MOUNT ALOYSIUS COLLEGE

INFORMATION TECHNOLOGY SECURITY AND OPERATIONAL PROCEDURES

Mr. Richard J Shea

10/6/2020

INFORMATION TECHNOLOGY SECURITY AND OPERATIONAL PROCEDURES

OVERVIEW

The purpose of this document is to protect authorized users of Mount Aloysius College from unauthorized access or modifications and to protect all computer related hardware and software from misuse by all users, authorized or not. Additionally, this document is to provide Mount Aloysius College with:

1. **Availability** -- Ensure that all network related hardware, software, information, and utilities are available and on-line to authorized users when they need them.
2. **Confidentiality** -- Assure that all data is viewed and/or modified only by appropriate individuals or departments.
3. **Integrity** -- Protect user information and data from unauthorized user modifications.
4. **Stability** -- Assure that system requirements, information access, and computer requirements are uniform and consistent throughout Mount Aloysius College.

SECURITY

To secure information at Mount Aloysius College, all student, staff, and faculty users are responsible for taking precautions to maintain the security of information stored on or accessed from their computer or account. By sharing accounts and passwords with other individuals, the user is then responsible for any data or network equipment accessed from that account and password. Failure to comply with this policy may result in Mount Aloysius College disciplinary procedures as well as criminal or civil prosecution.

Never share your password with anyone. You are responsible for any accidental or purposeful deletion of files or records resulting from your user ID. If you believe someone is using your ID and password, notify the IT department immediately so a new password can be created.

Terminals and computers should be logged off when unattended, and the office door should be locked and secured. If computers are unattended for 15 minutes, the computer screen will lock automatically so that the Novell Login screen appears. Making this part of your daily routine will provide the College with an added layer of security and prevent any unauthorized access to the College's computer system. By performing these simple procedures, you are forcing anyone who uses your computer to enter his or her own ID and password to gain access to the network.

The network and all computer systems are owned by Mount Aloysius College, and the College maintains the right to provide further regulation, as it deems appropriate, to limit use or access, deny access, and to monitor the systems for security purposes. Mount Aloysius College will respect individual privacy, but maintains the right to monitor the use of technology, including email. The College expects users to be responsible in their use of the system. **If the College determines it necessary or appropriate, monitoring of all resources may be instituted in order to ensure reasonable maintenance of hardware, software, data, network traffic or security.**

CONFIDENTIALITY

All information accessed through Mount Aloysius College's computer system should be treated as confidential information. Although some documents are considered more confidential than others, the best way to avoid problems is to treat all information as confidential. Access to any information is permitted to employees only if their job requires such access. In addition, all employees agree:

1. To access only information needed to perform their job.
2. Not to share passwords with anyone.
3. To assume responsibility for any access using their password.
4. To contact their supervisor if they feel their password has been compromised.
5. To assume responsibility for their failure to protect passwords or other access to confidential information.
6. That Mount Aloysius College may restrict access at any time.
7. That they will not make any unauthorized copies of software, forms, and print screens.
8. That they will not share any confidential information at any time even after employment has been terminated from Mount Aloysius College.
9. Not to use anyone else's password to access any system in the College.
10. Not to misuse or be careless with confidential information.

Failure to comply with this policy may result in Mount Aloysius College disciplinary procedures as well as criminal or civil prosecution.

PASSWORD

Password security violations are common to any network or computerized system. Any user who violates this policy will be held responsible for any disruption or damage to information or network performance. These violations will be considered a breach of security and disciplinary procedures as well as criminal or civil prosecution may result. All passwords will expire every 90 days and the system will force users to create a unique password at that time.

What could happen and how to prevent unauthorized access?

If you share your password with someone, this person will have access to all information and programs through the use of your ID. To prevent unauthorized access:

1. Never write down your password or post it near your work area.
2. Never share your password with anyone.
3. Never send your password over the Internet or via E-mail to anyone
4. Be smart in choosing a password. Do not use the following passwords because they are the first ones system hackers will try.

    1. Spouse.
    2. Last name.
    3. Phone number.

4. Any family member’s birthday.
5. Any anniversary dates.
6. Patterns of letters/numbers on the keyboard.
7. Interests, hobbies, pets.
8. Any family member’s name.
9. Any part of your Social Security number.
10. Any words or codes posted around or next to your workstation.
11. Any of the above spelled or listed in reverse order.

Recommendations for passwords are:

1. Easy to remember so it is not necessary to write down.
2. Chose a password so that it can be typed quickly.
3. Use combination of numeric and alphanumeric characters
4. Incorporate special characters. ! @ # $ % ^ & *

Examples of good passwords are:

1. sun*shine (the word sunshine broken up by *)
2. ttls&h (a phrase or saying - twinkle, twinkle, little, star, how&)

RESETTING OF PASSWORDS

If users become locked out due to using up all their grace logins, users are to call the Information Technology department. The Information Technology department can increment the number of grace logins allowed and instruct the user to follow the instructions on the screen to change his or her password.

As the 'custodian' for Mount Aloysius College information resources, The Information Technology Services Department has recently adopted the policy to not change or reset computer passwords without positive proof of identification. This policy change is being implemented for two reasons:

(1) it has become necessary to address increasing incidents of electronic identity fraud, and
(2) recent IT audits are requiring improved password security procedures.

4.0 MAC Password Resets
A student's Mount Aloysius College network password can be reset, but only under the following conditions.

4.1 Valid Cause
Before a MAC password can be reset, the student must show sufficient cause for such action. If the current password has been forgotten, a regular password change has been attempted and failed, or the account is believed to have been compromised, the password can be reset.

4.2 Identification Requirements
Once sufficient cause has been shown to exist, a password reset may take place. To have a password reset, the individual must contact the Help Desk office in Main 327 in person, or via telephone at (814)886-6502. The individual must also present his or her University ID card or state photo identification, either to the Help Desk staff, to a Faculty or Staff member, or via fax at (814)886-9548.

4.3 Reset Procedure
In the event of a password reset, the password will be temporarily reset to the eight-digit student ID number associated with the login ID. The MAC-ITS staff *CAN NOT* disclose student ID numbers.

NOTIFICATION OF NEW EMPLOYEES

The Human Resource Manager will notify the Director of Information Technology via Email of any new employee to Mount Aloysius College. The IT Director will meet or contact the appropriate supervisor and discuss account access, privileges, and rights to data in the system. The IT department will be responsible for creating the new account and assigning rights to data in the computer systems and the phone system. Adjunct and part time employees are not automatically given computer accounts and email. Computer accounts/email for part time or adjuncts need to be requested from the IT helpdesk by their supervisor or department head. The IT department will verify employment with HR before creating account. Once the account is created ITS will notify the supervisor or department head of the new account information.

NOTIFICATION OF TERMINATIONS

The Human Resource Manager will notify the Director of Information Technology via Email of any employee terminating employment. Depending on the account and information located in the account, the IT Director will meet with the appropriate supervisor and discuss options for movement of data to another account if necessary. The IT department will be responsible for removing all access and rights to all computer systems and the phone system. The HR Department has the ability to disable an employee's account simply by checking a box in the Jenzabar system.

NOTIFICATION OF TRANSFERS

The Human Resource Manager will notify the Director of Information Technology via Email of any employee transfer to another department. The IT Director will meet with the appropriate supervisor and discuss the necessary rights and accesses needed for the employee to perform his/her job at the new position. The IT department will be responsible for changing access and rights to all computer systems and the phone system.

NAMING CONVENTIONS

All accounts will be created using the three initials of the employee/student name followed by ending qualifiers. These qualifiers are as follows:

OP . information technology staff

AD . admissions staff

SA . student affairs staff

AA . academic affairs staff

PI . public information staff

PO . president staff

FO . financial aid staff

BO . business office staff

BS . bookstore staff

LI . library staff

FA . general faculty

ST . student

NU . nursing staff and faculty

SC . security staff

IA . institutional advancement staff

CA . CASS staff

EE . educational enrichment

SR . Sisters of Mercy

PT . physical therapy staff

PP . physical plant staff

HS . health studies staff

RO . registrar’s office staff

CL . center for lifelong learning staff

KH . housekeeping staff

ST . student

Example: John W. Smith (faculty member) . JWSFA1

In the event of a duplicate, the number 1 will be changed to 2 and so on for additional users.

If any account is not accessed for a period of year (180 days), the account will be deleted. In addition, all unattended terminals will be logged off after a period of 1 hour.

BACKUP PROCEDURES

Server backups to magnetic tape are performed daily or weekly depending on the frequency of change to the information on a particular server.

All servers that contain data that changes on a daily basis including the NDS schema will be backed up to magnetic tape or disk to disk media.

Data is keep for a period of one week for servers.

All backup tapes as well as the disk to disk backup system are stored in a secured location on campus. Remote backup processes occur daily.

MASTER LISTINGS AND ADMINSTRATIVE PASSWORDS

Master listings of all internet protocol (IP) numbers, administrative passwords, and network diagrams are kept in a secure area on campus. Complete listings of server racks, wireless access points, router information, etc is also documented and stored in the same location along with any important licensing information, master program media, and vendor and/or representative contact information.

DISASTER RECOVERY

1.0 Scope and Purpose

1.1 Introduction

The personnel, equipment, software systems, and databases, which comprise the Computer Center, are necessary in order for Mount Aloysius College to function in an effective manner. The purpose of this plan is to provide guidance in recovering from any disaster, which might occur to minimize downtime and assist users in accommodating their critical processing requirements.

The reliability of computers and computer-based systems has increased dramatically in the past few years, and those computer failures that do occur can normally be diagnosed automatically and repaired promptly using both local and remote diagnostic facilities. Many computer systems contain redundant parts, which improve their reliability and provide continual operations when some failures occur.

Almost any disaster will require special funding from the college in order to allow the affected system to be repaired or replaced. This report assumes that these funds will be made available as needed. Proper approval will be obtained before any funds are committed for recovery. It is also important to realize that this document will never be a fixed, finished document. It will continue to evolve and get better as time passes so periodic modifications will be necessary as equipment, software, and personnel change.

Also included in this document is a master password and IP listing which is located in the IT office.

1.2 Objectives/Constraints

A major objective of this document is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction of the central site or from minor disruptive incidents. **It is accepted that "business as usual" will be suspended at the time of a disaster, and that each office should develop their own plan to deal with manual operations within their office should computer and/or network services be disrupted**. Due to cost factors and timing of this document's creation hot sites and contracts with disaster recovery companies are not considered at this time. These will be considered as this document continues to develop.

This document does not plan for any "forms" that are essential for normal business operation. It is recommended that each department maintain copies of all forms off site. These forms include payroll checks, AP checks, and all other various "forms" that are not created by the college computer systems.

1.3 Authority/Assumptions

The decision to implement disaster recovery procedures is the responsibility of the Director of Information Technology (IT) or his/her designee. In his/her absence the most senior member of the IT staff will assume responsibility. Once an incident, which is covered by this plan, has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper college authorities are notified.

1.4 Distribution

One copy of this plan will be kept with the backup tapes off site and the second copy will remain in an electronic format on the server. Considering the size of the college and IT staff, the goal is to limit the number of outdated hard copies in existence.

1.5 Contingencies

The following are situations that can destroy or interrupt computer and telephone services:

Power/Air conditioning Interruption

Fire

Water

Weather and Natural Phenomenon

Sabotage

With each of these situations, one or more of the following three categories may exist:

Loss of information

Loss of access

Loss of personnel

As with each of these situations, there are varying levels of severity, which necessitate different strategies and different types, and levels of recovery. This plan covers strategies for:

Partial recovery – operating at an alternate site on campus and/or other areas on campus

Full recovery – operating at the current central site and other areas, possibly with a degraded level of service for a period of time.

2.0 Current safeguards

2.1 Physical security

Digital electronic locks are installed on the two main computer rooms located in the main building which house all servers. Employees gain access to these rooms via a code, which is keyed, into the keypad. To further secure the area, individual security guards are given codes to gain access to the room and not a key. There is also ID badge access that is controlled through the Security department. All other employees that need access to this room are restricted by a time of day feature, which is programmed into the locks and the badging system. Security cameras are also in the hall as well as at the door to the server room itself.

The DEMARC room is located in the basement of the main building which is the college entry point for all telecommunications and other outside services. This room is also the main distribution center for all fiber optics to each building on campus. This room is always locked with keys given to security and IT department.

Large matrix UPS supplies power to all computer equipment in the computer room and network switch areas to prevent surges/brownouts in electricity. Generator supplies power to the DEMARC room and the server room in the event of a power outage. The generator runs a full load test every Tuesday morning at 7am.

2.2 Environmental security

Central air conditioning supplies the main computer center. An automated calling device is also utilized in the server room. This device will call a series of home and cellular phones in the event of a high heat condition, loss of power condition, or high noise level. Fire extinguishers are also available in the server room.

2.3 Data security

Nearly all the servers are utilizing RAID 5 technology and contain a "hot spare" drive for easy replacement of a damaged disk. Redundant power supplies are installed and backups of all data to media are performed daily. This is done remotely and transmitted to a secure building on campus.

All network switches as well as the phone switch are leased and have support and maintenance agreements associated with them. Servers on the other hand are not leased but are closely monitored for degradation and replaced every 3 to 5 years.

3.0 Disaster Preparation

This section outlines the minimum steps needed to insure a full recovery from a disaster.

1) The disaster plan must be kept current and all of the personnel on the recovery team must be made
aware of any changes.

2) The offsite storage area should be inspected periodically to insure it is clean, organized and that the correct backups are in storage.

3) The fire fighting system in the computer room should be inspected regularly.

4) As many department heads as possible should be aware of the consequences of a disaster and what they can do while recovery is in process.

5) The physical plant and security department should have the telephone numbers of pertinent persons to contact in the case of an emergency occurring during off-hours.

6) Procedures and lead times for replacement equipment and communications should be established.

7) All computing personnel should be informed of the proper emergency and evacuation procedures.

8) Procedures for informing user community should be established.

9) In the event that there is a warning of an impending disaster the following steps should be taken:

   Notice should be given to as many recovery team members as possible

   The IT Director should be briefed and a decision made to shutdown the system.

   The recovery team should convene and review whatever actions may be necessary.

10) In the event that there is no warning of a disaster, the IT Director should be notified as soon as possible.

4.0 Organize recovery team

The IT Director is responsible for organizing the team. The IT Director keeps home phone numbers as well as cel numbers with him/her at all times. Due to the size of the IT department, all members of the department are important members of this team. If for any reason the IT Director feels the need to seek special outside or third party contractual assistance at any time throughout this process, he/she may do so.

Prior approval from an appropriate college official must be obtained before making any arrangements with outside vendors/consultants.

Once the team is gathered, prompt review of this document will take place, and the IT Director will assign duties to the team members in regards to their area of expertise. These duties include:

Review existing facilities

Review network switching equipment

Review servers and related hardware

Review telecommunication equipment

Review server software

Review client/server software

Gather backup tapes

List any minor supplies that will be needed to perform the above

A status report is then given to the appropriate college official once duties are assigned.

5.0 Assessment of damage

After gathering information on the extent of damage, the team is gathered to diagnose, evaluate, and recommend options to the IT Director. Time is always a critical factor in recovery so options to reallocate hardware to accommodate priority offices should be considered at this time. These offices are those that exist in the main building and thus receive a priority during the recovery process.

After evaluating the damage and a plan for recovery is established, status of the process is reported to appropriate college official. If outside vendors/consultants are contacted and participating in the recovery, all material and information must be reviewed with them.

6.0 Implement recovery

During the recovery process the IT Director oversees implementation and communicates with all outside vendors/consultants during the process. Daily status reports are communicated to the appropriate college official. During each phase of recovery the IT Director is responsible for making all final decisions during disagreements among team members and/or vendors/consultants.

7.0 Recovery timetable

The following timetable does not take into account the amount of time required to input data held on hardcopy during the recovery period, or re-inputting data which may have been lost during recovery.

Day 1 – 2 Convene the disaster recovery team and access damages. Begin to contact vendors which the college has support and maintenance agreements.

Day 3 – 4 Replace damaged equipment and begin installation/recovery of software.

Day 5 – 6 Restore partial operation to priority departments.

Day 7 – 14 Take delivery and setup additional replacement equipment. Restore full communications and network capabilities. Communicate with other departments to verify data and operation of applications.

8.0 Yearly plan review

Every December the Disaster Recovery Team will be convened to review the plan. Items to review are but not limited to the following:

Outstanding issues currently in the report

Verify that backup storage facilities are adequate

Verify that master password and IP listings are current

Modify the plan in the event that new hardware is added

Modify the plan in the event that facilities are changed or added

COMPUTER USE POLICY

Purpose

To ensure that all users can effectively share Mount Aloysius College computing resources for academic, administrative, public service or academically related communication purposes, this policy is intended to delineate the responsible use of information technology at Mount Aloysius College. Information technology includes, but is not limited to, computer networks, network servers, personal computers, printers, workstations, mainframe computers, software, e-mail, voice and video networks, transmission systems, and digital information. The College only for activities that support research, education, or administrative purposes allocates these computer and network resources. All office, campus network and Internet activities must be consistent with that purpose.

Scope

This policy applies to all students, faculty, and staff of Mount Aloysius College and to all other users who are authorized to access information technology at Mount Aloysius College. This policy is meant to augment and support existing College policy and also extends to use of those external networks with which Mount Aloysius College is interconnected, including, but not limited to, the college's present Internet service provider. For further information on the college's Internet service provider please contact Computer Services.

Authorized Use

An Authorized User is one who has been granted authority by Mount Aloysius College to access its computing and network systems and whose usage is consistent with this policy. Unauthorized use is strictly prohibited. The terms "authorized user" and "user" are hereinafter used interchangeably.

Privacy

All users must maintain confidentiality of **student information** in compliance with the Family Educational Rights and Privacy Act of 1974 (20 USC 1221 note, 1232g.) But users must recognize that there is no guarantee of complete privacy with their use of Mount Aloysius College computer and network systems. The College may find it necessary to view electronic data and it may be required by law to allow third parties to do so (i.e. electronically stored data may become evidence in legal proceedings). It is also possible that others may inadvertently view messages or data. Should the security of a computer system be threatened, the system may be monitored and user files may be examined. (Electronic Communications Privacy Act, 18 USC 2701-2711).

Statement of Responsibility

Access to the College's computing services is a privilege guided by the Honor Principle. It is assumed that users accept responsibility for their actions and how their actions affect others in the community. Users also accept the responsibility to abide by the policies of the College as well as any state or federal laws that pertain. Those who do not abide by the policies listed below risk disciplinary action or criminal prosecution under state or federal law.

Policies

All users are responsible to respect and value the privacy of others, to behave ethically, and to comply with all legal restrictions regarding the use of electronic data. College computers or networks should **not** be used to: install, run or copy software without a license to do so; conduct commercial business; express animus or bias against individuals or groups; transmit offensive material such as obscenity, vulgarity or profanity, sexually explicit material, name-calling or cursing; guess or decrypt passwords of other users; deprive authorized users of access; secure a higher level of privilege than allowed by the College; read, copy, change or delete another user's files or software without his/her permission; gain unauthorized access to remote servers; libel, slander or harass any other person.

Examples of Computer Harassment include **intentionally using a computer** to:

- Annoy, harass, terrify, intimidate, threaten, offend, or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;
- Contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

- Contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection);
- Disrupt or damage the academic, research, administrative, or related pursuits of another;
- Invade or threaten to invade the privacy, academic or otherwise, of another.

Each user is responsible for the security and integrity of information stored on his/her desktop/laptop system and for not installing or copying copyrighted software without permission or license. Generally speaking, faculty and staff users should check with Computer Services before attempting to install software on College-owned desktop or laptop computers. Faculty and staff users should refer to the Guidelines for Software installations by Staff and Faculty for more information. **Students are not permitted to install software on college owned computer equipment**. Only Computer Services personnel are authorized to install software on network systems. Computer accounts, passwords, and other types of authorization assigned to individual users or groups must not be shared with or used by others without authorization. Users are responsible for refraining from acts that waste College computer or network resources, prevent others from using them, or compromise the performance of campus computers, peripherals and networks. Users should avoid any willful action that would:

- Damage or modify College owned hardware or software;
- Introduce computer "viruses" or other disruptive/destructive programs into Mount Aloysius College networks;
- Degrade performance of a computer system or network;
- Reconfigure College owned software or hardware to intentionally allow access by unauthorized users or deprive authorized users of access;
- Create unnecessary multiple jobs, processes or network traffic (examples would be prolonged use of Internet Chat, sending e-mail chain letters or mass mailings, unnecessary use of the "All Students" e-mail address, printing multiple copies of documents to avoid using coin-operated copiers).

Each department has the responsibility of enforcing these policies. All users and departments have the responsibility to report any observed or discovered unauthorized access attempts or other improper usage of college computers, networks or other information processing equipment to their Department Head, Computer Services or Campus Security. Computer Services will provide each department with the resources to enforce this policy and help with data backup procedures as well as virus protection.

Disciplinary Actions: Anyone found to have violated this Computer Use Policy may be subject to suspension of computer privileges and possible disciplinary action under College rules for misconduct. Offenders may also be subject to criminal prosecution under federal or state law. As an example, under Pennsylvania law, it is a felony punishable by a fine of up to $15,000 and imprisonment up to seven years for any person to access, alter or damage any computer system, network, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization (18 Pa.C.S. 3933(a)(1). Disclosing a password to a computer system, network, etc, knowingly and without authorization, is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five years, as is intentional

and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software (18 Pa. C.S. 3933 (a) (2) and (3).

GUIDELINES FOR SOFTWARE INSTALLATIONS BY STAFF AND FACULTY

In recognition that software installation is more complex today than it has ever been, most institutions are using installation guidelines. In the Windows environment, software can often install new versions of DLL (Dynamic Link Libraries) and alter system files besides creating other problems. Keeping in mind that Mount Aloysius is a unique environment in which faculty and staff need the freedom to install and try new software, text book files, and other software components (for instance browser plug-ins), the following Guidelines are issued for software installation by faculty and staff:

1. Software cannot be installed on any public access computer (i.e. computer labs and computer classrooms) without prior consent of Computer Services. Certain classes may receive blanket permission for an entire semester due to the nature of the class. This is the exception rather than the rule and will be approved by Computer Services.
2. Operating systems cannot be installed by users on any college owned personal computers at Mount Aloysius College. This will be handled through Computer Services.
3. Faculty and staff may install software and other files on their Personal Computers per the following:
    1. Faculty and staff must recognize that the software installation may cause poor performance or total system failure.
    2. All software must be properly licensed software in accordance with current software laws. Faculty and Staff also accept the responsibility for providing proof of such licensing in the event it is required.
    3. Computer services will only provide software support for approved software.

Software must be in compliance with the Computer Use Policy in all respects.

COLLEGE EMAIL POLICY

Purpose of the Policy

There is an expanding reliance on electronic communication among students, faculty, staff and administration at Mount Aloysius College. This is motivated by the convenience, speed, cost-effectiveness, and environmental advantages of using email rather than printed communication. Because of this increasing reliance and acceptance of electronic communication, email is considered one of the College's official means of communication within the Mount Aloysius community.

Implementation of this policy ensures that faculty, staff, and students have access to this critical form of communication. For the majority of faculty, staff, and students, this will not represent any change from what is currently done. However, it will ensure that all faculty, staff, and students can access, and be accessed by email as the need arises.

Scope

This College email policy provides guidelines regarding the following aspects of email as one of the College's official means of communication:

- College use of email;
- Assignment of email addresses;
- Use and responsibilities associated with assigned email addresses; and
- Email communication expectation.

Policy

1. **College use of email**
   Email is an official means for communication within Mount Aloysius College. Therefore, the College has the right to send communications to faculty, staff and students via email and the right to expect that those communications will be received and read in a timely fashion. The College's email system can be accessed on campus and off-campus if you have an Internet Service Provider.
2. **Account disabled**
   All student login accounts including email are verified with class registrations. If a student is not registered in any courses for a period of one year then, IT Services will disable the student account including email. If you graduate or leave the College be sure to remove any emails you may need to a non-campus email account.
3. **Assignment of email addresses**
   The Information Technology Services will assign all faculty, staff, and students an official College email address. It is to this official address that the College will send email communications. This official address will be the email address listed in College directories.
4. **Redirecting email**
   The College recommends that faculty, staff, and students use the College's email system however; faculty, staff or students may have email electronically redirected to another email address. If a faculty, staff or student wishes to have an email redirected from his or her official address to another email address (e.g., @aol.com, @hotmail.com) they may do so at his or her own risk. The College will not be responsible for the handling of email by outside vendors. Having an email redirected does not absolve a faculty, staff, or student from the responsibilities associated with communication sent to his or her official email address.
5. **Email communications expectations**
   Faculty, staff and students are expected to check their official email address on a frequent and consistent basis in order to stay current with College communications. The College recommends checking email twice a week at a **minimum**, in recognition that certain communications may be time critical. "I didn't check my email," error in forwarding mail, or email returned to the College with "Mailbox Full" or "User Unknown" are not acceptable excuses for missing official College communications via email.
6. **Educational uses of email**

Faculty may determine how email will be used in their classes. It is highly recommended that if faculty have email requirements and expectations they specify these requirements in their course syllabus. Faculty may expect that students' official email addresses are being accessed, and faculty may use email for their course accordingly.

7. **Appropriate use of email**
   In general, email is not appropriate for transmitting sensitive or confidential information unless an appropriate level of security matches its use for such purposes. In addition, it is suggested that important documents be sent with a return receipt. The following criteria relate to email use:

   - All use of email, including use for sensitive or confidential information, will be consistent with the Systems Security and Operational Procedures policy located on the intranet.
   - All use of email will be consistent with local, state, and federal law, including the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of email, including use for sensitive or confidential information, will be consistent with FERPA.
   - Communications sent to a faculty, staff, or student's official Mount Aloysius College email address may include notification of college-related actions.
   - Email shall not be the sole method for notification of any legal action.
   - The College campus-wide email system is designed for use by sanctioned clubs and organizations for mass communication only with prior approval of the Director of Student Activities. Students who use the system for personal conversations or in any manner that does not follow the guidelines above will be subject to disciplinary action.
   - E-mail messages that have been in the trash for 30 days will be automatically purged.
   - Students may also create personal web pages on sites.google.com with their Mount Aloysius e-mail account.

JENZABAR AND ABRA EMPLOYEE ACCESS SECURITY AND REPORT CREATION

Purpose.

The purpose of this policy is: 1) to provide protocols when granting access privileges for Mount Aloysius College employees in the Jenzabar and Abra software systems, and 2) provide a process for employees to request, review, and approve new report creation and existing report modifications that are completed by the Information Technology Department.

Scope

This policy provides a process, by which the Technology Department receives, creates, reviews, and obtains approval for employee access into Jenzabar and Abra and provides a formal report request and approval track for all reports from these systems.

Policy

Notification of new employees, dismissed employees, or employees that change job responsibilities on campus originate from the Human Resources Department. This email notification is

then documented in the Information Technology Department using the JENZABAR-ABRA ACCESS FORM. After the notification is sent the Information Technology Department will initiate this form with the employee's name and other relevant information. The form will be then sent to the office manager or department manager for completion and proper signoffs. If the access being requested is the responsibility of multiple offices then multiple signatures and approvals are required for access. Once this is complete the Information Technology Department will create the account with the permissions listed and file the form in the Information Technology Department office. A new form can be used at any time by the division or department head if he or she requests changes to a person's rights or access privileges.

A separate spreadsheet will be kept documenting all users of Jenzabar and Abra along with their current rights and privileges. These spreadsheets will then be reviewed annually by the office manager or the department manager for accuracy. The Director of Information Technology will provide these for reviewing by the managers.

Reports created from the Jenzabar or Abra system by the Information Technology Department also requires a signoff form to be utilized. The JENZABAR-ABRA REPORT REQUEST FORM should be completed by the person requesting the report. If the report request does not come from the office who is owner of the data then proper approval must be obtained by that owner before any work is started on the report. The owner of the data is defined as the particular office manager or department manager who is directly responsible for the entering, modifying, and maintaining the particular information being requested. If the information crosses multiple offices then multiple signatures and approvals are required.

JENZABAR-ABRA ACCESS FORM

Security and confidentiality are of great concern to Mount Aloysius College. This document is used to clarify your responsibilities and access to such confidential information. You are expected adhere to the following:

1) Mount Aloysius College Confidentiality Policy
2) IT Security Policy

Employee Name: Effective Date:

Department: Termination Date:

Modules that require access

Employee Signature Date

Office Manger or Supervisor Signature Date

IT Director: Date

JENZABAR-ABRA REPORT REQUEST FORM

Requested by: Current Date: Date report needed:

Describe in detail the purpose of this report and who will be viewing this report:

Define criteria by which data is to be pulled (is it by term, all students that are named Smith, etc)

List fields required to be displayed on this report (Id number, lastname, firstname, etc)

List how the report is to be sorted. Choose a field from above:

What format does the final output need to be in (Excel, PDF, etc)

----------Office Signoff----------

Requestor: Date:

Requestor's Office Manager: Date:

Signing this form indicates that the above request was developed per my specifications

REPLACEMENT OF COLLEGE COMPUTER EQUIPMENT

Most college computer equipment is replaced on a regular cycle (see exceptions below). The Goals of the replacement plan are to:

- assure that appropriate computing resources are available in public and departmental computing facilities, classrooms, and college offices to support the mission of the institution;

- assure that each faculty and staff member who uses computing resources in his or her position has a computer of sufficient capability to fulfill his/her responsibilities;

- implement minimum standards for computing equipment on campus;

- encourage planning and cost-effective installation of new equipment.

Computer equipment is generally replaced during the summer months (July 1 - August 15). As summer work continues to increase timing of upgrades are carefully planned and may not only occur during the summer.

IT Services informs faculty/staff as early as possible which computers will be upgraded/replaced. Hardware configurations for new equipment are prepared in April/May and individuals with equipment scheduled for replacement are notified of those details. Ordinarily new equipment is ordered to arrive at the beginning of the fiscal year.

College computer equipment on the replacement cycle is divided into three cycles. Best practices indicate that technology equipment are at least evaluated for replacement every 3 years:

Cycle 1 Budget years 2009-2010 == 2012-2013 == 2015-2016

Cycle 2 Budget years 2010-2011 == 2013-2014 == 2016-2017

Cycle 3 Budget years 2011-2012 == 2014-2015 == 2017-2018

<u>YEAR 1 CYCLE</u>

Academic Affairs, Student Affairs, HR, Faculty Secretaries, Campus Ministry leased

Infrastructure (hubs, switches, and router) leased

Main lab 212

Smart classrooms 1st group

T3 laptops 2nd group

<u>YEAR 2 CYCLE</u>

Administrative office computers leased

Replace multimedia carts

Phone system evaluation – VoIP was installed in July 2007 expected to last 6-8 years

without major replacements. Only normal maintenance fees should be paid and normal software updating done periodically.

Network printers (in all offices and faculty areas)

T3 laptops 3rd group

Smart Classrooms 2nd group

YEAR 3 CYCLE

Replace and labs 215, 217, and Buhl, Library Reference, Virtuoso lab

Perkins Grant – replaces AH 212 lab

Repurpose equipment recovered from lab replacement if possible

Replace scanners for faculty secretaries

T3 laptops 1st Group

Computers are not purchased from department operating budgets. Only special funds designated for computer replacement or equipment purchases may be used for this purpose. The Budget committee approves request from budget groups during the budgeting process. Certain departments or individuals obtain grants or have special budget allocations for computing equipment. Computers purchased with these grants or budget allocations will not be on the replacement plan unless approval is obtained from the budget committee at the time the grant is received or the budget is allocated.

Departmental Equipment

All college computers are maintained in a central inventory at the time a computer enters the inventory the replacement cycle, if any, is designated. Computers that are an integral part of a piece of scientific equipment, or are used primarily for research purposes, are not generally part of the replacement plan. Old equipment is disposed of by ITS, in accordance with all applicable laws and regulations.

Assumptions/Considerations:

If the equipment in question was purchased through a grant, the grant guidelines determine where and how the equipment can be repurposed. Should a grant not be renewed the assets purchased through the grant will be repurposed, disposed of, or replaced according to the College needs and the technology replacement cycle.

Grant-Funded Equipment

Individuals pursuing grants for computing equipment should discuss their plans with the ITS Director, Controller, and Senior Vice President for Administrative Services, as part of the budgeting process. Computing equipment that is acquired under grants will enter the inventory and be upgraded on a regular replacement cycle *only* if approved at the time of the application for the grant.

Faculty members teaching in various special curricular programs are, under certain conditions, awarded research, or startup, funds. These funds may be used to buy additional computers and printers. Such equipment should be ordered through the College purchasing process and will not normally be upgraded or replaced by the college, except through further use of research funds. If this equipment is to be on the computer replacement plan the faculty member must obtain a commitment, in writing, from the Senior Vice President for Administrative Services indicating this. Otherwise, the equipment will not be on a replacement cycle.

Printers and Other Peripheral Equipment

Network printers are provided in central locations for office staff and faculty. Individual desktop printers are not normally provided. Other peripheral pieces of equipment such as scanners are also generally provided in clustered locations instead of individual offices. Since these pieces of equipment are usually used intermittently, it is cost effective to do clustering which allows sharing of specialized technical resources.

Responsibility for Equipment

Each employee is responsible for taking reasonable safety precautions in regard to Mount Aloysius College owned computer equipment. Employees will be held responsible for damage to such equipment arising out of their negligence or intentional misconduct.

Upgrades and Renewal

For computer equipment on the replacement plan ITS staff members consult with users prior to ordering and installing new equipment to determine the current and anticipated equipment needs. Computers that are replaced are returned to ITS. ITS then reassigns the computers or disposes of them through the campus disposal process. Mount Aloysius College will not upgrade non-Mount Aloysius College computers.

TESTING OF EMPLOYEE COMPUTERS PRIOR TO DISTRIBUTION

Once a new computer arrives, the operating system setup prior to connecting to the network. Once this is complete, network connection should then be established. Please check with a member of the IT staff for direction as to what version of the Novell client to install. Please follow the instructions in this manual for client installs or the text file in the software directory.

The standard set of software to be installed, which are located in the “bin” directory include:

Internet explorer, Firefox, Google Chrome

MS Office (current version – check with IT staff)

Sophos Antivirus with latest DAT files

All necessary security patches

Printer drivers

Verify the following are functioning:

Sound card and speakers

Monitor

TCP/IP connectivity

Internal and external web browsing

All necessary security patches

Printers

Allow computer to run 24 hours prior to delivery

Additional software to be installed

Some offices require additional software. This software may include:

Jenzabar software

Library card catalog

Blackbaud

After delivering the computer, be sure to perform the "winipcfg" command to set the proper IP address. Ask staff member as to the proper number.

FACULTY - STAFF TECHNOLOGY PURCHASES

The ability of technical support staff to support multiple systems is limited. As the college continues to grow, supporting multiple versions of computer systems, each requiring different images, etc., is an impossibility, especially given the full-time staff available to support the college and the reliance on student technicians to provide the support. MAC-ITS has established hardware and software purchasing guidelines for computing in administrative work areas and in all academic learning environments.

The guidelines were created for the following reasons:

- Standard configurations ensure faster response time and faster troubleshooting time since all systems are configured the same. This results in easier configuration, management, troubleshooting, and upgrading.

- The ability of technical support staff to support multiple systems is limited.

- Provides a long-term working relationship with a mainstream computer vendor, which makes it more likely that special service or pricing can be obtained for faculty, staff and students.

- Eliminates variables that must be considered with applications development and deployment, network access, and hardware configuration/reconfiguration.

- Positions the college to run newer software without requiring upgrades. Thus eliminates future costs.

- To ensure that future IT department initiatives will have the necessary networking and computing capacity.

The hardware and software guidelines:

- The purchase of hardware or software can place demands on the disk space on one of the file servers and on the server backup system. MAC-ITS may require that additional disk or backup capacity for the server be purchased along with a hardware or software purchase.

- Some products may place extraordinary demands on the Campus network. In these situations the MAC-ITS must consider the entire college operation and to meet these increased network requirements. Network-intensive purchases may also require the purchase of network equipment/software to sustain such a demand on the network.

- MAC-ITS strongly recommends that no product be purchased without also buying a support contract for that product. It is the responsibility of the purchaser of the equipment to arrange for any necessary support contracts with the vendor or manufacturer.

- MAC-ITS must be consulted in any purchasing decision so that it can offer advice about the potential performance of the product with our current network.

- MAC-ITS strongly discourages the purchase of any product that potentially creates a security risk for any user of Mount Aloysius College.

- Equipment may also have special needs for air conditioning, electrical power, or other facilities services. Therefore early consultation with MAC-ITS is essential to ensure a smooth installation.

- Some purchases require server requirements that MAC-ITS does not currently maintain. To facilitate your request for hardware or software, MAC-ITS may also require a purchase of a server which will be located the MAC-ITS area.

Therefore, MAC-ITS must make all technology purchases and must be involved during the early stages of the purchasing decision for new software and hardware. ALL hardware and software requests must be approved by the MAC-ITS. It is the Departments responsibility to ensure product quality, best possible price, and observe all copyright laws.

MAKING A HARDWARE/SOFTWARE DECISON

Personal computers and laptops for staff/faculty have been standardized as well as the Office package. The standard PC is an HP desktop and Microsoft Office 2010. Although Microsoft Windows 7 is preferred Windows 8 is an option.

Replacement cycles are in place and computers are frequently re-distributed across campus.

COMPUTERS

The minimum standards as of 2013 for a desktop/tower are as follows:

- Dual core or higher
- Memory 4 Gig
- 17" Flat screen monitor
- Convertible tower/desktop
- 104 keyboard
- Mouse
- Windows
- CD ROM/DVD/RW
- 1 TB hard drive
- Video Card

- Sound Card and speakers
- Intel 10/100 NIC
- Four-year on-site support
- Approximate cost is $1500 (NOTE prices are subject to change)

LAPTOPS

The minimum standards as of 2008 for a laptop are as follows:

- Quad core or higher
- Memory 4 Gig
- Windows
- CD ROM/DVD/RW
- Modem
- 1TB hard drive
- Intel PCMICA Card or Integrated NIC
- Carrying case
- CAT 5 Patch cable
- Four-year on-site support
- Approximate cost is $2500 (NOTE prices are subject to change)

SOFTWARE

The standard software packages to be installed on these computers are as follows:

- MS Windows operating system
- MS Office 2010 (which includes Word, PowerPoint, Excel, Access) OR
- MS Internet Explorer
- Sophos Antivirus
- Novell Client
- Adobe Acrobat Reader

In addition to the above, computers that are used in the administrative office may include Blackbaud, or Jenzabar software.

PRINTERS

Although most printing is done to network printers across campus, there are three different types of printers that can be purchased:

- HP DeskJet – This printer is designed for colored occasional personal uses.
- HP LaserJet – This printer is designed for more heavy use.
- Xerox work center – This printer is networked and is designed for high volume printing. Envelope feeder, duplexer, or other additional features are extra.

OTHER PERIPHERALS

- 17" monitor approximate cost $270
- 19" monitor approximate cost $370
- Thumb drives, flash drives, pen drives, or USB Drives. The costs of these devices are proportional to the storage amount they can contain. The College will not provide funding for these devices.

GRANTS

As grants are awarded and technology is added to the College infrastructure and equipment, the replacement cycle will continue to be modified based on objective determinations relative to the inclusion of these technologies. It is anticipated that future funding sources will remain consistent with current funding experience, and the College will continue to seek additional grants and donations in support of technology initiatives. As information technology resource demands increase, prioritization of the competing technology requests will be essential and cost benefit analysis will become an integral part of resource allocations.

GOAL

Purchasing technology can be stressful as well as rewarding for everyone involved. This process is intended to alleviate the stress for you, the MAC-ITS staff, and the College network so everyone can benefit from the technology.

The MAC-ITS will have the first right to re-assign the use of the computer being replaced if it was purchased with College funds

TECHNOLOGY HARDWARE DISPOSAL GUIDELINES

Mount Aloysius College disposes of all technology hardware and software in accordance with federal, state, and local laws. Mount Aloysius College also ensures that sensitive information is protected when equipment is disposed.

Technology equipment is slated for disposal for the following reasons:

Exceeded useful life

Unable to upgrade

Damage and out of warranty coverage

Excessive maintenance cost

Replacement equipment is acquired

Most computer equipment is scheduled for evaluation/replacement every three years based upon the established purchasing cycle guidelines. When this equipment is slated for replacement the existing equipment should be disposed by the IT department.

It is sometime useful to repurpose this refurbished equipment. Repurposing will take place with the overall need of the College in mind. If the equipment in question was purchased through a grant, the grant guidelines determine where and how the equipment can be repurposed. Should a grant not be renewed the assets purchased through the grant will be repurposed, disposed of, or replaced according to the College needs and technology replacement cycle. Equipment that is repurposed is not placed on the College equipment replacement schedule and a clear understanding is that this equipment will not be replaced when damaged or defective.

The intent of equipment replacement and disposal is to ensure that the College has current technology equipment in the hands of College users. Equipment beyond this life may still function, however, users must be made aware that it is used equipment, performance will be degraded, and the equipment will not be replaced when becomes inoperative. Care should be taken when repurposing this equipment to avoid issues with user's expectations of the equipment, when the equipment is beyond its intended life.

WIRELESS POLICY

Background

The Mount Aloysius College wireless network is intended to be a convenient supplement to the wired network for general functions, including web browsing, and e-mail. Wireless "access points", located in certain areas on campus; allow suitably equipped and configured computers to make wireless connections to the campus network, including the Internet.

Because everyone using the same wireless access point shares wireless radio signals, the bandwidth available to each connection decreases and performance deteriorates as the number of user and traffic increases. Distance from the access point, building or objects shielding the access point, signal interference, quality of your equipment, battery power, and other factors may also impact performance. As such, the wireless network should not be expected to provide the same quality-of-service as the wired network. When reliability and performance are a must, the wired network should be used.

Applications that generate high network traffic do not work well on wireless networks and negatively impact performance for everyone connecting to the same access point. Peer-to-peer programs (i.e. KaZaa, Napster, or Bearshare) are not permitted on the wireless network. In addition, wireless networks are highly sensitive to overlapping frequencies and can present a risk to the integrity and security of the entire data network. To promote efficient and secure wireless network access, IT must be notified before any deployment of a wireless access point on campus. Therefore, no wireless access devices are permitted on campus without prior approval of the ITS department.

I. Introduction

The use of wireless networking provides a more versatile way to access the Internet and to use a laptop computer, broadening the scope of mobile computing. With the added benefits of a wireless network at Mount Aloysius College, there also comes additional responsibility. A wireless user must be aware of the inherent security issues that exist in any wireless environment. Caution must be exercised to ensure a safe, secure, and reliable computing environment. This document of policies and guidelines serves to address three key issues regarding participation in the wireless network at Mount Aloysius College:

1. Security concerns while computing in a wireless networking environment.
2. Proper computing habits that can be used to minimize any possible repercussions in using the wireless network and to provide a safe and protected computing environment.
3. Acceptable user conduct on the wireless or wired network and the penalties for misuse of the wireless network.

II. Wireless Networking Issues

It is important to understand the unique nature of a wireless network. While it is not necessarily true that a wireless network is less secure than a wired network, the differences in the infrastructure of a wireless network versus a wired network create areas of concern, which should be known by all prospective users.

The MAC wireless network relies on the industry standard 802.11n networking protocol, which uses the 2.4GHz radio frequency range. In other words, communication of data between the client side (you) and the wireless access point, or receiver, is broadcast over radio waves. This means that data is being transmitted in public airspace where the communication could possibly be intercepted by eavesdroppers.

The 802.11n standard supports encryption standards known as WPA SHARE (Wi-Fi Protected Access) and WEP (Wireless Encryption Protocol), which provides a certain

level of encryption for wireless networking communications. But, as with any technology, there are security weaknesses.

It is worthy to note that communications on a wired network can also be intercepted. But due to the broadcast of wireless communications in open air, the likelihood of client communications being intercepted is increased. Also, as with any networked computer, a computer on the wireless network will be open to possible unauthorized access from other parties on the Internet. If resources on the computer are shared, such as the hard drive, outside parities will be able to see the shared hard drive and may be able to access the share if improperly configured and not secured with a strong password.

Therefore, without the implementation of an encryption key, it is vital for users to understand that **DATA SENT AND RECEIVED OVER A WIRELESS CONNECTION WILL GENERALLY BE IN CLEAR TEXT AND UNENCRYPTED**.

MAC has created one non-secure or "open network" and one "secure/encrypted network". All MAC laptops and computers must be running the secure/encrypted wireless network connection. The non-secure or open wireless network is for guests to the College for occasional use. If any personal computer/laptop would need access to the secure/encrypted wireless connection, directions will be placed on the Portal web page under helpdesk. As newer and better encryption technology is developed IT Services will implement these services.

III. Proper Computing Habits

The dangers of unencrypted communications can be minimized through good computing habits. Using the guidelines below will decrease your risk.

1. When submitting a username and password on a web site, make sure it is SSL encrypted. SSL, or **Secure Socket Layer** , is an encryption protocol drafted by the Netscape Communications Corporation to protect data being sent back and forth between a client user and a web site. **MAC-ITS HIGHLY RECOMMENDS THAT WIRELESS NETWORK USERS DO NOT SUBMIT IMPORTANT INFORMATION SUCH AS PASSWORDS AND CREDIT CARD NUMBERS ON A WEB SITE FORM UNLESS THE WEB SITE FORM USES SSL ENCRYPTION.**
2. Turn off any drive sharing on a computer using the wireless network. If sharing of drives and files is necessary, use a password to protect the drive shares.

These same habits not only apply to wireless networks, **BUT SHOULD ALSO BE CONSIDERED WHEN USING STANDARD WIRED NETWORK CONNECTIONS AS WELL**.

IV. User Conduct And Network Guidelines

Mount Aloysius College desires to protect its users as much as possible, and therefore, deems it necessary to define what constitutes improper usage of the wireless network and policies that will be employed for the wireless network.

1. We reserve the right to limit bandwidth on a per connection basis on the wireless network, as necessary, to ensure network reliability and fair sharing of network resources for all wireless users.
2. We reserve the right to monitor and log communications on a per connection basis to ensure proper usage of network resources.
3. Mass emailing, or spamming, will not be tolerated on the wireless network. Such practices are an unnecessary use of bandwidth resources and are socially improper.
4. Running servers or daemons on the wireless network is prohibited. Such programs use an exorbitant amount of network bandwidth and resources.
5. Any attempt to break into or gain unauthorized access to any computers or systems from a wireless or wired connection is prohibited. Any type of unauthorized access to computer systems is an unlawful practice that is not condoned by Mount Aloysius College.
6. Any type of Denial of Service attack (DoS attack) using the wireless or wired network will not be tolerated. DoS attacks not only cause unnecessary usage of network resources, but also can also cause bandwidth and financial losses for other affected parties.
7. Running any unauthorized data packet collection programs on the wireless or wired network is prohibited. Such practices are a violation of privacy and constitute the theft of user data.
8. All other standard usage policies for Mount Aloysius College networks apply to the Mount Aloysius College wireless network.

STUDENTS, FACULTY, AND STAFF THAT USE THE WIRELESS OR WIRED NETWORK ARE ASSUMED TO HAVE ACCEPTED THE ABOVE RULES AND CONDITIONS REGARDING THE WIRELESS NETWORK.

STUDENTS VIOLATING THE WIRELESS OR WIRED NETWORK POLICIES WILL BE DISCIPLINED BY MOUNT ALOYSIUS COLLEGE PER DISCIPLINARLY GUIDELINES.

As the deployment and usage of the Mount Aloysius College wireless network progresses, MAC-ITS reserves the right to change the usage policies and guidelines as necessary, for the sole benefit of Mount Aloysius College students, faculty, and staff, to provide a safe and reliable computing environment.

ACADEMIC LAB SOFTWARE REQUEST

Prior to each Fall and Spring semester, Mount Aloysius College faculty must request the software that they desire to have installed on Mount Aloysius College academic lab computers for instructional use. This is in essence a "zero-based" request, meaning that each lab computer will be reformatted and started from scratch. Even if you had software installed this semester, faculty must make a new request in writing for that software each semester. All requests must be received one month prior to the start of each semester.

Once the software is installed on a "build computer" (a computer that will be imaged to all others), each faculty member that requests software will be called into the computer center (3rd floor main building) and verify that the software is functioning properly. A signoff will be required that all software components are installed and the software is functioning properly.

To request software installation in the labs, please submit an online submission to the Help Desk and indicate the software needed. A confirmation call will be placed to you when we receive the request. This confirmation is to notify you that we have received your request. If you do not receive a confirmation please call the Help Desk at 814-886-6502.

MULTIMEDIA CART GUIDELINES

Multimedia carts are located in Cosgrave, Pierce Hall, Academic Hall, and the Main building's designated storage areas for use by faculty and staff. Any department or individual that does not adhere to the following usage guidelines for the Mobile Multimedia Carts or that allows unauthorized usage; care or movement of the Units will lose the privilege of using them.

Reservations:

1) Signup sheets will be located with the faculty secretary for each building.

2) Please call Robin Omasta 886-6531 for use of carts in the Main building, Karen Eppley 886-6345for use of carts in Academic, Jeanine Farabaugh 886-6417 for the use of carts in Pierce Hall, and Cathy Trexler 886-6472 for the use of the cart in Cosgrave.

3) Reservations can be made on a "first come first served" basis only.

4) Reservations guarantee the availability of equipment of one class period or a maximum of four hours.

5) A single reservation is not to exceed 3 consecutive days.

6) If you sign out the cart for 3 consecutive days one week you will not be allowed to sign out the cart the following week. You must skip a week so that everyone has an opportunity to utilize the equipment.

Location of equipment:

* Three carts are located on the second floor of Academic Hall in room 218.

* Three carts are located on the second floor of Pierce Hall in room 210A.

* Three carts are located in the Main Building in room 227.

* One cart is located in Cosgrave room 110

* The above rooms MUST be locked at all times.

* Information Technology Services will visually inspect all carts at the beginning of each semester to ensure equipment is not missing or damaged.

Uses:

* This equipment has been purchased for and is intended for direct instructional uses only in the buildings to which it is assigned.

* All equipment on the carts is for campus use only.

User responsibility:

* Units must not be left unattended at any time.

* Personal files are not to be saved on the computer's hard drive.

* No additional programs are to be loaded without prior consent of the ITS department. Standard software will be installed as per the lab installation guidelines. Microsoft Office is included in this standard install.

* Units are for use only within the building in which they are assigned. Units must be returned immediately following the class.

* Units may only be used for presentation, not for development of material.

* Although the units are network/internet ready the classroom in which they are to be used must have active data connection. The user is responsible for calling the helpdesk to request the time, day and room to be active. 24 hour notice is required. Please keep in mind that not all rooms in the Main building have network access. Pierce and Academic do have network connections and just need to be made active.

* All equipment must remain on the cart at all times. Do not disconnect or remove equipment or cables from the unit at any time for any reason.

* Users are responsible for reporting any problems to the Helpdesk x6502.

NETWORK PRINTING

Mount Aloysius College has installed networked color printers available for use by staff and students for Mount Aloysius College **academic** purposes. Although suitable for printing multiple copies, printers are not copiers and no more than 10 copies of any document, Web page, assignment, etc. should be printed from any printer on campus. If multiple copies are required, copy machines are available for this purpose. Again, these network printers **ARE NOT** copiers so do not treat them as such. Copiers are available in the Library and Cosgrave.

The Color Printers are located throughout campus. Class times will be posted on the door to each lab. If there are no classes scheduled, you may login to the lab machine and print your material.

Additional network printing

Additional black and white network printers are available in the Library, Academic Hall, the Perkins lab, and Educational Enrichment.

Absolutely NO Personal use

Maintenance of these printers can get very expensive if the below policy is not followed. If cost (number of toner cartridges used) becomes prohibitive, the policy will become more restrictive. Please respect the equipment so it can remain in good working order for years to come. Additional maintenance to these printers will be required if they are abused. This inconvenience will impact all users and may include extended printing downtime, reassigning of printers, or removal of printers until repairs can be made.

Monitoring and restrictions

All printouts to network printers are monitored. If we notice large quantities of the same document, or several print jobs from the same user, in a short amount of time, we will remove your printing rights to Mount Aloysius College network printers. You will be notified via E-Mail if this occurs.

Mount Aloysius College Information Technology Department will provide plain paper only to the labs in the Main Building. The Library, Perkins, and Educational Enrichment will supply paper and supplies in their respective areas. If you would like to print on special paper, you will need to provide your own.

Each semester every student will be encouraged to use only the given allotment of 400 pages. This allotment is reset every semester in which you are enrolled. During any semester if your total number of pages reaches 350 pages, you will be sent a warning notification via your Mount Aloysius College E-mail account that your limit is rapidly approaching. You will receive this notice after every print job over the 350 mark, which you send to the printer. If you reach the 400-page limit, your printing services will be disabled automatically. You will be required to pay $10 to the Controller's office for an additional 500 pages or $5 for 250 pages. After you pay this fee please bring your receipt to the 3rd floor Information Technology Center in the Main Building to request the additional pages. Additional pages will not roll to the next semester.

This policy is to encourage you to be mindful of unnecessary printing and wasteful practices that we must all try to avoid.

Comments about this policy can be sent to:

Mount Aloysius College Administration

7373 Admiral Peary Highway

Cresson, Pa 16630

or email your comments to helpdesk@mtaloy.edu

Please include your full name in all correspondence

The Credit Card industry has developed guidelines and procedures for entities that gather credit card information for services or products. Mount Aloysius College must comply with these guidelines to be permitted to accept credit card payments.

CREDIT CARD PAYMENT GUIDELINES

Storage of Credit Card Information

Credit Card numbers are not permanently stored electronically on any College owned servers. This includes but is not limited to: word documents, excel spreadsheets, various administrative software systems, bookstore system, Email, or any other server.

Paper records of credit card numbers are obtained through various offices that include but are not limited to: Admissions, Institutional Advancement, Bookstore, and Controller's office. Offices are not to store electronic or physical copies of credit card numbers. All copies of forms are to be sanitized before storage. In addition, any office that receives facsimiles or other printed material with credit card information must protect against unauthorized access to these documents and must forward the documents to the Controller's office immediately. If copies are maintained for that office, all credit card information must be sanitized on the copy.

ONLINE FORMS

Online forms that transmit credit card information are sent directly to a designee in the Controller's office through Paypal or CashNet. These credit card number are scrubbed prior to arriving at the college. Once these forms are obtained, the credit card information is sanitized if displayed and forwarded to the appropriate office for notification. No form is forwarded with credit card information. It is the responsibility of the Controller's office to debit/credit the card and forward in a timely manner to the appropriate office. The Controller's office will follow its own policy regarding physical storage and disposal of these documents as per their auditing requirements.

SECURITY AWARENESS

Once a year the IT Director will issue an email and post in campus periodicals an Information Security Awareness document. This document will provide all users of the campus community with information security details.

SECURITY INCIDENCES

All security incidences are reported to the Information Technology Director. The IT Director is responsible for initiating the Incident Response Team.

RISK ASSESSMENT

Purpose

Risk Assessments are conducted to bring sense and identify weaknesses in current College practices that could jeopardize confidential information.

Background Overview

Risks to College information may come in many forms. Risks to information are mostly thought of as computer and server hacking, but a number of breaches in data often occur from within organizations. Some examples are the most common risks are when users leave passwords near workstations or leave confidential papers on desks in offices where students can see them.

When performing risk assessments, internal office practices should also be reviewed for unnecessary access to computer systems and information and leaving unlocked workstations unattended.

Process

The Information Technology Director will meet with office managers on an annual basis to review risks in their offices. These risks along with the mitigation will be documented and stored with the IT Director.

Risk Assessments should:

1) Take into account the potential adverse impact on the College's reputation, operations and assets.
2) Ensure full review and classification of College information assets by the level of security objectives assigned to them
3) Be conducted by departments on a periodic basis
4) Address the appropriateness and frequency of staff and management security awareness.

Risk Assessments are conducted to:

1) Determine the nature of campus electronic resources.
2) Understand and document risks in the event of failures that cause loss of confidentiality, integrity, or availability of information. These are primarily thought of as technological in nature but can be as simple as confidential documents not physically secured in offices
3) Identify the level of security necessary for protection of the resources.

Although IT risks are usually thought of as external in nature, internal risks also do exist. The purpose of this assessment is to establish guidelines and provide potential risks to information assets and information technology resources that support the College. Each department, however, should conduct its own risk assessment. The Business Office and Admissions Office have provided their own plan in accordance with the Gramm-Leach-Bliley Act (GLBA). These documents can be found in the policy area of the College internal webpage.

INFORMATION SECURITY

I. The designated employee for the coordination and execution of the information security plan is the Director, Information Technology Services at Mount Aloysius College. All correspondence and inquiries should be directed to the Information Technology Services (ITS) office.

II. The following have been identified as relevant areas to be considered when assessing the risks to customer information:

Employee Management and Training

Information Systems

Managing System Failures

Student Loans

Security Office

Admissions

Registrar's Office

Financial Aid Office

Residence Life

Student Health Center

Center for Lifelong Learning

III. The ITS office will coordinate with the offices to maintain the information security program. It should be noted that the ITS office is NOT the data owner but, the custodian of the data. The owner or office has the authority to grant or revoke access to data. The ITS office will provide guidance in complying with all privacy regulations. Each relevant area is responsible to secure customer information in accordance with all privacy guidelines. A written security policy that details the information security policies and process will be maintained and will be made available to the campus. In addition, the information technology department will maintain and provide access to policies and procedures that

protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information.

IV. Mount Aloysius College will select appropriate service providers that are given access to customer information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information. Contracts with service providers shall include the following provisions:

an explicit acknowledgement that the contract allows the contract partner access to confidential information;

a specific definition of the confidential information being provided;

a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;

a guarantee from the contract partner that it will ensure compliance with the

protective conditions outlined in the contract;

a guarantee from the contract partner that it will protect the confidential information it accesses according to the commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;

a provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;

a stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;

a stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Mount Aloysius College to immediately terminate the contract without penalty;

a provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and

a provision ensuring that the contract's protective requirements shall survive any termination agreement.

V. This information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the university's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance shall be done per the internal auditing schedule. Annual risk assessment will be done through the internal auditor's office. Evaluation of the risk of new or changed business arrangements will be done through the legal counsel's office.

INFORMATION SECURITY INCIDENT REPORTING

Introduction

Information Technology security and identity theft is and will continue to be a growing concern for everyone. Compromises in security can potentially occur at every level of computing. Security breaches have occurred at various institutions, businesses, and government agencies. From an individual's desktop computer to the largest and best-protected systems, incidents have happened throughout the world. These incidents can be accidental incursions or deliberate attempts to break into computer systems. They range from benign to malicious in purpose or consequence. Regardless, each incident requires careful response with its potential impact to the security of individuals and the campus as a whole.

For the purposes of this policy an "IT security incident" is any accidental or malicious act with the potential to:

* result in misappropriation or misuse of confidential information (social security number, grades, health records, financial transactions, credit card numbers, etc.) of an individual or individuals,

* significantly degrade the functionality of the information technology infrastructure of the Mount Aloysius College campus,

* provide for unauthorized access to college resources or information,

* allow Mount Aloysius College information technology resources to be used to launch attacks against the resources and information of other individuals or organizations.

In the case where an IT security incident is determined to be of potentially serious consequence, the responsibility for acting to resolve the incident and to respond to any negative impact rests with the College rather than individuals or departments. The College has established procedures and identified an IT Services Response Team (ITSRT). This response team consists of members of the IT services department supervised by the IT Director. This team is responsible for investigating alleged security analysis and required to report the findings to the Assistant to the President for Administrative Services. From this point incidents may be reported to law enforcement, other College offices, or other College officials.

This document outlines the procedures individuals should follow to report potentially serious IT security incidents. College IT staff members are responsible for securing systems, monitoring and reporting IT security incidents, and assisting individuals, administrators, and others to resolve security problems.

1. Reporting and Responding to IT Security Incidents

Individuals should attempt to stop any IT security incident as it occurs, if possible. Powering-down the computer or disconnecting it from the campus network will stop any potentially threatening activity.

Report IT security incidents to an information technology support professional. IT support staff will help you assess the problem and determine how to proceed.

1. Individuals should contact the helpdesk at extension 6502 or email helpesk@mtaloy.edu and report the incident. Provide as much information as you can if you suspect some information security incident occurred.
2. If the incident requires attention after business hours call the IT pager at 941-1587.

Following the report, individuals should comply with directions provided by IT support staff to preserve evidence of the incident and document details of the incident. Individuals should not take any retaliatory action against a system or person believed to have been involved in the IT security incident.

2. IT Support Professionals

IT staff have additional responsibilities. IT support staff should:

1. Respond quickly to reports from individuals.
2. Take immediate action to stop the incident from continuing or recurring.
3. Determine whether the incident should be handled or escalated to the IT Director.
    - If the incident does not involve the loss of confidential information or have other serious impacts to individuals or the College, the IT support person should:
        1. Repair the system, restore service, and preserve evidence of the incident.
        2. Document the incident and how it was resolved. Then provide the IT Director with this report.
    - If the incident involves the loss of confidential information or critical data or has other potentially serious impacts, the support specialist should:
        1. Contact the IT Director. The Director will assemble the ITSRT and will begin investigating the incident and develop a response plan to report to the Assistant to the President for Administrative Services.
        2. Contact the helpdesk and include the incident and documenting any actions taken thus far.
        3. Notify the appropriate college department or administrator that an incident has occurred and that the IT Director has been contacted.
        4. Refrain from discussing the incident with others until a response plan has been formulated.
        5. Follow the response plan from IT security incident team to:
            - Repair the system and restore service.
            - Preserve evidence of the incident.
4. Information support staff should not take any retaliatory action against a system or person believed to have been involved in the IT security incident.

Mount Aloysius College Music and Video Downloading Notification

Did you know that copyright infringement is against the law and by downloading music or videos you may be in violation of this law. "Intellectual property" or more in particular "copyright" covers most artistic works including, but not limited to: music, films, videos, and software. Title 17 of the United States Code recognizes that among other exclusive rights of the copyright holder of audio and visual works are the sole rights to reproduce, display, or perform their work. Furthermore, the Digital Millennium Copyright Act (DMCA) of 1998 sets forth higher penalties for copyright infringements performed via the Internet.

What you need to know when using the network and Internet at Mount Aloysius College?

As your Internet provider it is our obligation to inform you that illegal downloading of copyrighted material is not permitted. Network equipment is installed and in place in an effort to deter this type of downloading. While this technology is constantly changing, it is your responsibility to be sure that you are acting within the law.

The College network alerts the IT staff of users that use excessive bandwidth. This may be further investigated and your access may be terminated until a determination can be made as to the activity taking place. In most situations such as this, computers are infected with viruses or trying to act as a server for distribution of illegal downloading.

Peer-to-peer (P2P) programs such as LimeWire, BearShare, Bit Torrent, etc are file sharing programs that facilitate downloading of files. Be extremely cautious if you have any of these programs installed on your computer. These programs contribute to the spread of computer viruses and also may result in identity theft. That is to say that YOUR IDENTITY may be stolen by criminals using this software.

All campus computing falls under the guidelines of the Computer Use Policy. Be sure to read and follow it.

What are the consequences of downloading copyrighted files from the Internet?

1) Potential lawsuits by recording companies and copyright holders such as the Recording Industry Association of America (RIAA). In a recent case of RIAA vs. Jammie Thomas, Ms. Thomas was fined $2 million dollars ($2,000,000).
2) Your identity may be stolen.
3) Viruses or worms can be introduced on computers that use P2P programs.
4) Mount Aloysius College also reserves the right to enforce sanctions if violations are determined.

Where can you find out more information about copyright and music downloading?

http://www.campusdownloading.com/

http://www.copyright.gov/title17/

What legal sources are there for downloading files?

Please note that using a legal service such as those provided below DOES NOT PROTECT you from being prosecuted for illegal downloading or uploading with another program. Always review the terms and conditions of any site you use to download files.

http://www.apple.com/itunes/

http://www.amazon.com/music

http://www.musicmatch-10.com/

http://www.napster.com/

http://www.buymusic.com/

Vendor Management

It may be necessary at times to permit vendors access to certain areas of the network for the purposes of installation or testing of new hardware, software or other applications. Special accounts will be created for these vendors and limits will be imposed where reasonable so that they are only granted access to the permissions required to fulfill the job obligation. At the conclusion of their work these accounts will be disabled.

If special accounts are required to remain active for proper function of the task then the MAC IT Services department will modify the password AFTER the vendor has left or completed their work. This is to be done prior to completion signoff so that 1) vendor access is completely removed from system and 2) systems remain functioning with vendor access removed or reset.

College owned/purchased tablets or Ipad device

Revised 5/13/13

Purpose

The purpose of this policy is to provide guidelines and inform users of mobile computing best practices when using College owned tablets/Ipads and/or other mobile computing devices.

Guidelines

- Do not disable security settings on your device or install any apps that claim to "jailbreak" or "root" your device. Doing so may increase the risk of virus or malware infections and loss of data may occur. Read the description of the app in its entirety and email any questions to helpdesk@mtaloy.edu if there any concerns.

- All apps and software as well as the operating system should be regularly patched by the user of the device. Apps and software patches usually contain security patches and should be applied when updates become available.
- A passcode must be used to gain access to the device. This helps prevent unauthorized individuals from gaining access. In addition, idle timeout lock is also required to be set.
- If your device is lost or stolen or if you suspect it to be lost or stolen, email or call helpdesk@mtaloy.edu immediately. Devices owned by the College with a data plans can be remotely erased by the IT Department. This remote erasing of the device is to prevent the data which the device contains from being viewed and/or prevent identity theft of the user assigned to the device.
- Protect and know where your device is at all times.
- If connecting to Wi-Fi off campus you should only do so if passwords and encryption to the Wi-Fi is enforced. If encryption is not offered then any transmission of data could be intercepted which could lead to identity theft or other significant loss of College data. Do not process any College data through a non-encrypted open Wi-Fi.
- Confidential college data should not be stored on the device for privacy, security, and compliance reasons. Confidential data includes but is not limited to Social Security Numbers, credit card numbers (PCI-DSS), financial/banking information (GLBA), Health records (HIPPA), and all Student protected education records (FERPA) including but not limited to ID numbers, grades, etc. Be cautions of what you download to the device and where it is stored. Likewise, be cautious of what apps you install. These apps have access to a variety of data on the device and transmit this data freely back to the app developer.
- The College, through the Information Technology Services Department reserves the right to periodically inspect and audit the devices for proper security configuration and compliance.
- The devices are College property and should be treated as such and must be returned when asked.
- Do not lend your device to others. You are responsible for the device and the data which it holds.

Information Services Security Awareness Training

1. Purpose

The purpose of this policy is to ensure that all Mount Aloysius College employees with access to college data, are provided Information Security Awareness training in order to gain an understanding of the importance of securing the College's data. This policy and associated procedures establish the minimum requirements for the Security Awareness and Training controls.

2. Scope

This policy applies to all Mount Aloysius College employees, faculty and staff and identified College affiliates.

3. Definitions and Authority

"Security Awareness Training" educates employees about data and computer security. The training should educate employees about safeguarding data within institution and their own personal protection.

"Personally Identifiable Information (PII)" is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another.

"The Family Educational Rights and Privacy Act (FERPA)" is a Federal law that protects the privacy of student education records.

"education records" under FERPA, which - with limited exceptions - means all records in any format or medium that are directly related to a student and are maintained by the College;

"Health Insurance Portability and Accountability Act (HIPAA)" demands that all HIPAA covered businesses prevent unauthorized access to "Protected Health Information" or PHI. PHI includes patients' names, addresses, and all information pertaining to the patients' health and payment records.

"Gramm-Leach-Bliley ACT (GLBA)" Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

4. Policy

Mount Aloysius College is required to protect and safeguard college-owned electronic information and paper records. All employees regardless of access have a responsibility to safely use and handle student information. These College records must be protected and secured at all times and only a business or legal need should determine who can see or share any College owned information.

All employees are required to attend Security Awareness Training annually. Employees have 90 days to complete the training, or they will be deemed non-compliant with this policy. The security awareness training program is subject to yearly review and enhancement based on changes to the information security environment.