mail to the IT helpdesk
- Delete any hoaxes or chain letters you receive

- Don’t distribute distasteful jokes or images

2.6.6.9 Identity Theft

Your personal information can be targeted by thieves. Once obtained, they can use your identity to obtain cash or purchase items using your credit. The results can be a financially devastating. Take steps to protect yourself by following these tips:

- Never give out financial information to unknown callers
- Guard your credit cards, ATM card, its PIN and receipts
- Immediately report lost or stolen checks and credit cards
- Always shred unwanted financial solicitations
- Store both new and canceled checks in a secure location
- Thoroughly review your bills, bank statements and credit card statements; report unauthorized activity
- Consider using a postal service collection box to mail financially-related items instead of using your residential mailbox
- Periodically obtain and review your credit reports

If you believe another member of the MSMC Community has fraudulently used your information to obtain/use credit, you need to file a report with the MSMC Security/Safety Office [(845) 569-3200] so an official case can be opened and addressed.

If you would like to check to make sure that your identity has not been stolen, you can follow the steps below. The Federal Trade Commission has installed a toll-free number, 1-877-IDTHEFT (877-438-4338) where consumers who have been victims of identity theft can report the crime and get advice from telephone counselors trained to provide assistance to ID theft victims.

To best protect against becoming an ID theft victim, the agency gives the following guidance:

- Be careful about giving out your personal information. For example, don't give out personal identifying information (SSN, date of birth, mother's maiden name) to someone over the phone (or the Internet) when you haven't initiated the transaction. And don't carry your Social Security card (or your children's SSNs) in your wallet.
- Put passwords (NOT your mother's maiden name) on credit card and bank accounts, to make it harder for an ID thief to make changes to, or "takeover," your account.
- Order your credit reports once a year from each of the three national credit bureaus. That way you're likely to catch any identity theft before it gets out of hand -- and not when you're waiting for a mortgage application to be approved.

If you discover that your identity has been stolen, the agency advises the following steps:

- Call the fraud departments of all three credit bureaus. Ask them to put a "fraud alert" on your file (this tells creditors to call you before they open any more accounts in your name). Also, ask for a copy of your credit report, and ask the credit bureau to remove any fraudulent or incorrect information.

- Contact the credit grantors involved - e.g., the bank or credit card issuers who opened the fraudulent account or permitted access to your existing account.
- Immediately close all affected accounts.
- Contact your local police, and ask to file a report. Even if the police can't catch the identity thief, having a police report can help you in clearing up your credit records later on.

For more information about Identity Theft, please visit the following websites:

The website for the FTC's Identity Theft Support is http://www.consumer.gov/idtheft/

The Department of Education has created a website to help students protect against identity theft – http://www.ed.gov/about/offices/list/oig/misused/index.html

2.6.6.10 Passwords

Also refer to ITP 2.4.5.2

Passwords are an integral part of overall security. Unfortunately, they are one of the vulnerabilities most frequently targeted by someone trying to break into a system. If your password is compromised, then anything your user account is able to access could be at risk. There are numerous ways that you can help protect your password and our information.

- Do not use familiar names
- Avoid using commonly known facts about yourself
- Do not use words found in the dictionary
- Use at least seven (7) characters
- Utilize both letters and numbers
- Use special characters, if possible
- Use upper- and lower-case letters, if possible
- Combine misspelled words
- Do not share your password with anyone
- Never write down your password
- Do not store your password in a computer file
- When receiving technical assistance, enter your password instead of telling it to the technology staff member
- If you ever receive a telephone call from someone claiming to need your password, report it immediately

2.6.6.11 Device Security

Also refer to ITP 2.4.5.2, ITP 2.4.5.3

The physical security of our technology assets is a serious issue. If a computer is stolen, there is a lot more at stake than just a piece of hardware. It can take hundreds or even thousands of hours to re-create the information that would be missing along with the computer. There are several things that can be done to help reduce the chance of computer theft.

- Always use a security cable or locking device
- Lock your office door when you leave
- Never remove any assets tags from our equipment
- Lock away any laptops, PDAs or computer peripherals overnight
- Configure a password-protected screen saver
- Logout of the system when you are finished working
- Utilize a power-on password

2.6.6.12 Physical Security

Also refer to ITP 2.4.5.2, ITP 2.4.5.3

There are things to be aware of to help prevent a mishap that could lead to a loss of our information, personal property, or worse. The key is knowing how to prevent a situation from happening. Consider these words of advice:

- If you expect to be working late, park in an area that will have adequate lighting when you leave.
- When entering secured areas do not let strangers "tailgate" in behind you. Never prop open doors that lead to secured areas. If you encounter strangers or unknown visitors in secured work areas, ask them if you could be of some assistance with a simple “May I help you?”
- If you ever lose an access card or key, report it immediately to MSMC Security/Saftey.
- When leaving at night, try to exit with other coworkers if possible. There is some truth to the saying “safety in numbers.”

2.6.6.13 Securing your PC

Also refer to ITP 2.4.5.2, ITP 2.4.5.3

It is important to maintain your computer up-to-date with the latest patches, fixes, service packs and virus definitions (of your anti-virus software). This prevents computer viruses and worms from spreading from your computer and denies hackers the potential opportunity to damage or steal data from your computer.

2.6.6.14 Social Engineering

A social engineer is a person that will deceive or con others into divulging information that they wouldn't normally share. It is one of the most commonly used methods of hacking. By building trust with their victims through deception and lies, a social engineer will try to get information that can be used later, usually for wrongdoing. If someone phones or appears and asks you for information that you know is confidential company, client or personal information, don't be afraid to ask them a few questions yourself.

2.6.6.14.1 To protect data by phone

- Ask for the correct spelling of the caller's name.
- Ask for a number where you can return the call.
- Ask why the information is needed.
- Ask who has authorized the request and let the caller know that you will verify the authorization.

2.6.6.14.2 To protect data in Person

- Ask for some identification.
- Ask who has authorized this request so you may verify the authorization.
- If you are not authorized to provide that information, offer to locate the correct person.
- Seek assistance if you are unsure.

2.6.6.15 Data Classification Security

Responsibility for Data Management

Data is a critical asset of Mount Saint Mary College. All members of the College community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the institution, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of College data in compliance with this policy.

Data owned, used, created or maintained by Mount Saint Mary College is classified into the following three categories:

- Public
- Official Use Only
- Confidential

Departments should carefully evaluate the appropriate data classification category for their information. When provided in this policy, examples are illustrative only, and serve as identification of implementation practices rather than specific requirements. Nothing in this policy is intended to identify a restriction on the right of departments to require policies and/or procedures in addition to the ones identified in this document.

Data Classification

Public Data

Public data is information that may, or must, be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to Mount Saint Mary disclosure rules, is available to all members of the College community and to all individuals and entities external to the institution.

By way of illustration only, some examples of Public Data include:

- Publicly posted press releases
- Publicly posted schedules of classes
- Publicly posted interactive campus maps, newsletters, newspapers and magazines
- Publicly posted academic calendar

Official Use Only Data

Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to members of the College community who have a legitimate purpose for accessing such data.

By way of illustration only, some examples of Official Use Data include:

- Employment data
- College partner or sponsor information where no more restrictive confidentiality agreement exists
- Internal telephone books and directories

Official Use Only Data:

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
- Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
- Must not be posted on any public web site.
- Must be destroyed when no longer needed subject to the college Records Management Policy. Destruction may be accomplished by:
    - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste or recycled.
    - Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with the college's Electronic Equipment Recycling Policy.

Confidential Data

Confidential Data is information protected by statutes, regulations, Mount Saint Mary policies or contractual language. Managers may also designate data as Confidential.

Confidential Data may be disclosed to individuals on a need-to-know basis only.

Some examples of Confidential Data include:

- Medical records
- Student records and other non-public student data
- Social Security Numbers
- Personnel and/or payroll or records
- Bank account numbers and other personal financial information
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction

Confidential data:

- When stored in an electronic format, must be protected with strong passwords and stored on servers that have protection measures provided by Information Technology in order to protect against loss, theft, unauthorized access and/or unauthorized disclosure.
- Must not be disclosed to parties without explicit management authorization.
- Must be stored only in a locked drawer, locked room, or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public web site.
- Must be destroyed when no longer needed subject to the College's Records Management Policy. Destruction may be accomplished by:
    - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste or recycled.
    - Electronic storage media shall be sanitized appropriately by effective destructive measures prior to disposal. Disposal of electronic equipment must be performed in accordance with the Mount Saint Mary Electronic Equipment Recycling Policy.

The Mount Saint Mary College Information Security Officer (Director of Institutional Research & Planning) must be notified in a timely manner if data classified as Confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the College's information systems has taken place or is suspected of taking place.

Data Classification Roles and Responsibilities

Information Technology, in concert with the Mount Saint Mary College Technology Governance Committees, is the primary entity charged with developing policy and procedures subordinate to and in support of this policy. The Mount Saint Mary Information Security Officer is charged with the promotion of security

awareness within the college community, as well as responsibility for the creation, maintenance, enforcement and design of training on relevant security standards in support of this policy. The Director of Institutional Research & Planning will serve as the Information Security Officer for Mount Saint Mary College and will receive/maintain reports of incidents, threats and malfunctions that may have a security impact on the institutions information systems, and will receive/maintain records of actions taken or policies and procedures developed in response to such reports. The Information Security Officer will assist with internal information Technology audits, as appropriate, to verify College awareness of the Data Classification Security Policy and determine compliance with this policy.

The Information Technology Office will facilitate distribution of this policy, assist the Information Security Officer in the investigation of policy breaches, and administer the Mount Saint Mary College 24 hour Regulatory Compliance Help and Referral e-mail address (compliance@msmc.edu), which provides a confidential method for reporting instances of suspected misconduct or violations of law or College policies.

The Mount Saint Mary College Administrative Council will review procedures issued under authority of this policy for compliance with applicable regulations.

The Information Systems Technology Advisory Committee (TAC) and the Academic Technology Advisory Committee (ATAC) will be the initial forums for discussion of questions arising out of or in response to this policy.

2.6.6.16 Records Management

Federal, state and local regulations require that the College adhere to numerous record retention mandates. The appropriate time periods for record retention are fact specific and subject to ongoing statutory and regulatory changes. Therefore, each department should develop its own records management plan in cooperation with the Office of the applicable Vice President, the Administrative Council, and General Counsel as warranted and is consistent with information stated in other College publications to include the College catalog.

Retention and Maintenance of Records

Mount Saint Mary College requires that its records be maintained in a consistent and logical manner and be managed so that the College:

1. Meets legal standards for protection, storage and retrieval;
2. Protects the privacy of faculty, staff, students, and patients of the College;
3. Optimizes the use of space;
4. Minimizes the cost of record retention; and
5. Destroys outdated records in an appropriate manner.

Departments that maintain College records are responsible for establishing appropriate records management procedures and practices. Each department's administrative manager or a designee must:

1. Be familiar with the College's Records Management Policy;
2. Develop the department's and/or office's record management procedures and practices, consistent with this policy;

3. Educate staff within the department in understanding sound record management practices;
4. Restrict access to confidential records and information; and
5. Coordinate the destruction of records as provided in the applicable procedures.

Confidentiality Requirement

Many records subject to record retention requirements contain non-public confidential data. Such records are protected by federal, state and local statutes, including the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley (GLB) Act, and the Health Insurance Portability and Accountability Act (HIPAA). In addition to the RECORDS MANAGEMENT POLICY statutory requirements, any record that contains confidential data should be treated in accordance with the College's privacy and security policies (see the Related Information section of this policy).

Electronically Stored Information

Recent years have witnessed a tremendous growth in the use of electronically stored information ("ESI") by the College. The ease with which ESI may be created, the number of places where ESI may be stored, and new rules regarding the use of ESI in litigation, all require that Mount Saint Mary College manage its ESI effectively, efficiently and consistent with its legal obligations. Accordingly, departments must include ESI in the development of their records management plans.

Preservation of Records Relevant to Legal Matters

Any record that is relevant to any pending or anticipated litigation, claim, audit, agency charge, investigation or enforcement action shall be retained at least until final resolution of the matter. In these circumstances, the Office of the President, Administrative Council and General Counsel will notify relevant departments and work with staff to identify and preserve any records (including electronic records) and other information that could be relevant to the matter. This will include a directive that the relevant unit's normal document destruction policies or protocols temporarily be suspended. Employees who become aware that an investigation or legal proceeding has commenced or is anticipated against their department or unit must promptly notify the Office of the President and their respective Vice President so that all records with potential relevance to the investigation or legal proceeding can be preserved as necessary.

Disposal and Destruction of Records

If you have determined that, consistent with the College's Records Management Policy, and with the records management practices and procedures applicable to your department, it is appropriate to dispose of any records, they can be destroyed in one of the following ways:

1. Recycle non-confidential paper records;
2. Shred or otherwise render unreadable confidential paper records; or
3. Erase or destroy electronically stored data. (Information Technology can assist you in effectively disposing of this data.)

If you have questions about your responsibilities, please contact the administrative manager or department designee.

Definitions

Confidential Data

Confidential Data is information protected by statutes, regulations, College policies or contractual language. Managers may also designate data as Confidential. By way of illustration only, some examples of Confidential Data include:

- Medical records
- Student records and other non-public student data
- Social Security Numbers
- Personnel and/or payroll records
- Bank account numbers and other personal financial information
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction

Confidential Records

Confidential Records are records that contain confidential student, patient or employee data that should have limited access and be protected from inadvertent disclosure.

Record

A Record is information that has been recorded in some fashion which can be retrieved. It can be an original document, photograph, blueprint, sound or video recording, microfilm, or electronically maintained.

Responsible Department

The department designated as having the responsibility for retention and timely destruction of the particular types of College records in their control.

College Record

A College Record is College information that has been recorded in its original source or copy. These can be either electronic or paper and were either received or created by the department.

2.6.7 CONSEQUENCES OF MISUSE

Misuse of computing, network, or information resources may result in the loss of privileges. Additionally, misuse of a computing account could result in disciplinary action by Mount Saint Mary College and may include civil and/or criminal action.

Users may be held accountable for their conduct under any applicable College policies. Any actions which deter other users from doing their work or which would otherwise be deemed malicious will result in the loss of access to the network and possible disciplinary action by Mount Saint Mary College and may include civil and/or criminal action.

Unauthorized use of the computing resources and the Mount Saint Mary network AND use for overt personal gain constitute theft under state and federal law and will be prosecuted by the College. Furthermore, anyone using the Mount Saint Mary computing equipment and/or network with the intent to breech security protocols or individually assigned passwords will be in violation of state and federal law and College Acceptable Use (ITC 2.6) and Data Security (ITC 2.8) Policies. Such individuals will be prosecuted to the fullest extent of the state and federal law and will face applicable College disciplinary action.

2.6.8 ACCESS AND/OR OWNERSHIP

The College owns the computers and networks that comprise the institutional information technology infrastructure. The electronic allocation of file space to a user does not assign legal ownership of the content. The College can access or deny access to data and/or files located on College owned resources. This does not relieve the College from understanding, protecting and properly handling intellectual property.

Files stored on University systems may be subject to disclosure under the U.S. Freedom of Information Act. In addition, it is the policy of the College to cooperate with all legally empowered investigations initiated by law enforcement agencies when presented with a legitimate court order such as a warrant or subpoena. As has been made abundantly clear in highly publicized legal cases, this may include archives of electronic mail sent or received. In addition, the contents of files on College systems may be inspected in the context of a duly authorized investigation. (See **2.6.6.16 Records Management)**

Anyone associated with the College (employees, students, consultants, contractors) leaving MSMC must turn in their issued devices. Requests to keep any issued devices must be approved by the Vice President managing the area from which the associated person left and must be based upon the need to provide continued services and/or support to the College or students of the College.

Anyone associated with the College (employees, students, consultants, contractors) leaving MSMC asking to access “personal” electronic files (including email) must request this through MSMC Human Resources (HR). If access is granted, a meeting will be arranged with the Office of information Technology (IT) to supervise the access. IT can choose to deny the acquisition of anything that appears to be property of the College or outside of the terms of the access defined by HR.