Q. Information Security Policies and Procedures

Overview
The Mount recognizes that information pertaining to students, faculty, staff, alumni, donors, and other members of the Mount community needs to be protected as a confidential asset of both the individual and the University. The Mount maintains appropriate administrative procedures and technical systems to limit both physical and electronic access only to those individuals who have a legitimate need for the information.

Scope
These policies and procedures apply to all individuals who have either electronic or physical access to data resources at the Mount. Data resources includes all items covered by federal, state and local laws relating to the use of electronic media, copyrights, security, pornography, obscenity, and privacy.

Responsible Use Policy
The Policy for Responsible Use of Information Technology at Mount St. Joseph University is as follows:

Mount St. Joseph University provides information technology and resources to support activities related to the mission of the institution. It gives students the privilege of access to the campus computer network and other information technology on the assumption that they will use them responsibly.

Irresponsible use, which includes but is not limited to: unauthorized revealing of passwords to others or inappropriate communication within social media, may result in loss of your network privileges and may lead to disciplinary action up to and including suspension or dismissal as defined in the University's Student Handbook.

All members of the Mount community, including students and employees, are bound by the mission of the Mount as well as by federal, state and local laws relating to the use of electronic media, copyrights, security, pornography, obscenity, and privacy.

The distribution of copyrighted materials using the University's network is strictly prohibited. In addition to actions taken by the University, illegal distribution of copyrighted materials may subject the user to criminal and civil penalties.

The illegal distribution of copyrighted materials using the University's network is strictly prohibited. In addition to actions taken by the University, illegal distribution of copyrighted materials may subject the user to criminal and civil penalties.

The distribution and safeguarding of student, employee, and customer information is protected by multiple federal laws and regulations including the Gramm-Leach-Bliley Act of 2003 (GLBA),

the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). All Mount school officials are personally liable for adhering to all federal, state, and local laws and regulations pertaining to the protection of covered information.

A school official is a person employed by the University in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the University has contracted as it's agent to provide a service instead of utilizing University employees or officials (such as an attorney, auditor, agency, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, and volunteers or persons assisting another school official in performing his or her tasks.

Responsible Use of Electronic Mail
The Mount's guidelines for the responsible use of electronic mail may be found at: https://mymount.msj.edu/ICS/Portlets/ICS/Handoutportlet/viewhandler.ashx?handout_id=5ff077ca-3ad9-4109-9f25-6576dbe019db

Peer to Peer (P2P) File Sharing Policy
H.R. 4137, the Higher Education Opportunity Act (HEOA), includes provisions designed to reduce illegal uploading and downloading of copyrighted materials through peer to peer (P2P) file sharing. The Mount's policy for P2P file sharing may be found at: https://mymount.msj.edu/ICS/Portlets/ICS/Handoutportlet/viewhandler.ashx?handout_id=84e9b27b-b265-4718-966f-ae13d312530a

Copyright Policies
The Mount's copyright policy for students may be found at: http://www.msj.edu/copyright-compliance

The Mount's copyright policy for faculty and staff may be found at: http://www.msj.edu/copyright-compliance-emp

Guidelines for Responsible Use of Social Media
The Mount's Social Media guidelines for students may be found at: https://mymount.msj.edu/ICS/Portlets/ICS/Handoutportlet/viewhandler.ashx?handout_id=2b4811bd-9292-4bec-95c6-e28ac1edd841

The Mount's Social Media Guidelines for faculty and staff may be found at: https://mymount.msj.edu/ICS/Portlets/ICS/Handoutportlet/viewhandler.ashx?handout_id=07ba8d98-431e-4d76-a59a-5cac3a677a6b

Record Access and Retention Policy
Access to student information is protected under federal, state, and local laws and regulations. The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the

privacy of student education records. Access to all student information, with the exception of directory information, is governed by and limited under FERPA.

Student rights to information and Mount employee responsibilities under FERPA may be found at: http://registrar.msj.edu/undergraduate-catalog/rights-policies/academic-policies/ferpa/

The Mount's record retention policy may be found at: https://mymount.msj.edu/ICS/Portlets/ICS/Handoutportlet/viewhandler.ashx?handout_id=50e55117-f6cc-449f-be14-ebfede8b9788

Forms and procedures for requesting access to information for new employees, for removing access to information for terminated employees, and for requesting changes in access permissions for existing employees are available only to employees on myMount.

External service providers utilized by the Mount are required to adhere to and maintain appropriate safeguards for all student, employee, and customer information.

An independent, external, comprehensive audit of the Mount's data network and information security policies and procedures will be periodically conducted to ensure the integrity of the information safeguards that have been implemented and to identify any gaps in information safeguards.

Physical Access to Campus Buildings

Procedures for requesting after-hours physical access to buildings on campus may be found at: https://mymount.msj.edu/ICS/Portlets/ICS/Handoutportlet/viewhandler.ashx?handout_id=af0aa9aa-2ba2-4d45-aae7-aed3f6bd1c28

Passwords

It is as important to protect your campus network privileges as it is to protect your computer equipment. Employees are required to change your password regularly and to never give your password to anyone.

Passwords must meet the following minimum requirements:

- Passwords may not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Passwords must be at least seven characters in length
- Passwords must contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)
- Complexity requirements are enforced when passwords are changed or created

Mount St. Joseph University's Information Services and Support (ISS) Help Desk will never ask for your password. Always protect your account logon ID and password.

Questions or Comments
Questions or comments regarding these policies and procedures should be submitted, in writing, to:

Mount St. Joseph University
Attn: Vice President for Information, Technology, and Strategic Planning
5701 Delhi Road
Cincinnati, Ohio 45233