TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

Introduction

Eastern Mennonite University (EMU) provides a wide range of technology resources in order to support the educational mission and administration of the university. The Information Systems (IS) department provides and maintains the campus network, servers, e-mail, course management system, audio-visual resources, general and departmental computing facilities and laboratories, and institutionally-owned desktop and laptop computers. The IS department is organized as two collaborating teams:

- User Services: Provides support to the campus community with the operation of the Help Desk.
- Technical Systems: Designs, builds and maintains the technology infrastructure systems as well as custom web applications operating on EMU web servers. The Data Center is a significant focus of their work.

The systems provided by the IS department have become essential resources for academic and administrative uses for members of the campus community. As such, all members of the campus community are encouraged to use these resources, provided they respect the rights of others, abide by the rules and regulations of the university, and assume shared responsibility for safeguarding institutional data. Proper and fair use is essential for all to derive maximum benefit from them. Thus, the university has developed these IS policies.

These policies may be modified at any time. An annual review of these policies is performed each spring by the Information Systems Planning Committee (ISPC). ***Use of EMU technology resources implies consent to abide by these policies***. Users found in violation may be subject to penalties of varying degrees, including temporary or permanent denial of access to IS resources. Violators may also be subject to action by campus, civil, or criminal judicial bodies.

Guiding Principles

In making information technology resources available to all members of the campus community, EMU affirms its commitment to a free and open educational environment, conducive to learning and governed by legal and ethical principles. The university provides technological resources to faculty, staff, and students as important tools for research, innovation, classroom instruction, creativity, collaboration, and administrative tasks. In that spirit, the policies that follow are meant to promote responsible access to these tools while limiting abuses that may drain these limited resources.

EMU values the free flow of information. The university respects individual privacy, civility, and intellectual property rights. Because an open networked environment can be disrupted by abusive behavior and electronic information is readily copied, users of the university's resources are honor-bound to promote and protect these institutional values.

Under normal circumstances, university officials will not examine personal information transmitted over the network or stored on university-owned computers. However, the university reserves the right to monitor system resources, including activity and accounts, with or without notice, when:

- It is necessary to protect the integrity, security, or functionality of university technology resources.
- An account or system is engaged in unusual or excessive activity.
- There is probable cause to believe that policies, regulations, rules, or laws are being violated.

Additionally, the normal operation and maintenance of the university's technology resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities as may be necessary in order to provide desired services.

1. Information Security and Technology Code of Responsibility for Employees

All information maintained by Eastern Mennonite University (EMU) is subject to this agreement. It applies to all constituent records including, but not limited to, prospective students, students, alumni, employees, donors, contractors and vendors. The records may be in any form, electronic or otherwise, stored in manual systems, the Student Information System (SIS) or any other EMU-owned or controlled technology resources.

The security and confidentiality of this information affects all EMU constituents. Individuals with access to this sensitive information are in a position of responsibility to maintain that security and confidentiality. Any breach of this security and confidentiality will be strictly dealt with by university officials and may result in discipline up to and including termination of employment.

All EMU employees (e.g. full-time, part-time, adjunct, temporary, work-study, contractors, etc.) must read and periodically agree to the following *Information Security and Technology Code of Responsibility for Employees*.

Employees may be periodically prompted during the network login process to affirm this Code of Responsibility. A version, appropriate for signing, is available at http://www.emu.edu/is/policies/tech-code-of-responsibility-employee.pdf.

Eastern Mennonite University
Information Security and Technology Code of Responsibility for Employees

My use and continued use of the EMU network constitutes my agreement to the following:

1. I will abide by all EMU Information Systems (IS) Policies at www.emu.edu/is/policies.
2. I will not engage in prohibited activities, including, but not limited to:
   a. Using technology resources to threaten or harass others, even as a joke.
   b. Using, distributing or propagating chain letters.
   c. Knowingly distributing viruses or other malicious code.
   d. Attempting to gain access to computers or network accessible resources for which I am not authorized.
   e. Transmitting music, movies, or software in breach of copyright over the network.
   f. Hosting for-profit activities using EMU resources (e.g. selling items for personal profit, promoting a personal business—with the exception of advertisements in the eClassifieds system on www.emu.edu).
   g. Using the EMU network or other technology resources for criminal or malicious activities.
   h. Engaging in prohibited activities outlined in the EMU Community Lifestyle Commitment.
3. I will safeguard my account access to EMU systems by:
   a. Not allowing others to use my EMU accounts; nor will I use someone else's account.
   b. Securing my computer against unauthorized access, including using a password-secured screen saver.
   c. Not leaving my computer unattended without securing it by either logging out from it or using a

Eastern Mennonite University
Information Security and Technology Code of Responsibility for Employees

password-protected screen saver.

d. Using strong passwords[1] and not storing my password(s) in places where others can easily see them.

4. I will respect all copyright laws by not infringing upon copyrights[2].

   The Digital Millennium Copyright Act (DMCA) provides strict rules governing the use of copyright protected materials. [www.copyright.gov/legislation/dmca.pdf]

   EMU response to copyright infringement allegations

   When EMU receives notification of alleged copyright infringements, the computer owner (if computer is not owned by EMU) or the computer user (if the computer is owned by EMU) will face disciplinary actions outlined in the Responsible Use of Information Technology Resources Policy.

5. I will report any suspicious activity related to electronic equipment or information systems to my supervisor or the IS Help Desk.
6. I will safeguard the integrity and security of personal or confidential information by:
   e. Not knowingly including false, inaccurate or misleading data in records or reports.
   f. Not inappropriately sharing confidential information gained by my position, nor benefiting from it.
   g. Accessing information only to the extent I need it to perform my job responsibilities.
7. I will accept responsibility for ensuring the appropriate use and confidentiality of constituents' information according to the Family Educational Rights and Privacy Act (FERPA) and all other applicable federal, state and local laws and regulations.
8. I will properly secure and/or securely dispose of all documents containing EMU constituents' personal information (e.g. EMU ID numbers, Social Security Numbers, birth dates, addresses, and any other personally identifiable information). I will not store this data in cloud storage systems. If I store this data on a personally-owned devices (laptop, tablet, smartphone, etc.) I will secure it with strong passwords, encryption (where possible) and other measures as appropriate.
9. I will always ensure that my email is stored securely and I agree not to configure my emu.edu e-mail account to automatically forward to any other e-mail address.

Employee's signature _____ EMU ID# _____ Date _____

Employees may be periodically prompted during the network login process to affirm that by using the EMU network they are agreeing to this code of conduct.

Distribution: Faculty/Staff Handbook

[1] Refer to EMU strong password recommendation at www.emu.edu/is/wiki/index.php/Password#Royal_Password

[2] Examples of copyright infringement include: Downloading digital formats of music, videos or other electronic media resources and using/sharing them with others without copyright holder permission, using peer-to-peer networks or similar utilities to download copyright protected music, movies or software without permission from the copyright holder, using corporate logos or corporate owned photos without permission

2. Technology Code of Responsibility for Students

All Eastern Mennonite University (EMU) students who are granted accounts to any EMU technology system(s) must read and periodically agree to the following *Technology Code of Responsibility for Students*. Students may be periodically prompted during the network login process to affirm this Code of Responsibility. A version, appropriate for signing, is available at http://www.emu.edu/is/policies/tech-code-of-responsibility-student.pdf.

Technology Code of Responsibility for Students

My use and continued use of the EMU network constitutes my agreement to the following statements:

1. I will abide by all EMU Information Systems (IS) Policies at www.emu.edu/is/policies.
2. I will not engage in prohibited activities, including, but not limited to:
   a. Using technology resources to threaten or harass others, even as a joke.
   b. Using, distributing or propagating chain letters.
   c. Knowingly distributing viruses or other malicious code.
   d. Attempting to gain access to computers or network accessible resources for which I am not authorized.
   e. Transmitting music, movies, or software in breach of copyright over the network.
   f. Hosting for-profit activities using EMU resources (e.g. selling items for personal profit, promoting a personal business--with the exception of advertisements in the eClassifieds system on www.emu.edu).
   g. Using the EMU network or other technology resources for criminal or malicious activities.
   h. Engaging in prohibited activities outlined in the EMU Community Lifestyle Commitment.
3. I will safeguard my account access to EMU systems by:
   i. Not allowing others to use my EMU accounts; nor will I use someone else's account.
   j. Securing my computer against unauthorized access, including using a password-secured screen saver.
   k. Not leaving my computer unattended without securing it by either logging out from it or using a password-protected screen saver.
   l. Using strong passwords[3] and not writing them in places where others can easily see them.
4. I agree that it is illegal to download or share materials in violation of copyright law; that I will respect all copyright laws and that the following referenced documents define the enforcement processes relating to copyright violation allegations for the EMU campus community.
   a. The Digital Millennium Copyright Act (DMCA) provides strict rules governing the use of copyright protected materials. [www.copyright.gov/legislation/dmca.pdf]
   b. The Higher Education Opportunity Act of 2008 requires that EMU to disclose certain information to students. These are shown on the helpZone page (www.emu.edu/is/helpzone) using the HEOA P2P Disclosure link. It is important that all students read and understand this disclosure information.
   c. When EMU receives notification of alleged copyright infringements, the computer owner (if computer is not owned by EMU) or the computer user (if the computer is owned by EMU) will face disciplinary actions outlined in the HEOA P2P Disclosure and Responsible use of Electronic Files and Communications Policy.
5. I will report any suspicious activity related to electronic equipment or information systems to the IS Help Desk.

   Students will periodically be prompted during the network login process to affirm that by using the EMU network they are agreeing to this code of conduct.

Distribution: Student Handbook

[3] Refer to EMU strong password recommendation at www.emu.edu/is/wiki/index.php/Password#Royal_Password

3. Responsible use of Information Technology Resources

Policy Purpose

Eastern Mennonite University (EMU) expects all members of its community to use university-owned technology resources in a responsible manner. The university may restrict the use of its computers and network systems in response to complaints presenting evidence of violations of other university policies or codes, or state or federal laws.

Policy Statement

EMU seeks to enforce its policies regarding use of its technology resources to: protect the university against damaging or legal consequences; prevent the distribution of proprietary software or electronic copies of literary works in violation of copyright restrictions or contractual obligations; safeguard the integrity of computers, networks and data, either at EMU or elsewhere; and ensure that the use of technology resources complies with the provisions of the Community Lifestyle Commitment.

User Responsibilities

Access to technology resources and network capacity is a privilege to which all university faculty, staff and students are entitled. (Access may be granted to other individuals affiliated with the university or university personnel, as situations warrant and with approval from the director of Information Systems.) Certain responsibilities correspond with that privilege. These include those responsibilities listed below. Since no list can cover all possible circumstances, the spirit of this policy must be upheld, that is, any action that hinders legitimate computer usage or invades the privacy of another person or institution is unacceptable.

Use of EMU-Owned Technology Resources

1. All EMU-owned technology resources, including those located in remote sites, are for the use of EMU students, faculty and staff. University guests may request temporary access to computers in the library and public computer labs (see EMU Guest Access system).
2. Users must not abuse equipment and are asked to report any mistreatment or vandalism of technology or network resources to Information Systems (IS) staff (IS Help Desk, 540-432-4357) or to University Security (540-432-4911).
3. When using computers in labs, users should relinquish the computer they are using if they are doing non-essential work when others are waiting for a computer to perform course-related activities. Equipment should not be monopolized. Users should not use more than one computer at a time and should plan work so that the computer session is no longer than absolutely necessary.
4. When using computer labs, users may not disconnect any cables on computers or other equipment. When using any other EMU-owned computers users should contact IS Help Desk before installing software or making any changes to equipment connected to the computer.

5. Users are expected to respect other users and IS staff. Verbal or physical abuse of others, students or staff, will not be tolerated. A user must identify herself or himself fully (e.g., by showing an EMU ID card) upon request of any IS staff member, IS student employee or security personnel.
6. Users must respect all posted notices (such as those concerning hours of operation, printing, etc.) in computer labs.

Legal Usage

1. EMU-owned technology resources may not be used for defamation, theft, terrorism, spam, illegal or harmful purposes, including:
   - Threats to others.
   - Harassment of others.
   - Intentional destruction or damage to equipment, software or data.
   - Intentional disruption or unauthorized monitoring of electronic communications.
2. Software is normally distributed under three kinds of licenses: Proprietary, public distribution, and shareware. Unless otherwise indicated, users should assume that all software made available by the IS department is proprietary and may not be legally copied.
3. IS will not knowingly provide support for software that a user possesses in violation of its license agreement. IS staff will ask for proof of ownership before helping users with their software.
4. IS will not knowingly allow pirated software to be used on EMU-owned computers. IS will remove any suspect software loaded onto EMU-owned computers or servers.
5. IS will not knowingly allow use of EMU-owned technology resources (computers, equipment, network, etc.) for the illegal copying of digital media or files. Note: U.S. Copyright Law protects copyright owners from the unauthorized reproduction, adaptation or distribution of digital material, including the unauthorized use of copyrighted sound recordings (e.g., music files), video files and interactive digital software (i.e., video games).
6. Unless specifically provisioned by the software license, EMU-owned software may not be installed on non-EMU-owned equipment.

Ethical Usage

1. Users should not use EMU-owned technology resources or personally-owned computers connected to the university network for non-university, unsanctioned commercial activity.
2. Users should make no attempt to alter the condition or status of any EMU-owned network device in any manner.
3. Users should make no attempt to alter software other than their own or to copy software intended only for execution.
4. Users should not interfere with, interrupt or obstruct the ability of others to use the network or other EMU-owned technology resources.

5. Users should not attempt to connect to a host via the network without explicit permission of the owner.
6. Users should not provide, assist in or gain unauthorized access to university technology or network resources.
7. Users should not attempt to circumvent or defeat computer or network security measures.

Account Usage

1. Usernames are assigned to accounts for all EMU-owned systems that require authenticated access.
2. Royal Username is the username created for all EMU systems users. It is a permanent identifier assigned by Information Systems and cannot be changed unless extraordinary circumstances are judged to exist by the Director of Information Systems.
3. Account holders must use only their own username and password to access EMU-owned technology resources. Account holders may not allow others to use their usernames and passwords. The account holder is responsible for its use and all activity originating from that account at all times.
4. Account holders must protect their passwords and keep them confidential. IS requires periodic password changes. Any problem resulting from irresponsible use of a password (e.g., a password that can be easily guessed or oral or written dissemination of a password) may be treated as grounds for action against the account holder. Any attempt to determine the passwords of other users is strictly prohibited.
5. Account holders must not abuse any electronic mail, bulletin board, or communications system, either local or remote, by sending rude, obscene, or harassing messages (including chain letters) or by using these systems for non-essential purposes during the times when the computers are in heavy demand.
6. Account holders must identify themselves clearly and accurately in all electronic communications, meaning no anonymous postings. Unofficial mass e-mailings (i.e., spam) are prohibited.
7. Account holders must access only their own files, those that have been designated as public, or those that have been made available to them with the knowledge and consent of the owner.

Network Usage

The following are responsibilities that are particularly applicable to users of EMU's campus-wide network, including residence hall users. While the following items are geared toward on-campus usage, the same principles apply to accessing EMU network resources from EMU's remote sites or via the Internet:

1. Only devices that have been authorized through the Network Access Control (NAC) system may be used on the campus network, unless specifically authorized by IS department systems administrators. Users must not attempt to circumvent the NAC system.

2. The person established via the NAC system as the owner of that authorized network device is responsible for that device's use and all activity originating from it at all times.
3. Excessive or improper use of network resources that inhibits or interferes with use by others is prohibited and will be cause for action by IS, which may include restricting, limiting or disabling network access.
4. No device that acts as a server may be connected to the EMU network, unless specifically authorized by IS department systems administrators.
5. Internet Protocol (IP) and MAC addresses may not be forged or spoofed. To maintain smooth operation of the network, IP addresses used must be those assigned dynamically by IS, unless specific instructions are otherwise given by IS department systems administrators.
6. No device or service that provides remote access to the EMU network or its network-connected equipment may be connected to the network.
7. In no case shall the following types of servers be connected to the network: DNS, DHCP, BOOTP or any other server that manages network addresses.
8. Due to the serious negative impact on network availability created by improperly configured routers, all routers (except those configured and used by IS department systems administrators), or devices which function as routers, are disallowed.
9. Users are not permitted to set up wireless access points on the campus network due to significant operational conflicts with existing EMU-provided wireless devices. EMU provides wireless capability at many locations throughout campus, including the common areas of most residence halls. Check the online map for updates to locations providing wireless access (www.emu.edu/is/wiki/index.php/Wireless).
10. Wireless printers are not permitted to operate on EMU campus locations.
11. Users are not permitted to register their own domain names for systems on the EMU network.
12. Information Systems must be informed prior to acquisition of any domain name to be used by an entity in which EMU has an ownership interest. Unless extraordinary circumstances exist, Information Systems will register, administer and maintain all such domain names.

Personal Usage

EMU recognizes that its employees may occasionally make personal use of University owned computers and does not wish to prohibit such use altogether. The following procedures apply to personal data on EMU-owned computers.

1. Information Systems will not be responsible for the backup and restoration of non-work related data including: music, personal pictures, games and non-EMU-owned software.
2. Information Systems may ask that such data/software to be removed if it is hampering the function of the computer and the ability of the employee to perform his/her job function.

3. In the event the employee gets a new computer or hard drive replacement, Information Systems will not be responsible for the restoration of personally-owned data. It is recommended that employees store personally-owned data on personally owned external devices such USB/Firewire external drives.
4. User Services technicians performing the data transfer or computer configuration will have discretion in identifying personally-owned data.
5. As a general guideline, files in My Pictures and My Music, including iTunes, will be considered personally-owned data which will not be transferred to a new hard drive by Information Systems. Users will assume responsibility for this transfer should it be desired. Music, photographs, and videos used in scholarly work are exempt from this policy requirement.

Enforcement

Penalties for violations of this policy may include the following:

- Loss of access to all or some EMU technology resources, including disconnecting from the Internet and/or EMU network.
- EMU Student Life staff review for student cases and Human Resources department review for employee cases.
- Prosecution under applicable civil or criminal laws

Responsibility and Review

Responsible Party

Responsibility for this policy lies with the provost. Policy implementation is the responsibility of the director of information systems.

Policy Review

This policy is to be reviewed annually by the Information Systems Planning Committee (ISPC).

Distribution: Information Systems web site

4. Responsible Use of Electronic Files and Communications

Policy Purpose

Computers and network systems offer powerful tools for communication among members of the Eastern Mennonite University (EMU) campus community and of communities outside of the university. When used appropriately, these tools can enhance dialogue and communications. Unlawful or inappropriate use of these tools, however, can infringe on the rights of others. The university recognizes the complexity of deciding what constitutes appropriate use of electronic communications services. What is appropriate or inoffensive to some members of the community may be inappropriate or offensive to others.

Policy Statement

Members of the campus community are expected to be judicious in their use of technology resources. These resources must never be used for unsanctioned commercial activities, theft, fraud, invasions of privacy, distribution of illegal materials or distribution of copyrighted or licensed materials without appropriate approval. Individuals bear the responsibility to avoid libel, obscenity, undocumented allegations, attacks on personal integrity and acts of harassment.

The university may restrict the use of its computers and network systems for electronic communications in response to complaints presenting evidence of violations of other university policies or codes, or state or federal laws. Specifically, the university reserves the right to limit access to its networks through university-owned or other computers, and to remove or limit access to material posted on university-owned computers.

Data Protection and Preservation

Cloud computing services (like Gmail, Dropbox, Evernote, and MobileMe) and personal devices that store data (like laptops, smartphones, tablets, USB drives and SD cards) pose unique challenges for institutions. Staff and faculty appreciate these devices' and services' ease of use, low cost and ubiquity. But cloud services and personal devices also move EMU data beyond the institution's control, creating the opportunity for data theft, data breach and data loss.

To mitigate this risk:

- Confidential data—financial, employment, educational and health records, etc. (see below for further examples)—*must not be stored in cloud services or personal devices*[4]. Storing confidential data in cloud services or on personal devices is grounds for disciplinary action up to and including termination of employment.
- Non-confidential institutional data *must not be stored only in cloud services or personal devices*. We recommend storing data on network drives and copying only working files to cloud services, and then only temporarily. Information Systems is not responsible for data lost in cloud services.

[4] Exceptions may be made for personal devices that have been configured with strong encryption and strong passwords.

Examples of confidential data possibly stored within electronic or physical systems at EMU include:

- Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity such as name and address in conjunction with social security number, biometric records, ID number, birthdate, place of birth, mother's maiden name[5].
- Financial: Budgets, payroll data, account and transaction information, credit card numbers.
- Employment: Personnel records, employee evaluation forms, disciplinary records.
- Educational records: Records directly related to a student and maintained by an educational agency or institution such as enrollment records, transcripts, grades, attendance records, student ID number, disciplinary records[6].
- Health: Any information, recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual[7].

Privacy of Electronic Files and Communications

EMU recognizes users' reasonable expectations of privacy in information technology data generated automatically by computer systems and by voice and data network devices. Therefore, Information Systems (IS) management will disclose EMU systems data only under the following circumstances:

1. In response to a court order or other legal papers.
2. In the investigation of a legal or policy violation.
3. In the event of a health or safety emergency.
4. In specific instances of reasonable requests in the interests of the university, such as collaborative research with other institutions.
5. To maintain the operation and security of the campus network.

All requests for EMU systems data must be submitted through the director of information systems, who will forward these requests to the Vice President, as appropriate.

[5] Personally Identifiable Information (PII) defined in OMB Memorandum 07-16: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

[6] Information Systems recognizes that the Registrar's Office has declared certain kinds of information to be Directory Information which can be disclosed without notice as provided by FERPA. However, because any student can request non-disclosure of Directory Information all such information is considered "confidential data" for the purpose of this policy.

[7] Protected Health Information definition at hhs.gov website: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#protected

Requests must include all of the following:

1. Reason for the request, which must correspond to the disclosure rules provided by this policy
2. Who requests receipt of the data
3. Intended use of the received data

Description of Private Files

Electronic files stored on an individual's computer or in a folder on a file server where access is restricted to an individual's account are considered private and are to be viewed only by the original creator of the files unless otherwise designated by the creator. Access to such files by others is prohibited without just cause.

Faculty and staff should take steps to ensure that documents necessary to the operation of the university are available to those who may require them.

E-mail messages are considered private, to be viewed only by the original sender and designated recipient(s). Access to messages by others is prohibited without just cause or permission.

As a matter of principle and ethics, individuals bear the responsibility for assuring that e-mail messages, including attachments and previous appended messages, are forwarded only to parties whose interest is consistent with the purpose of and intent of the previous correspondents. If in doubt, obtain the consent of the original correspondents before forwarding.

Faculty, staff and students should be aware of the following considerations:

1. Data storage and electronic communications are not perfectly secure. There are software and physical limitations that can compromise security. IS tries to minimize such exposures, but risks exist.
2. Mail delivered outside of the university is notably insecure and should be treated like a postcard. It is possible that mail received by individuals may be redirected (forwarded) to another Internet site off-campus. Unless you know that the intended recipient of an e-mail message has not redirected mail to an off-campus site, you should assume the possibility that others may see the content of the message.
3. Deletion of files or e-mail messages does not guarantee the inaccessibility of those files and messages. Centrally maintained file-storage systems and e-mail systems are archived regularly. These backup procedures store files and e-mail messages in multiple off-site locations. Thus, even deleted files and e-mail may be available from backups taken months or even years earlier.
4. Information security depends upon individuals keeping their password secure. Anyone issued EMU electronic systems account(s) must have difficult-to-guess passwords and must not share these passwords with others. Guidance for choosing a password is available at helpZONE (http://www.emu.edu/is/wiki/index.php/Password).
5. Many off-campus Internet sites may record information you provide and divulge this to others without your prior consent. In some circumstances, information about you, your activities on the remote site, and information about your

computer may be recorded without your knowledge. Some remote Web sites may store information on your computer in the form of hidden files or "cookies." Caution and prudence are advised when providing any information you would consider confidential to unknown third parties.

Access to Private Files or E-Mail Messages for 'Just Cause'

Access to another individual's electronic files or e-mail messages on EMU systems is permissible only if there is just cause in the following situations:

1. If the creator of the files, or the sender/recipient of e-mail messages, has granted specific permission for another individual or individuals to view designated files and messages.
2. In the event of a significant e-mail system problem that prevents automatic delivery of e-mail and the e-mail message headers must be read by authorized IS staff in order to direct e-mail to the intended recipients.
3. In cases of suspected violations of university policies, especially unauthorized access to EMU systems, the director of information systems may authorize detailed session logging and/or limited searching of user files to gather evidence on a suspected violation.
4. In the event of a situation involving a member of the campus community which renders them unable to access files or messages considered essential for the continuation of university business, another individual may access the individual's electronic files and communications under the procedures set forth in the Emergency Access to Electronic Files and Messages section below.
5. In the event of a need-to-know emergency (suicide or homicide threat), access to an individual's files or messages will be governed by the procedures outlined in the Emergency Access to Electronic Files and Messages section below.
6. In the event that a local, state, or federal law-enforcement authority in the investigation of a crime, civil litigation, or regulatory proceeding produces a subpoena, discovery request, or warrant granting access to files or messages, following the procedures outlined in the Emergency Access to Electronic Files and Messages section below.
7. In the event of a financial or legal audit, following the procedures outlined in the Emergency Access to Electronic Files and Messages section below.
8. In any other instance, no access is granted to an individual's electronic files or messages without prior review and approval by the appropriate body as indicated in the Emergency Access to Electronic Files and Messages section below.

Emergency Access to Electronic Files and Messages

Emergency access to another individual's electronic files and messages is granted only under conditions noted in the Access to Private Files or E-Mail Messages for 'Just Cause' section above.

Before invoking any such procedure, the circumstance creating the need for access shall be reviewed in a timely fashion, access shall not take place without approval, and specific procedures and strictures may be recommended for each circumstance.

The persons involved in the review and approval process will vary depending upon the individual involved:

- The provost will assume review and approval responsibility in cases involving a faculty member.
- The director of human resources will assume review and approval responsibility in cases involving a staff member.
- The vice president for student life will assume review and approval responsibility in cases involving a student.

The IS department will work with the individuals mentioned above to determine if the needs of the university or third party requesting access outweigh the privacy concerns of the individual.

Persons directly examining files and messages on the individual's computer, mailbox or file-server space shall not include the individual's supervisor, adviser or teacher. Only the specifically requested file(s) or message(s) made by the requester shall be accessed.

The student, staff or faculty member will be notified that access has been granted to their files or messages unless there is sufficient and compelling reason not to have done so.

No other files or messages may be copied, transferred or forwarded.

IS personnel charged with the administration of EMU's technology systems and file servers take their obligations to protect individuals' privacy very seriously. The professional standards consistent with positions that require select individuals to have access to personal and sensitive information are strictly enforced. In accordance with general university policy, inappropriate use, access or sharing of confidential information is grounds for disciplinary action up to and including termination of employment.

Harassment

EMU seeks to enforce its policies regarding harassment and the safety of individuals, to protect the university against seriously damaging or legal consequences and to ensure that use of EMU technology resources complies with the provisions of the Community Lifestyle Commitment for maintaining order and the campus environment.

Categories of policy violations

Policy violations fall into three categories that involve the use of electronic communications. EMU technology resources may not be used to:

1. harass, threaten or cause harm to specific individuals *(for example, sending an individual repeated and unwanted [harassing] e-mail or using e-mail to threaten or stalk someone)*
2. impede, interfere with, impair or cause harm to activities of others *(for example, propagating electronic chain mail or sending forged or falsified e-mail)*
3. harass or threaten classes of individuals *(for example, posting hate speech regarding a group's race, ethnicity, religion, gender or sexual orientation)*

Reporting Violations

If you believe that a violation of this policy has occurred, make contact as follows:

- The provost will assume review and approval responsibility in cases involving a faculty member.
- The director of human resources will assume review and approval responsibility in cases involving a staff member.
- The vice president of student life will assume review and approval responsibility in cases involving a student.

There may be situations when the following additional offices will be contacted:

- EMU Health Services if an individual's health appears to be in jeopardy
- EMU Security office if an individual's safety appears to be in jeopardy
- IS department, if you are unsure how best to report it or are unable to do so through normal channels

Procedures for IS Department Personnel

Reports of violations should be handled as follows:

Inform the director of information systems, or if not available, an available IS manager. The IS director or manager will be responsible for ensuring that appropriate actions are taken to address the complaint.

IS department management personnel handling these matters must document the incident and any actions taken. This information must be protected as confidential material and may be subject to review by appropriate university authorities. It must be kept current, complete and correct, as well as maintained in a secure repository which is easily retrievable by persons authorized to access the information.

In exceptional cases, the priorities of protecting the university against seriously damaging consequences and/or safeguarding the integrity of computers, networks and data either at the university or elsewhere, may make it imperative that IS department management personnel take temporary restrictive action on an immediate basis. Prior approval by the appropriate university policy officer is to be sought whenever possible.

Copyright Protected Electronic Content

All members of the campus community must adhere to the provisions of the Digital Millennium Copyright Act (DMCA) and the US Copyright Law (Title 17, U.S. Code). Copyright is a form of legal protection for the creators of original works that include literary, dramatic, musical, artistic, filmed and other intellectual products. Copyright owners have a number of rights under current federal law that includes the right to control the reproduction, distribution and adaptation of the work, as well as the public performance or display of the work.

Copyright exists, without the need for a specific notice, in any original work which exists or is part of any perceptible medium of expression. These works may be displayable on computer screens. Computer software, music, books, magazines, scientific and other journals, photographs and articles are some of the things subject to copyright.

Subject to certain exceptions, it is a violation of copyright law to copy, distribute, display, exhibit or perform copyrighted works without permission from the owner of the copyright. Both copying and distributing are, by definition, components of electronic transmissions. Downloading music or displaying photographs without specific permission of the copyright owner is likely a violation of the DMCA.

Under the DMCA, EMU is permitted to immediately take down any infringing site/computer on the EMU network and block access to any infringing sites on other networks, upon proper notice from the copyright owner or upon actual knowledge of infringement.[8]

If EMU receives notification from a copyright owner or its agent alleging that a DMCA infringement has occurred, the following actions will be taken.

DMCA Violation Allegations Involving Students

IS will research the alleged violation and determine whether the offending address was present on the network at the alleged date and time. Information linking a specific device and corresponding user will be used to identify the person responsible for that device.

IS will suspend the student's Internet access. This will prevent file sharing while allowing them to access EMU resources. If, while the student's Internet access is suspended, another user account authenticates the computer to the Internet the owner of that user account will be subject to the same Student Life procedures as the student with the suspended user account.

Student Life will meet with the student to explain the situation and require that the student remove the peer-to-peer software and infringing content.

IS will restore Internet access after the student has removed the peer-to-peer software. The student will need to bring the computer to the IS Help Desk for confirmation that the software has been removed.

The first incident will be recorded in their Student Life file as a "warning" only. Subsequent incidents will be recorded in their Student Life file as infractions and the student will need to pay $25 to have Internet access restored.

DMCA Violation Allegations Involving EMU Employees

IS will research the alleged violation and determine whether the offending address was present on the network at the alleged date and time. Information linking a specific device and corresponding user will be used to identify the person responsible for that device.

IS will contact Human Resources and turn the allegation notification and information developed from the research over to them. Human Resources will handle the matter as a personnel disciplinary incident.

[8] These copyright descriptions are based on policy and content published by Johns Hopkins University. An extensive list of copyright questions and answers can be found at http://www.library.jhu.edu/researchhelp/general/copyright/index.html

Mass Electronic Mailing – to Off-Campus Audiences

The following procedures apply to anyone sending mass electronic messages to groups of recipients whose e-mail addresses include domains other than emu.edu.

SPAM CONTROL

The sender must be mindful of and respect provisions of the CAN-SPAM Act of 2003. There may be state laws that also apply to mass mailings.

While definitions vary, it is commonly accepted that for purposes of anti-spam legislation, an unsolicited commercial e-mail is any electronic message, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. Transactional or relationship messages, such as EMU announcements, and messages requested by or consented to by the recipient, are not considered unsolicited commercial e-mail.

While it is likely that most mass electronic mailings sent on behalf of EMU would not technically be covered by the CAN-SPAM Act of 2003, in the spirit of being good e-mail stewards the characteristics of CAN-SPAM compliant messages should be strongly considered for all EMU mass electronic mailings. The following table lists these characteristics along with compliant and non-compliant examples.

Compliance Checklist for Unsolicited Commercial E-Mail Messages

Requirement	Compliant examples	Non-compliant examples
Message must contain clear and conspicuous notice that it is an advertisement or solicitation.	"Notice: This message is a solicitation for….." "Announcing a new service."	"A message for you." "For your interest"
Message must contain honest (non-deceptive) subject line	"Solicitation" "Advertisement" "New service offering"	"Open this message now." "Urgent message… You must act now."
Display a clear and conspicuous notice of the opportunity to decline to receive future e-mail from the sender.	"Notice: You may choose not to receive future e-mail from us. To do so, please follow this procedure…."	*A message that does not contain the required notice.*
Contain a valid physical postal address of the sender.	The physical address for the sender of this message is "123 Anystreet, Hometown, USA" "Sender's postal address: 123 Anystreet, Hometown, USA"	*Missing or invalid postal address of the sender.*
Return e-mail addresses must be valid and functioning for not less than thirty (30) days after transmission of the original message, or… a functioning opt in/opt out choice must be available to the recipient.	The "from" field contains an active e-mail address that has assigned responsibility for reading. Or… A functioning opt in/opt out function is made available, by automated or manual means.	Inactive e-mail address, or… Lack of assigned responsibility to read the e-mail box, or… Lack of functioning opt in/out function, or… Failure of the return e-mail address to accept mail within the required thirty day period after the original message is sent.
Senders must not send additional e-mail to a recipient who has objected to receipt of additional e-mail.	Once an objection is filed, no further e-mail is sent to the recipient.	Failure to honor recipient objection.
Senders must not release e- mail addresses to third parties after an objection has been filed by a recipient.	E-mail addresses proposed for release to third parties, are scrubbed of addresses for which an objection to release has been filed.	Failure to "scrub" e-mail lists of individuals who have filed objections.
Senders may not send e-mail to an address that has been "harvested", "lifted", or formulated by automated means, or otherwise obtained from a website without the consent of	Senders refrain from sending mail to addresses obtained by indicated methods.	Sending a message to addresses obtained by indicated methods.

the owner of the e-mail address.		

Using EMU E-mail Server Resources

Whenever possible, Information Systems recommends using low cost third party mass e-mail service providers to send mass electronic mailings to off-campus audiences. Reasons for this include:

- Spam controls used today could erroneously flag our servers as possible spam sources if large numbers of messages are sent during short periods of time
- To guard against possible hi-jacking of EMU e-mail accounts we have implemented controls that monitor the number of total recipients receiving sent messages.

Users should seek advice from Marketing & Communications when they need to send mass electronic mailings to off-campus audiences.

Mass Electronic Mailing – to On-Campus Audiences

Consistent procedures are used for notification and processing mass electronic mailings to the faculty, staff and student constituencies. The university expects anyone sending mass electronic mailings to any or all of these constituencies to do so in accordance with the procedures outlined in this document.

EMU employs two forms of mass e-mail (broadcast) communication: Emergency and non-emergency.

- Emergency mailings go to all faculty, staff and students.
- Non-emergency mailings follow one of two tracks: 1) Specific constituencies (faculty, staff or students) or 2) General campus-wide distribution.

Emergency Broadcast E-mail

Depending upon the intended audience, emergency broadcast e-mail messages can be sent to three “urgent” groups (i.e. ”everyone”, “all students”, “non-students”).

Only designated employees are authorized to send e-mail messages to these three e-mail groups, as determined by President’s Cabinet.

Non-emergency Broadcast E-mail to a Specific Constituency

Non-emergency broadcast e-mail can be sent to specific constituencies (i.e “all students”, “non-students”, “all faculty”, “all staff”). With the exception of the “all students” group, you must be a member of the constituency in order to send a message to that constituency. Only employees are authorized to send e-mail to “all students”, with one exception: Upon annual registration with IS, special permission is granted to SGA and YPCA co-presidents to send messages to all-students.

Non-emergency Mailing for Campus-wide Distribution

Any employee who has an e-mail communication intended for broadcast to the entire university community can send it using the “everyone” broadcast list. However, before sending an “everyone” broadcast e-mail message, employees are

urged to consider alternative communication channels. These alternatives and details about how the EMU broadcast e-mail system works can be found in the IS helpZONE: (www.emu.edu/is/wiki/index.php/Broadcast_Communication)

Broadcast E-mail Digests

Users can elect to receive broadcast messages (all-students, non-students and everyone) aggregated to a single digest message that is delivered several times each day. Emergency broadcast e-mail messages are not included in the digest list aggregation process. Details about how the digest system works and how to activate it can be found in the IS helpZONE (www.emu.edu/is/wiki/index.php/Broadcast_Communication)

Personal Contact Information

To ensure that accurate student, faculty and staff personal contact information is available for contact purposes, students, faculty and staff are asked to provide personal contact information. This information (either residence address(es), telephone number(s), or both) may be requested to be private.

Personal contact information not requested to be private will be made available through the campus web directory. This directory is available only to students, faculty and staff. It is not available to the general public.

Personal contact information requested to be private will not be made available through the campus web directory. Only a small number of university personnel, designated by the President's Cabinet because of their functions, will have access to personal contact information requested to be private. Such personnel may use this information only to the extent that it is required for specific tasks of their job and they may not share it with others.

Responsibility and Review

Responsible Party

Responsibility for this policy lies with the Provost. Policy implementation is the responsibility of the director of information systems.

Policy Review

This policy is to be reviewed annually by the Information Systems Planning Committee (ISPC).

Distribution: Information Systems web site

5. Security of Information Technology Resources

Policy Statement

Information Systems (IS) designs, builds, maintains and administers the Eastern Mennonite University (EMU) campus network. Certain data security procedures are used to ensure that administrative data and technology resources are protected from vulnerabilities, and any device connected to the campus network is identified as to its type and user(s).

Policy Specifics

The EMU campus data network is subdivided into network segments to provide different network services depending upon the user's role. Administrative data and technology resources are limited only to connections with authenticated users and devices that are authorized to access these data and resources. A Network Access Control (NAC) system is used to gather information about any device connected to the network. This information will identify the type of device connected to the network and its user.

Network Access Control Procedures

1. EMU uses a network access control (NAC) system to control all user devices connected to the EMU campus network and to identify and authorize all users of devices connected to the network.
2. EMU's network is divided into segments, including those for these roles:
   - Guests
   - Students (using their personally owned devices)
   - Labs (for students using EMU-owned computers)
   - Faculty/Staff (for employees using EMU-owned computers
   - Special Purpose (for EMU-owned utility systems, e.g. HVAC, door access, security controls, etc.)
3. EMU's network segments have security measures in place to protect users and systems from inappropriate access (e.g., guests do not have access to administrative systems).

Network Security Procedures

1. The NAC system will be configured to ensure that all devices connecting directly to EMU-owned or controlled networks will meet a minimum standard of operational requirements for anti-virus protection and operating system types and security standards.
2. All persons who have non-guest access to the EMU campus network must annually read and agree to the provisions of the *Technology Code of Responsibility* agreement.

Data Backup Retention Specifications

IS performs backups of all user data stored on EMU-owned servers, except as indicated below. Backed up data files will be retained according to the retention counts for the category of data and interval specification in the following table.

DATA CATEGORIES	RETENTION COUNTS BY BACKUP INTERVAL		
	Daily Backups	Weekly Backups	Monthly Backups
E-mail	7	4	12
SIS Databases	7	4	12
Network File Storage	7	4	12
All Other Data Categories	7	4	12

Data Backup Exclusion List
• Data stored on student "Z:" drive

IS procedures ensure that the data backup files are protected from destruction, data loss and unauthorized access and that they are available, if needed, for recovery from a catastrophic failure of the primary storage devices.

Data Backup Repositories

Data backup occurs daily. Incremental backups are performed six days per week with a full backup on the seventh.

Backups are initially made to backup disk and copied to tape the following business day. That aids restore speed, while adding the protection of a tape copy. Tapes are moved from the tape device to a safe weekly. The backup disk, tapes and safe do not reside in the primary Data Center.

Secondary copies of all retained data are made quarterly and stored offsite in a safe deposit box. The quarterly backup procedure also includes device configurations, equipment lists and other documentation suitable for use in rebuilding the servers and storage area network in the event of a disaster that would require starting from scratch.

Responsibility and Review

Responsible Party

Responsibility for this policy lies with the Provost. Policy implementation is the responsibility of the director of information systems.

Policy Review

This policy is to be reviewed annually by the Information Systems Planning Committee (ISPC).

Distribution: Information Systems web site

6. Security of Electronic Administrative Information and Implementation Procedures for Gramm-Leach-Bliley Act

The Jenzabar Student Information System (SIS) is the primary data store of Eastern Mennonite University (EMU). The university has made a substantial investment in human and financial resources to obtain and manage this system. The following procedures have been established to protect this investment and the good reputation of the university, to develop data stewardship to safeguard the information contained in these systems, and to enhance the fulfillment of the mission of the university.

Further, the Federal Trade Commission (FTC) requires colleges and universities to establish polices and procedures for protecting information in compliance with the *Gramm-Leach-Bliley Act* (GLB Act). This act requires that financial institutions, including colleges and universities, develop plans and establish policies to protect customer financial information (customer information)[9].

Information Systems (IS) staff members are responsible for the administration of these security procedures, in accordance with all university information policies dealing with security, access and confidentiality of university records.

All users of the SIS and applications that depend on SIS data (e.g. myEMU, PowerFAIDS, etc.) are required to comply with these security procedures.

Information Security Plan

The director of information systems will be responsible for the coordination and execution of the Information Security Plan at (EMU).

Possible Internal and External risks to security

This section identifies anticipated threats to customer information including but not limited to unauthorized access, eavesdropping, electronic student record protection, non-electronic student record protection and disposal of information.

A list of possible threats to customer information follows; the list is not comprehensive. This plan has been created in part to mitigate the risks identified in the list:

- Unauthorized[10] read/write access through software applications.
- Unauthorized access to extracted or downloaded data.
- Unauthorized copying of data files.
- Weak password selection.

---

[9] *Covered data and information* for the purpose of this policy includes student financial information (defined below) required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage which is required under federal law, EMU chooses as a matter of policy to also include in this definition any credit card information received in the course of business by the university, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.
Student financial information is that information that EMU has obtained from a customer in the process of offering a financial product or service, or such information provided to the university by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format Source: Excerpted from document at http://counsel.cua.edu/glb/resources/baylor1.cfm (2/25/04)

[10] *Unauthorized access* is assumed to mean both internal and external access by students, faculty, staff and intruders.

- Improper protection of passwords.
- Unrestricted physical access to servers.
- Unrestricted physical access to storage media.
- Unrestricted physical access to networks.
- Unauthorized printing of data.
- Improper storage of printed data.
- Unauthorized viewing of printed data.
- Unauthorized viewing of computer displayed data.
- Unprotected documentation usable by intruders to access data.
- Improper destruction of printed material.
- Improper disposal of magnetic media.
- Uncontrolled changes in technology or configuration.
- Accidental viewing of data.

Information Systems (IS) Responsibilities

Electronic access to customer information

Access to Customer Information is protected by usernames and passwords. The IS department is responsible for the administration of all access controls for the SIS and will process activations and deactivations to user accounts upon receipt of a qualified request from the Human Resources

Requests to add or change access must include all required approvals for the appropriate level of access. Requests to deactivate access may be processed by an oral request from Human Resources prior to the receipt of the written request. Network Systems staff will periodically run processes that monitor employee status to ensure that former employees are deactivated.

Programmers and other technical staff with application or programmatic access to customer information are to be authorized by the director of information systems.

Resetting of SIS passwords is done only when a user is positively identified.

Network access to systems with customer information is controlled by restrictions on unauthorized networks and computers within routers or firewalls protecting these systems.

Access to systems with customer information over the Internet is secured by SSL encryption. All financial transactions over the Internet are likewise secured by SSL encryption.

Access to backup and test servers storing customer information is tracked, just like production servers.

Descriptive names for systems with customer information, which identify them as storing customer information, are to be avoided in public lists like Domain Name Service (DNS) records.

When a subset of customer information is downloaded or extracted from files or databases to a local computer, the computer is identified and protected with the same care as customer information on the original servers.

Physical access to customer information

Customer information media to which these procedures apply include hardcopy files, electronic files, servers, media and networks.

Production and backup servers with customer information are housed in secure areas. Access to core server area is to be authorized by the director of information systems. Only authorized staff have keys to the data center. Unauthorized personnel in secure areas are to be escorted by authorized personnel.

Access to networking equipment closets is restricted by lock and key. All network closet keys and the master key are kept in the computer center. Keys are signed out to IS employees under supervision of the director of information systems.

Lost or stolen keys to secure areas must be reported to the director of information systems and to campus security immediately. If there have been stolen or lost keys, the affected locks will changed.

Archival backup media is to be kept in a secured off-site location.

Media used to store customer information must be properly erased before disposal. Deleting files is not sufficient. Media must be, at a minimum, reformatted in a manner which prevents the restoration of deleted files.

Documentation handling

Administrative and network system documentation which can be used by intruders to discover the location of and/or methods of access to customer information will be handled by the same standards as customer information itself.

Passwords of systems with customer information must be mailed only in an opaque, sealed envelope.

Printed copies of documentation must be shredded when no longer in use.

Department Responsibilities

Data stewardship has, as its main objective, the management of the university's data assets in order to improve their usability, accessibility and quality. This is accomplished through the role of the department directors who have planning and policy level responsibility for data within their areas, and management responsibilities for defined segments of the institutional data. In the simplest terms, the data stewards are the “owners” of the data. Ultimately, data stewardship is the responsibility of departmental directors and their designees, in conjunction with IS staff.

Access to customer information is protected by usernames and passwords. In addition, the director of each department has control over who has access to individual areas. Authority to access customer information is given by the security officer or the head of the department. For example, in the case of financial aid information, the financial assistance director approves access to customer information on a person by person basis reflected by the privileges associated with the user’s account in the Financial Aid Office.

Supervisor and Manager Responsibilities

Supervisors and managers will:

- Provide appropriate support and guidance to assist employees in fulfilling their job responsibilities under these security procedures.
- Promote and provide appropriate data stewardship in their areas of responsibility.
- Work with the IS staff to create and validate proper authorizations for access to customer information for current and new employees.
- Create appropriate control practices, standards and methods designed to provide reasonable assurance that all employees observe these security procedures.

Department heads will e-mail the names of users who are no longer authorized to access customer information to helpdesk@emu.edu as soon as is practical.

Students with access to customer information must sign *Technology Code of Responsibility for Employees*. Signed copies of the *code* should be submitted to IS along with the access request.

All individuals with access to customer information will receive regular reminders of their obligations when they stop working with customer information.

Human Resources Responsibilities

HR will notify IS of employee new-hires, transfers and terminations in a timely fashion. Involuntary terminations will be reported concurrent with the termination.

Human Resources office will e-mail the names of users who are no longer authorized to access customer information to helpdesk@emu.edu as soon as is practical.

Training for faculty and staff

Training for new faculty and new staff will include, at a minimum, an explanation of the purpose of the GLBA, a synopsis of the GLBA, the contents of the Plan, their responsibilities stated by the GLBA and the use of encryption as a method of protecting transmissions of customer information.

Existing faculty and staff with access to customer information will receive the same training as new faculty and staff and be reminded, at a minimum, yearly of their responsibilities under the GLBA.

Oversight of Service Provider Arrangements

EMU 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 must include the ability of the service provider to safeguard customer information. Contracts with service providers must include the following provisions:

An explicit acknowledgment that the contract allows the contract partner access to customer information.

A specific definition of the customer information being provided.

A stipulation that the customer 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 customer information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' customer information.

A provision allowing for the return or destruction of all customer 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 the university to immediately terminate the contract without penalty.

A provision allowing auditing of the contract partners' compliance with the contract safeguards requirements.

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

Employee Responsibilities

Electronic information handling

Employees will ensure that all SIS access is requested and used for professional reasons and is required to fulfill the requester's current job responsibilities.

Employees will use and protect their personal user account passwords and privileges, and will not share those with other persons (employees or non-employees). Employees will use strong (hard to guess) passwords. Passwords will not be shared by users or within departments.

Employees will be responsible for the content of all SIS data that are transmitted over the Internet, sent through e-mail or passed to other departments for university use. They will avoid transmission of protected SIS information. If it is necessary to transmit protected information, employees are required to take steps to reasonably ensure that the information is delivered securely to the proper person who is authorized to receive such information for legitimate university use.

Know and abide by all university information policies dealing with security and confidentiality of university records.

Image files and other representations of customer information must be protected with the same care as regular data files and printed materials.

Employees will secure their workstation by logging off or locking the screen before leaving it unattended for extended periods of time.

Controlling viewing access/inquiry access

Placement of computer terminals which display customer information will be done in such a way as to prevent casual viewing or eavesdropping by unauthorized personnel.

Computer terminals used to display customer information will not be left unattended by the user with customer information still displayed.

Employees will positively identify all customers requesting access to customer information.

Lost or stolen keys to secure areas must be reported to the director of information systems and to campus security immediately. If there have been stolen or lost keys, the affected locks will be changed.

Attempts to break into secure areas will be reported to campus security and to the director of information systems.

Printed material handling

Printed copies of customer information:

- Are to be handled or viewed only by authorized personnel.
- If used in unrestricted areas, copies in use by authorized personnel are to be put away in lockable storage when unattended.
- Will be stored in secure areas.

All printed copies of customer information that are no longer needed must be shredded.

Responsibility and Review

Responsible Party

Responsibility for this policy lies with the provost. Policy implementation is the responsibility of the director of information systems.

Policy Review

This policy is to be reviewed annually by the Information Systems Planning Committee (ISPC).

Distribution: Information Systems web site

7. Technology Resource Allocation Policy

Eastern Mennonite University (EMU) procures and administers technology systems and components centrally. This policy identifies the principles and processes used by Information Systems (IS) to determine how technology resources are allocated to meet the needs of the EMU community.

General Resources and Services Provided

The institution provides the following resources to students, faculty, and staff:

1. A wired campus network with access to the Internet and network connections in all classrooms, meeting rooms, offices, and residence hall rooms.
2. A wireless campus network with access to the Internet in all residence halls, classrooms and common spaces.
3. A desktop computer and a telephone with voicemail for all staff and faculty (half-time or greater). All part-time staff and part-time/adjunct faculty will be provided access to shared versions of these resources installed in a space that can be reasonably shared with employees of similar classification.
4. Printers located in common areas for departmental printing.
5. Copiers located in common areas for departmental copying.
6. Public student computer laboratories and some small departmental labs.
7. Multimedia projection systems in all classrooms regularly scheduled by the registrar.
8. Several technology classrooms with adequate computers for each student per class section.
9. A web-accessible library catalog and related research tools.
10. An integrated administrative computer system, including web access to data used by employees and students.
11. A facilities and rooms scheduling system.
12. A web-based course management system.
13. A central Help Desk for requests for everything technology-related on campus.
14. Access to network storage, sharing of files, printing and backup of files.
15. E-mail accounts are provided for all faculty (including retirees if requested), staff, and students. Non-returning students or graduates may request continuation of their e-mail accounts for a transition period of 12 months. Non-returning faculty or staff will have their e-mail options explained to them during the exit interview process by Human Resources. E-mail accounts provided to retirees are considered guest accounts with the option to receive, but not send, institutional broadcast messages.

Specifications for Resources and Services Provided

Cell Phones

Access to cell phone resources is governed by policy administered by Financial Affairs/Human Resources. IS will work with departments that need a cell phone that

is shared frequently among department employees. With approval from the vice president for finance, these phones will be provisioned under an institutional cell phone contract but must be funded by the requesting department.

Computers - Desktops

Desktop support is provided for institution-owned computers running Windows and Mac OS. Windows is provided for administrators and staff, except for graphic designers in the Marketing department who use Mac OS. All new faculty will receive a Windows computer unless a Macintosh is preferred.

Desktop computers include sound capabilities, but no speakers are provided. Speakers can be supplied to any employee for a small fee charged to the department. Speakers are not available for computers in computer labs (public or departmental). Headphones may be used with any computer but will not be supplied by IS.

Resource limitations make it impossible to guarantee the availability of a computer for faculty on sabbatical. A computer may be provided, when available. Faculty whose primary computer is a laptop may continue to use it on sabbatical.

Computers - Laptops

Departments that require their employees to use a laptop as their primary computer will be required to fund the difference in cost from a standard Windows desktop computer. There may be additional charges for software.

Laptops that are shared in a department will be funded entirely by the department. The department will also need to fund all upgrades and replacements for these shared laptops. IS may have older laptops available at a reduced cost.

If a faculty/staff laptop is stolen, Information Systems will pay $800 and the department pays the remaining amount. If submitted to insurance, the department pays the deductible.

If a faculty/staff windows computer is damaged after the complete care warranty has expired, it will result in an early computer upgrade. If a faculty/staff Mac computer is damaged and is not covered by AppleCare, the cost will be split 50/50 between Information Systems and the department. Before the repair is made, the cost of repair will be reviewed to determine whether to proceed with the repair or to upgrade early. An early upgrade will follow the normal laptop process.

Computers - Work-Study/Shared

Older computers and monitors will be made available to departments for use as work-study or shared computers. If the department requires a more powerful computer, the department will need to fund the full cost and any future replacements.

Photocopiers/Multifunction Devices

Photocopiers are provided in central locations and departments. These devices also function as scanners and printers, and are sometimes referred to as multifunction devices (MFDs). The IS department is responsible for copier procurement, maintenance and supplies. Departments and individuals will be charged for paper

output (copies, prints), and scanning. Copiers may be cascaded on campus if usage metrics indicated that copiers are being over- or under-utilized. Departments that continually underutilize their copier may be subject to a monthly fee to cover the lease cost of the copier.

Disposal of Obsolete Electronic Resources

All EMU-owned electronic equipment removed from service by IS will be processed in a manner that meets all state and federal requirements for disposing of electronic equipment.

E-mail

Every current student and current employee will be provided an emu.edu e-mail address that will be recognized as the e-mail address to which all official electronic university communications are sent. The following provisions apply to administration of students' and employees' emu.edu e-mail accounts (e-mail account holders):

1. E-mail account holders will always ensure that their email is stored securely and regularly check for e-mail sent to their e-mail account.
2. Students may elect to automatically forward their emu.edu account to any e-mail address of their choosing but, in doing so they recognize that EMU cannot guarantee the delivery of e-mail forwarded to addresses outside the emu.edu domain. The emu.edu account holder remains accountable for all emu.edu originated e-mail sent to their emu.edu domain address.
3. Employees are not permitted to automatically forward their emu.edu assigned e-mail accounts to any other e-mail address.
4. All users will take precautions to safeguard their EMU e-mail accounts from access by any other party, in part because they may contain important and confidential institutional data, regardless of whether the account is accessed via the web, a mobile device or a computer on campus.
5. Non-returning students or graduates may request continuation of their e-mail accounts for a transition period of 12 months after the end of their last academic term at EMU.
6. Non-returning employees will have their e-mail options explained to them during their exit interview with Human Resources.
7. Retirees may request continuation of their emu.edu e-mail accounts for life. The retiree's account will be considered a guest account with the option to receive, but not send to, institutional broadcast messages.

Equipment: Departmental

All university computers are maintained in a central inventory. 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. Replacement of such equipment must be funded entirely by the department. All departmental equipment is labeled and part of the inventory database. If equipment is re-deployed, the department that funded the equipment will be given first priority; however, IS may use such equipment anywhere on campus.

Equipment: Grant-Funded

Individuals pursuing grants for technology equipment should discuss their plans with IS as part of their budgeting process. Technology equipment that is acquired under grants will be inventoried. Any upgrade will be funded by the grant or the department.

Faculty members teaching in various special curricular programs are, under certain conditions, awarded research or startup funds. Some faculty members may have research or discretionary funds available to them when they hold endowed chair positions. When these special funds are used to buy additional computers and other electronic equipment, this equipment will belong to the university. Such equipment must be ordered through the IS purchasing process and will not normally be upgraded or replaced by the university, except through further use of these special funds.

Equipment: Loaners

Employees may borrow laptop computers for uses related to university business. Both Macintosh and Windows laptops are available. Laptop reservations and checkouts are handled through Learning Resources. The IS department is committed to providing Learning Resources with laptops in a reasonable working condition. Student clubs may borrow laptops from Learning Resources when requested by an adviser; however, the laptop must be checked out personally by the club adviser who becomes responsible for the laptop while on loan to the club. Borrowers will be responsible for loss or damages of the laptop up to a maximum of $200 which will be charged to either the employee or the department, depending on the circumstances.

Fax Machines

All fax machines are funded by the department. IS will provide phone service and basic support. The department will be charged a monthly fee for the phone service along with any long-distance charges incurred (see Telephones section).

Financial Processes

Technology at EMU is financed through the annual budgeting processes. Costs for connecting students' computers to the campus network are included in tuition and/or housing costs.

An attempt is made to anticipate as many purchases as possible in the budget planning stage. Near the start of each spring semester, division heads ask departments to identify and submit technology requests for replacements or newly identified needs. If supported by the division head, these are then turned over to IS for compilation and comparison to needs identified through inventory review. Information Systems then submits a review of needed equipment to the Information Systems Planning Committee, which makes a recommendation to the Cabinet for the annual capital budget. IS pays particular attention to equipment needs that cross departments, such as classroom equipment.

Computer technology items (includes all hardware and all software installed on EMU owned computers) purchased by the institution are to be requested, approved, and

purchased through the centralized process, regardless of the source of funds. This ensures compatibility, monitoring of inventory, compliance with licensing, cost efficiency and to provide assistance with warranty issues. All technology purchased with IS assistance will be labeled and included in the inventory database. Support for any technology resource procured without the assistance of IS will be at the discretion of the director of information systems. The department may be charged an hourly rate for this support.

In purchasing equipment, IS considers total cost of ownership. To keep this cost lower, the department purchases equipment from industry-recognized vendors. Cost, functionality, life-span, and overall quality are balanced in selecting appropriate equipment.

Mobile Computing Devices

Persons considering purchasing a mobile computing device should contact IS to determine the best device for their needs.

Information System's Responsibilities:

- Mobile computing devices are prone to periodic synchronization errors which can be very time consuming to resolve. IS will try to assist with diagnosing these problems; however, the individual may need to manually work through Outlook entries to determine which records are causing the problem or deleting duplicate entries. While diagnosing the problem it may be necessary to overwrite either the device's database or the Outlook database; either one could result in the loss of data.
- IS will try to provide a timely response to mobile computing device issues; however, this may not always be possible.

User's Responsibilities:

- Synchronize regularly.
- Contact the IS Help Desk if a synchronization error cannot be resolved.
- Refrain from storing confidential information on your mobile computing device.

A list of specific supported mobile computing devices is located at the IS helpZONE website (http://www.emu.edu/is/wiki/index.php/Mobile_Computing_Devices)

Network storage: Personally Secured

All current students and current employees are provided network storage space that is considered their private storage space (see privacy provisions in *Responsible Use of Electronic Files and Communications).* For students, this space is intended as a secure place to store files that need to be protected and/or backed up. For employees, this space is intended for institutional files that are private to the employee, including space for backing up data if a laptop is provided to an employee.

Students will be provided 100 MB (megabytes) of private network file storage.

Employees will be provided 150 MB of private network file storage but they may request additional space by sending a request to helpdesk@emu.edu with the reason why the additional space is needed.

New Technology Adoption

Technology is continually evolving. As new technologies emerge, the IS department evaluates how and when to make it standard for all users. Until the technology is adopted as "standard" by IS, any department requiring the new technology will provide the funding. Any equipment purchased as non-standard technology will be marked with a sticker indicating that it was purchased with special funds. Should the equipment be re-deployed, the department that funded the equipment will be given first priority in using the equipment. All technology equipment will be part of Information System's inventory and may be used anywhere on campus.

Printers

Networked printers are provided in central locations wherever possible. In most cases this means a personal printer is not provided or supported. The latter are provided in limited cases where the departmental printer is distant (per decision of the director of information systems). The IS department is responsible for printer replacements, including working with departments on functionality needs and cascading when appropriate.

Costs for all networked, laser, printers and copiers are the responsibility of IS. For these devices, departments will be charged per page on a monthly basis. Costs for all other printers are the responsibility of the department. The IS department is responsible for consumable supplies in the public computer labs (see computer lab definitions at http://www.emu.edu/is/info/lab).

Projectors: Departmental

Any department that desires to have a projector available on a permanent basis will need to fund the purchase and arrange for IS to procure it. The projector will be labeled and entered in the inventory database. It will be considered similar to departmental equipment (see section on Departmental Equipment).

Replacement Cycle

With rapid technological advances, regular replacement of technology is essential. For desktop computers the goal is a four-year replacement cycle. In many cases the newest machines are placed in locations that require the highest performance, and some cascading of older machines may result. Regular reviews are performed to determine other replacement and upgrade needs.

An inventory of desktop and other technology equipment and software is maintained to permit evaluation of existing equipment and identification of priority needs. The oldest, least functional desktop machines are retired annually.

Software

Software Support Levels

The IS department provides three different levels of support for four categories of software as outlined in the following table:

SOFTWARE CATEGORY	SUPPORT TYPE	SUPPORT DESCRIPTION	FUNDING SOURCE	UPGRADE DETER-MINED BY	LICENSING

SOFTWARE CATEGORY	SUPPORT TYPE	SUPPORT DESCRIPTION	FUNDING SOURCE	UPGRADE DETER-MINED BY	LICENSING
Infrastructure: Programs needed for each University-owned computer or used by IS to maintain systems.	FULL	Includes installation, orientation for new users and assistance with operational problems.	Information Systems	Information Systems	Site licensing or internal license manageme nt
Special Shared Software: Programs typically installed on every University-owned desktop computer because of a site license. (i.e. EndNote: site license, shared)	LIMITED	Limited to installation and assistance with run-time errors.	As designated.	Information Systems	Site licenses
Subscription Software: Programs used for a special purpose by a limited number of users across multiple departments. Departments are required to upgrade when new software versions are available.	LIMITED	Limited to installation and assistance with run-time errors.	Individual Department s	Information Systems	Individual per user licenses
Hosted Software: Programs needed exclusively by individual departments.	HOST	Installation only.	Individual Department s	Information Systems	Individual and multi-use licenses

Software Metering

A license management system will be used to maintain a limited number of licenses for software used by many people.

Computer Lab Software

Software for each image for each computer laboratory is also listed on the website (http://www.emu.edu/is/wiki/index.php/Computer_Labs). In order to add new software to EMU's list of approved software faculty must contact the IS Help Desk.

Personal Software: If users install software not on the list of supported software (i.e. "personal software"), they are responsible to ensure that it causes no harm to the network or university servers and are entirely responsible for its support. If IS is required to reinstall Universal, Special or Hosted Software on a computer *more than once* because of use of personal software, a fee will be charged to the individual. If "personal software" is installed on EMU-owned hardware, the user must be prepared to provide IS with proof of purchase and proper license documentation upon request.

Software Training

Training by IS staff for software is limited to "Universal Software" and then only for general "orientation" to the software. Additional assistance for application software is outlined on the website and may include finding user experts on campus, checking listings of Frequently Asked Questions (FAQs), searching software vendors' Knowledge Bases, and acquiring off-campus training.

License Procurement

Licenses for software must be kept up to date. The IS department purchases licenses for all EMU approved software installed on EMU computers regardless of funding source. EMU owned licenses may not be installed on computer hardware that is not owned by EMU.

Computer Maintenance and Operational Procedures

Users are responsible to keep their computers free from programs that consume unreasonable resources or otherwise slow the computer performance. If the IS department is required to re-image a computer more than once because of Spyware/Malware infestations, a fee will be charged to the individual.

Special Needs Accommodations

Occasionally university employees may require special equipment for their computers due to health concerns or special needs. The university will provide suitable technology equipment as may be required by the user to adequately perform their tasks as defined in their written job description. Funding for such accommodations will be provided through the budget processes that would have otherwise made available the standard technology provided to the user. If special equipment is required due to medical conditions, the employee may be requested to provide a doctor's note for documentation of the circumstances before the equipment is purchased.

Standardized Peripherals

IS supplies a monitor, keyboard and mouse to each user. Standardized models and features have been established to reduce support issues. If a department needs or wants a different model peripheral or feature that is not a part of the standard, the full purchase cost will need to be funded by the department. These peripherals must be purchased in consultation with IS to ensure compatibility with EMU systems.

Telephones

The IS department will provide a telephone, dedicated extension and voicemail for all EMU employees upon request. There will be a monthly charge to the department for all extensions assigned to the department. Extensions may only be added and deleted on an annual basis for billing purposes. The addition of a telephone is contingent on the availability of wiring to the desired location. The IS department has conference speakerphones available for use upon request.

Responsibility and Review

Responsible Party

Responsibility for this policy lies with the Provost. Policy implementation is the responsibility of the director of information systems.

Policy Review

This policy is to be reviewed annually by the Information Systems Planning Committee (ISPC).

Distribution: Information Systems web site

8. Implementation Procedures for Red Flags Rule

Program Adoption

Eastern Mennonite University (EMU) developed this identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students and to the safety and soundness of the creditor from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Definitions

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

A **covered account** means an account that a creditor offers or maintains, primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.

A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

University Covered Accounts

EMU has identified five types of accounts, four of which are covered accounts administered by the university and one type of account that is administered by a service provider.

1. Refund of credit balances involving PLUS loans
2. Refund of credit balances, without PLUS loans
3. Deferment of tuition payments
4. Faculty loans

Service provider covered account:

The university shall take steps to ensure that the activity of every service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. The university uses Tuition Management Systems to administer the monthly payment plan and Campus Partners administers the Perkins Loan Program. Students contact these agencies directly through its website or by telephone and provide personally identifying information to be matched to the records that the university has provided.

Identification of Relevant Red Flags

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above
2. The methods provided to open covered accounts; acceptance to the university and enrollment in classes requires all of the following information:
   - Applications to the university with personally identifying information
   - high school transcript, official ACT or SAT scores and two letters of recommendation for undergraduate students
3. The methods provided to access covered accounts:
   - Disbursement obtained in person require picture identification if the person processing the disbursement does not know the requester.
   - Disbursements obtained by mail can only be mailed to an address on file
   - The university's previous history of identity theft.

The Program identifies the following red flags:

1. Documents provided for identification appear to have been altered or forged
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification
3. A request made from a non-university issued e-mail account
4. A request to mail something to an address not listed in the SIS database
5. Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts.

Detection of Red Flags

The Program will detect red flags relevant to each type of covered account as follows:

1. **Refund of a credit balance involving a PLUS loan** – As directed by federal regulation (U.S. Department of Education) these balances are required to be refunded in the parent's name and mailed to their address on file within the time period specified. No request is required.

   Red Flag – none as this is initiated by the university.

2. **Refund of credit balance, no PLUS loan** – Requests from current students must be made in person by presenting a picture ID or in writing from the student's university issued e-mail account. The refund check can only be mailed to an address on file or picked up in person by showing picture ID. Requests from students not currently enrolled or graduated from the university must be made in writing.

   Red Flag – Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
3. **Deferment of tuition payment** – Requests are made in person only and require the student's signature.

   Red Flag – none.
4. **Faculty loan** - Requests must be made in person by presenting a picture ID or in writing from the university issued e-mail account. The loan check can only be mailed to an address on file or picked up in person by showing picture ID.

   Red Flag - Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from the university issued e-mail account.
5. **Tuition payment plan** – Students must contact an outside service provider and provide personally identifying information to them.

   Red Flag – none, see Oversight of Service Provider Arrangements section of this procedure.

Response

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.

Oversight of Service Provider Arrangements

Responsibility and Review

Responsible Party

The Program Administrator is the vice president for finance and has responsibility for:

1. Developing, implementing, updating and administering this Program
2. Ensuring appropriate training of university staff on the Program,
3. Reviewing any staff reports regarding the detection of Red Flags,

4. Reviewing the steps for preventing and mitigating Identity Theft, and

Determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

Policy Review

This Program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of the university from identity theft. At least once per year, in October, the Program Administrator will consider the university's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the university maintains and changes in the university's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program.

Distribution: Information Systems web site

APPROVAL

The Information Systems policies in this manual were reviewed and approved by the following entities:

Information Systems Planning Committee (ISPC)

Reviewed and approved 04/09/2013

President's Cabinet

Reviewed and approved 09/09/2009

ACKNOWLEDGMENTS

Overall policy manual framework

The framework for this policy manual was patterned after concepts used at Cornell University as found during early research for this policy re-write in spring of 2009. The Cornell Office of Information Technology policy web pages since then have been updated and are no longer available online but the general concepts of Cornell IT policy framework are described in the following Power Point presentation made at the EDUCAUSE Security Professional Conference, April 2006: http://net.educause.edu/ir/library/powerpoint/SPC0662.pps

Section 3-Responsible use of Information Technology Resources

This section was modeled from similar policies found at Oberlin and Earlham universities.

Section 4-Responsible Use of Electronic Files and Communications

This section was modeled from similar policies found at Goshen College and Cornell University.

Section 4- Responsible Use of Electronic Files and Communications

Compliance Checklist for Unsolicited Commercial E-Mail Messages

Substantial portions of the guidelines on this checklist were adapted from the Northeastern University July 2004, Summary of Federal and State anti-spam regulations.

Section 6-Security of Electronic Administrative Information

This section was modeled from similar policies found at Goshen College.

Section 8-Implementation Procedures for Red Flags Rule

This section was modeled from a similar policy found at Kalamazoo College which was posted on the EDUCAUSE.edu website.