Mohave Community College
Information Technology Security Manual

Version 2.0

25 July 2016

Table of Contents

Information Technology Security Manual

"Security is never black and white, and context matters more than technology. Just because a secure operating system won't protect against hand grenades doesn't mean it's useless; it just means that we can't throw away our walls and door locks and window bars. Different security technologies have important places in an overall security solution. A system might be secure against the average criminal, or a certain type of industrial spy, or a national intelligence agency with a certain skill set. A system might be secure as long as certain mathematical advances don't occur, or for a certain period of time, or against certain types of attacks. Like any adjective, "secure" is meaningless out of context."

Bruce Schneier - Secrets and Lies - Digital Security in a Networked World

1. Preamble

Mohave Community College acknowledges an obligation to ensure appropriate security for all Information Technology (IT) data, equipment, and processes in its domain of ownership and control. Within this context the College endeavors to balance the need for security against unreasonable risk with the need of students, faculty, and staff to be able to use its systems with the minimum of encumbrance. The obligation for security is shared, to varying degrees, by every member of the College.

This document will:

a. Enumerate the elements that constitute IT security.

b. Explain the need for IT security.

c. Specify the various categories of IT data, equipment, and processes subject to this policy.

d. Indicate, in broad terms, the IT security responsibilities of the various roles in which each member of the College may function.

e. Indicate appropriate levels of security through standards and guidelines.

2. Scope of IT Security

2.1. Definition of Security

Security can be defined as “the state of being free from unacceptable risk.” Risk for the College concerns the following categories of losses:

- Confidentiality of Information.
- Integrity of data.
- Assets.
- Efficient and Appropriate Use.
- System Availability.

Confidentiality refers to the privacy of personal or corporate information. This includes issues of copyright.

Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disk fails, or subtle, as when a character in a file is inappropriately altered.

The assets that must be protected include:

- Computer and Peripheral Equipment.
- Communications Equipment.
- Computing and Communications Premises.
- Supplies and Data Storage Media.
- Computer Programs and Documentation.
- Information/Data.

Efficient and Appropriate Use ensures that college IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others or established policy.

Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

The potential causes of these losses are termed “threats.” These threats may be human or non-human, natural, accidental, or deliberate.

2.2. Domains of Security

This policy will deal with the following domains of security:

- Computer system security: CPU, Peripherals, Operating Systems. This includes data security.
- Physical security: The premises occupied by the IT personnel and equipment.
- Operational security: Environment control, power equipment, operation activities.
- Procedural security by IT, vendor, management personnel, faculty, staff and students.
- Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.

3. Reasons for IT Security

Confidentiality of information is mandated by common law, formal statute, explicit agreement, professional practice, and/or convention. Different classes of information warrant different degrees of confidentiality.

The hardware and software components that constitute the College's IT assets represent a sizable monetary investment that must be protected. The same is true for the information stored in its IT systems, some of which may have taken significant resource investments to generate, and some of which can never be reproduced.

The use of College IT assets other than in a manner and for the purpose for which they were intended represents a misallocation of valuable College resources, and possibly a danger to its reputation or a violation of the law.

Finally, proper functionality of IT systems is required for the efficient operation of the College. Some systems, such as the Human Resources, Finance, Student Administration, and Library systems are of paramount importance to the mission of the College. Other systems (e.g. somebody's PC) are of less importance.

4. Roles and Responsibilities

4.1. Policy Management

Approval of the IT Security Manual is vested with the President, the Chief Executive Officer of the College.

Advice and opinions on the Manual will be given by:

- Information Technology Unit (ITU)
- Information Technology Advisory Council (ITAC)

Formulation and maintenance of the IT Security Manual is the responsibility of the Executive Director of Information Technology.

4.2. Policy Implementation

Each member of the College will be responsible for meeting published IT standards of behavior. IT security of each system will be the responsibility of the designated system custodian.

4.3. Custodians

- ITU will be the custodian of all strategic system platforms.
- ITU will be custodian of the strategic communications systems.
- ITU will be custodian of all central computing laboratories.
- Department Chairs and Heads will be custodians of strategic applications and platforms under their management control.
- Individuals will be custodians of desktop, laptop, and tablet systems under their control.

4.4. Individuals

All users of College IT resources:

1. Will operate under the provisions of the "Appendix A: Standards and Guidelines for All Users of College Computing and Network Facilities."

2. Must behave under the "Code of Practice" provisions of the "Standards and Guidelines for All Users of College Computing and Network Facilities."

3. Are responsible for the proper care and use of IT resources under their direct control.

4.5. College Services

It is recognized that various sections of the College provide services that relate to IT security, both directly and indirectly. It is expected that there will be collaboration between these sections and Information Technology Unit (ITU) in generation of standards and implementation of the policy. Some of these sections and their services are:

- <u>Human Resources:</u> Personnel selection, induction, and exit-processing. Disciplinary action for faculty/staff.
- <u>Registrar:</u> Policies concerning confidentiality, privacy, and copyright.
- <u>Facilities:</u> Physical building security.
- <u>Campus President:</u> Disciplinary agent for students.
- <u>Instructional Effectiveness:</u> institutional reporting
- <u>Dental Hygiene:</u> Customer database including confidential information

4.6. Standards and Guidelines

Standards (mandatory) and guidelines (suggestions) will be published as attachments to this policy to assist users and system custodians to meet their IT security responsibilities. These standards and guidelines, though presented as attachments, are an integral part of this College's IT Security Manual and therefore define it.

5. Policy Documentation

5.1. Documents

This policy is enunciated by four documents:

1. "IT Security Manual"

2. "Guidelines for All Users of College Computing, Learning and Network Facilities" (IT Security Manual)

3. "Standards and Guidelines for Strategic Systems" (IT Security Manual)

4. "Standards and Guidelines for Desktop Computers" (IT Security Manual)

5. "MCC Standards of Acceptable Use of Computing Equipment" (IT Security Manual, Employee and Student Handbooks, web: http://www.mohave.edu/Assets/documents/Information_Technology/IT_Acceptable_Use.pdf)

5.2. Availability

It is intended that this IT Security Policy be publicly accessible in its entirety via the College's Web page. There is the requirement that all users of College IT resources be familiar with relevant sections of this policy.

5.3. Changes

The IT Security Manual is to be a "living" document that will be altered as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers, etc.

Major changes will be made in consultation with ITUAC, and with the approval of the President.

Appendix A – Standards and Guidelines for All Users of College Computing and Network Facilities

1. Conditions of Use of Computing, Learning & Networking Facilities

1. It is the policy of the College that the computing, learning, and networking facilities are intended for use for teaching, learning, research and administration in support of the College's mission. Although recognizing the increasing importance of these facilities to the activities of staff and students, the College reserves the right to limit, restrict, or extend access to them.

2. All persons using the computing, learning and networking facilities shall be responsible for the appropriate and reasonable use of the facilities provided as specified by the "Codes of Practice" of this policy, and shall observe conditions and times of usage as published by the Custodian of the system.

3. It is the policy of the College that the computing, learning and associated network facilities are not to be used for personal, commercial or non-College-related purposes without written authorization from the College. In any dispute as to whether work carried out on the computing, learning and networking facilities is internal work, the decision of the President or his/her designee shall be final.

4. The user will not record or process information/data which knowingly infringes any patent or breaches any copyright.

5. The College will endeavor to protect the confidentiality of information and material furnished by the user and will instruct all computing personnel to protect the confidentiality of such information and material, but the College shall be under no liability in the event of any improper disclosure.

6. The College will endeavor to safeguard the possibility of loss of information within the College's computing, learning and networking facilities but will not be liable to the user in the event of any such loss. The user must take all reasonable measures to further safeguard against any loss of information within the College's computing, learning and networking facilities.

7. In the event of a loss of information/data within the system, ITU will endeavor to help restore the information. Please note that personal documents or documents not saved to the server could be lost if you do not back them up to your H: drive or another location. ITU does NOT back up individual computers.

8. The use of the computing, learning and networking facilities is permitted by the College on the condition that it will not involve the infringement of any patent or the breach of any copyright and the user agrees to indemnify and keep indemnified the College and each member and every member of its staff against all actions, claims, and demands for infringement of patent and or breach of copyright which may be brought or made against the College or any member of its staff arising out of or in connection with the use of the computing and networking facilities.

9. Users of the computing, learning and networking facilities recognize that when they cease to be formally associated with the College (e.g. no longer an employee, enrolled student, or visitor to the College), their information/data may be removed from College computing, learning and networking facilities without notice. Users must remove their information/data or make arrangements for its retention prior to leaving the College.

10. The College reserves the right to limit or restrict any user's usage of the computing, learning and networking facilities; to copy, remove, or otherwise alter any information/data or system that may undermine the authorized use of the computing, learning and networking facilities; and to do so with or without notice to the user in order to protect the integrity of the computing, learning and networking facilities against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.

11. The College, through authorized individuals, reserves the right to periodically check and monitor the computing, learning and networking facilities, and reserves any other rights necessary to protect them.

12. The College disclaims responsibility and will not be responsible for loss or disclosure of user information or interference with user information resulting from its efforts to maintain the privacy, security, and integrity of the computing, learning, and networking facilities and information.

13. The College reserves the right to take emergency action to safeguard the integrity and security of the computing, learning and networking facilities. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords. The taking of emergency action does not waive the rights of the College to take additional actions, up to and including disciplinary actions, under this policy.

14. Users of the computing, learning and networking facilities do so subject to applicable laws and College policies. Mohave Community College disclaims any responsibility and/or warranties for information and materials residing on non-College computer systems or available over publicly accessible networks, except

where such responsibility is formally expressed. Such materials do not necessarily reflect the attitudes, opinions, or values of Mohave Community College, its staff, or students.

15. The Executive Director of Information Technology or Campus President may suspend any person from using the computing, learning and networking facilities after appropriate investigation. Actions that may result in suspension include, but are not limited to, the following:

    - responsible for willful physical damage to any of the computing, learning and networking facilities;
    - in possession of confidential information/data obtained improperly;
    - responsible for willful destruction of information/data;
    - responsible for deliberate interruption of services provided by ITU;
    - responsible for the infringement of any patent or the breach of any copyright;
    - gaining or attempting to gain unauthorized access to accounts and passwords;
    - gaining or attempting to gain access to restricted areas without the permission of the Executive Director of Information Technology;
    - responsible for inappropriate use of the facilities;
    - responsible for prohibited use of the college email system, including forwarding jokes, engaging in social commentary, personal quotes in signatures, etc. as detailed in the Email Use Directive,
    - responsible for the display, generation or distribution of offensive material in violation of College policy.

16. External work or use of the computing, learning and networking facilities shall not be undertaken which would prevent College users from having their usual access to the facilities.

Appendix B: MCC Standards of Acceptable Use of Computing Equipment

Primary Principles

Mohave Community College strives to promote a culture of openness, trust, integrity, and an environment wherein freedom of expression and scholarly inquiry are encouraged and supported. The intention of this Acceptable Use Policy are not to impose restrictions that are contrary to these values, which are the core of our academic and administrative community. Some computing resources dedicated to specific roles, including administrative systems and teaching systems containing information protected under the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), necessarily limit access in order to protect the privacy of our students, faculty, and staff.

Effective security is a team effort involving the participation and support of the entire Mohave Community College team, including our students, faculty, and staff. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

This policy sets forth standards for the responsible use of Mohave Community College information technology resources. Individuals and groups using MCC resources both on and off campus are responsible for complying with security standards set forth in this policy, including securing passwords, identification numbers, and security codes and using them solely for their intended purposes. Individuals are solely responsible for their personal use of IT resources, including computer accounts and other resources under their control. This policy is in place to protect the MCC community and to ensure the smooth, secure operation of our information technology systems.

Scope

This policy applies to all information technology resources, including but not limited to computer systems, data and databases, computer labs, smart devices including cell phones and tablets, e-mail boxes, data and voice networks, applications, software, files, and portable media. MCC provides the resources to support the academic, research, administrative, and instructional objectives of the college. The use of these resources are limited to college students, faculty, staff and other authorized users to accomplish tasks appropriate to the status of the individual.

General Acceptable Use Guidelines

The guidelines below are not intended to be comprehensive, but to define and explain the intent of this policy. Situations not specifically covered by this policy will inevitably arise and should be judged and interpreted in the spirit of this policy.

Generally Prohibited Conduct

1. Altering system hardware or software without authorization, including installation of unlicensed or unapproved software or hardware. “Freeware” and “Shareware” programs usually contain a provision denying use in professional environments without payment, so the installation of such programs violates this policy.
2. Disrupting or interfering with the delivery or administration of information technology assets, including network communications, e-mail, hardware, or software.
3. Attempting to access or accessing an account other than the account provided for your use.
4. Intercepting or reading electronic communications, including e-mail and chat messages not addressed or assigned to you.
5. Misrepresenting your identity in an e-mail, chat, or university owned social messaging platform.
6. Installing, copying distributing, or using digital content in violation of copyright and/or software agreements or applicable federal or state law. This includes the use of file sharing software including but not limited to BitTorrent, uTorrent, Sharefile or other services that allow the illegal download or use of copyrighted media.
7. Interfering with others’ use of share resources, including computers, lab space, or common technology areas.
8. Using college resources for commercial or profit-making purposes or to represent the positions or interests of groups unaffiliated or unassociated with the MCC community or the normal professional practices of students, faculty, and staff.
9. Ignoring or evading departmental or lab policies, procedures, and protocols.
10. Assisting unauthorized users’ access to college IT resources.
11. Exposing sensitive or confidential information or disclosing information that you do not have the authority to disclose.
12. Using IT resources for illegal activities, including threats, harassment, copyright infringement, defamation, theft, identity theft, and unauthorized access.
13. Using IT resources to access gambling or gaming sites.

14. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

Security and Proprietary Information

1. All mobile and computing devices that connect to the network must be capable of minimum 128 bit encryption for network traffic.
2. System and user level passwords must comply with college standards (currently 10 characters, including an uppercase, lowercase, number, and a symbol). Failing to protect passwords or allowing others access to resources using your account is prohibited.
3. All computing devices must be secured with password protected screen savers with an automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.
4. Users should assume that attachments or unsolicited message may contain or do contain malware and viruses and avoid opening, executing, or downloading such attachments.
5. Employees posting to forums, social media, Usenet groups, or other communications platforms that use an MCC e-mail address must include a disclaimer stating that their posting does not represent the views of Mohave Community College unless such posting is part of their normal business duties.

System and Network Access

1. Accessing data, a server, or an account for any purpose other than conducting Mohave Community College business is prohibited.
2. Exporting software, technical information, encryption information, or information about the capabilities of information systems is prohibited.
3. Introduction of malicious programs, including viruses, worms, malware, adware, or similar programs is prohibited.
4. Port scanning, security scanning, and other types of network scanning is prohibited without the written permission of the information technology unit.
5. Disrupting network communication through the use of network sniffing, ping flood, packet spoofing, denial of service, forged routing information, e-mail spoofing, or otherwise misrepresenting network traffic is prohibited.
6. Providing information about, or lists of MCC students, faculty, or staff to outside parties unless it is part of your normal duties is prohibited.

E-mail and Electronic Communication

1. Use of MCC resources to access and use the internet requires good judgement on the part of the user. Users must realize that they represent the college and must, when stating an affiliation to the college, include verbiage indicating that the opinions expressed are their own and not necessarily those of Mohave Community College.
2. Sending unsolicited e-mail messages, including "spam" or "junk mail" or other advertising material to individuals who did not request it is prohibited.
3. The unauthorized use or forging of e-mail headers is prohibited.
4. Any form or harassment, including via e-mail, voice mail, and chat services whether through language, frequency, or size of messages is prohibited.
5. Solicitation of e-mail for any e-mail address other than your own is prohibited.
6. Forwarding chain letters, Ponzi or Pyramid scheme messages, or messages not related to college business is prohibited.
7. Use of MCC e-mail addresses for any purpose other than college business is prohibited.

Policy Compliance

1. The Information Technology Team will verify compliance to this policy through various methods, including but not limited to business reports, internal and external audits, audit tools, and security related hardware and software tools.
2. The Information Technology team routinely monitors inbound, outbound, and internal network traffic for the purposes of policy compliance and network maintenance. Mohave Community College reserves the right to audit systems and network traffic to ensure compliance with this policy.
3. Exceptions to this policy must be approved by the Information Technology team in advance, and in writing.

Resource Degradation

1. It is inappropriate use to deliberately perform any act which will impair the operation of any part of the computing, learning and networking facilities, or deny access by legitimate users to any part of them. This includes but is not limited to wasting resources, tampering with components or reducing the operational readiness of the facilities.

2. The willful degradation of computing, learning and networking resources is inappropriate use. Degradation includes but is not limited to passing chain letters, willful generation of large volumes of unnecessary printed output or disk space, willful creation of unnecessary multiple jobs or processes, or willful creation of

heavy network traffic. In particular, the practice of willfully using the College's computing, learning and networking facilities for the establishment of frivolous and unnecessary chains of communication connections is an inappropriate waste of resources.

3. The sending of random mailings (“junk mail”) is unacceptable. It is poor etiquette at best, and harassment at worst, to deliberately send unwanted mail messages to strangers. Recipients who find such junk mail objectionable should contact the sender of the mail, and request to be removed from the mailing list. If the junk mail continues, the recipient should contact the ITU Help Desk.

Game Playing

Limited recreational game playing that is not part of an authorized and assigned research or instructional activity, is tolerated as long as the user does not install any software nor play any game that utilizes network resources (i.e. only pre-installed games that run locally on the pc). College computing, learning and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a public computing facility must give up that computing position when others who need to use the facility for academic or research purposes are waiting.

Additional Guidelines at Local Sites

The College computing, learning and network facilities are composed of many "sites." Each site may have local rules and regulations, which govern the use of computing, learning and network facilities at that site. Users are expected to cooperate with and comply with College and local site policies. Site policies may be more restrictive than College policy. It is the intention that the College IT Security Manual represent a minimum standard. Local administrators may impose more restrictive policies, which become their responsibility to administer.

Connection to the Campus-Wide Data Network

To maintain the integrity of the College computing, learning and network facilities, connections to the campus network are made only by specialized personnel under the direction of the ITU network staff. Users are encouraged to attach appropriate equipment only at existing user-connection points. All requests for additional Network connections or for the relocation of a connection should be directed to ITU Help Desk.

Use of Desktop Systems

Users are responsible for the security and integrity of College information/data stored on their personal desktop system. This responsibility includes making regular backups to disc or H: drive and controlling physical and network access to the machine. Users should avoid storing passwords or other information that can be used to gain access to other campus computing resources. Users should not store College passwords or any other confidential data or information on their laptop or home PC or associated media. All such information should be secured after any connection to the College network.

Use of External Services

It is the user's responsibility to adhere to the standards of external networks. The College cannot and will not extend any protection to users should they violate the policies of an external network.

Printouts

Users are responsible for the security and privacy of hard-copy versions of College information, data, and reports.

Found Media

One common vector of attack used by hacks and crackers is to “salt” common areas with removable media like thumb drives, CD or DVD ROMS. If media is “found” in a common area on campus the user should turn the media or device into the Information Technology Department for evaluation and/or disposal.

Appendix C: Student Laboratory & Network Code of Practice

General

The College provides access to the College network for administrative, academic, research or study purposes only. The network is a valuable but limited resource, which must be shared with others. It is your obligation to use the facilities in an efficient, ethical, legal and responsible manner, in accordance with the College’s “Code of Practice in the Use of Computing, Learning and Network Facilities” (Appendix A) “Appropriate and Reasonable Use of Electronic Mail” (Appendix A) and the Code of Conduct specified below. Grossly improper behavior may be grounds for termination of your access or be subject to other penalties, up to and including disciplinary action.

Account Management

1. Your account is provided by the College in your name for your use only.
2. You must not share your account with family, friends or make your password available to any other person.

3. Passwords expire every 90 days and must be reset. The system does not allow the reuse of passwords.
4. You may not use the account of any other person. If you inadvertently gain such access to any unauthorized information, you should advise the ITU Help Desk immediately.
5. In certain circumstances you may share an account with others where shared duties apply. Such accounts will be specifically authorized by the Executive Director of Information Technology or delegate. In such cases all sharers are jointly responsible for the account but may not share with others outside the group.
6. You MUST NOT attempt to find the password of another user or access their account in an unauthorized username.

Appropriate Electronic Behavior

Users of the College network and the Internet are asked to comply with guidelines of network etiquette (netiquette). Netiquette is based on the use of good manners and common sense. Some are:

1. Always acknowledge electronic mail.
2. Limit your email to a single screen of text where possible.
3. Do not send large files as email attachments.
4. Do not use offensive language.
5. Be polite to other users of the Internet.

Appropriate Use

Avoid wasting network resources:

1. FTP should be used for academic and study purposes only.
2. Participating in multi-user Internet applications (e.g. MUDS, MOO's) is NOT acceptable use unless authorized and monitored by your instructor as being an essential component of your studies and ITU has been notified prior to its use.

Illegal Activities

1. Do not download or copy software without appropriate authority or license.
2. It is an offense to knowingly inject viruses into any system or otherwise access any system for which you have not received prior authorization from the owner / custodian.
3. It is an offense to transmit material, which is offensive, obscene, harassing, slanderous, damaging to the files or programs of others, or which violate any applicable law.

Laboratory Etiquette

1. No food, drink, or cigarettes are to be consumed in the labs.
2. Avoid excessive noise. It annoys other users. Cell phones should be set to silent operation.
3. Cell phone conversations should be conducted outside the labs.
4. The number of workstations is limited. If possible, please limit your sessions to 30 minutes when others are waiting.
5. Please be courteous to staff and fellow users.
6. Game playing is not desirable. It is forbidden when there are people waiting unless authorized in writing by your lecturer as part of your course.
7. You are required to comply with any instruction by a College staff member or Lab Assistant.

Appendix D: Internet Conditions, Standards, and Guidelines

Scope

The resources, services, and inter-connectivity available via the Internet introduce new opportunities and new risks. In response to the risks, this statement describes the Mohave Community College official policy regarding Internet use and security. It applies to all College employees, students, contractors, and temporaries who use the Internet with College computing, learning or networking resources, as well as those who represent themselves as being connected with Mohave Community College.

Transmission of Information

Downloading

ALL downloaded software should be applicable to work at MCC. All software downloaded from non-College sources via the Internet must be screened with virus detection software prior to being invoked. Whenever the provider of the software is not trusted, contact ITU for assistance. ***Remember that not all "freeware" or "shareware" is available for evaluation by the college. Some license agreements specifically forbid use of the software in a corporate environment.***

Suspect Information

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Contacts

Contacts made over the Internet should not be trusted with College information unless reasonable steps have been taken to ensure the legitimacy of the contacts. This applies to the release of any internal College information.

Information Security

Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, College, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods. Credit card numbers, log-in passwords, and other parameters that can be used to gain access to College systems, networks and services, must not be sent over the Internet in readable form. Credit card numbers shall not be stored on any server accessible through the Internet.

Software Security

College computer software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-College party for any purposes other than College purposes expressly authorized by the Executive Director of Information Technology or Campus President.

Exchanges of software and/or data between College and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected. Regular business practices--such as shipment of software in response to a customer purchase order--need not involve such a specific agreement since the terms are implied.

The College strongly supports strict adherence to software vendors' license agreements. Adherence to these agreements is subject to random audits by these vendors. When College computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Personnel Security

Privacy

Staff using College information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers should not send information over the Internet if they consider it to be private. Any doubts regarding the privacy of information should be resolved by contacting ITU.

Right to Examine

At any time and without prior notice, College management reserves the right to examine email, personal file directories, and other information stored on College computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of College information systems.

Resource Usage

Mohave Community College encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not College time. Likewise, games, news groups, and other non-College activities must be performed on personal, not College time. Use of College computing, learning and network resources for these personal purposes is acknowledged so long as the incremental cost of the usage is negligible, and so long as no College activity is pre-empted by personal use.

Public Representations

Staff may indicate their affiliation with the College in bulletin board discussions and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an email address. In either case, whenever staff provide an affiliation, they must also clearly indicate the opinions expressed are their own, or not necessarily those of Mohave Community College. All external representations on behalf of the College must first be cleared with the Executive Director of Information Technology, Director of MPIO, or the Campus President. Additionally, to avoid libel problems, whenever any affiliation with the College is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited.

All staff must not publicly disclose internal College information via the Internet that may adversely affect the College's relations or public image.

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If a user is working on a research and/or development project, or related College matters, all related postings must be cleared with the Executive Director of Information Technology or Campus President prior to being placed in a publically accessible forum or posting on the Internet.

Access Control

Unless the prior approval of ITU has been obtained, staff may not establish Internet or other external network connections other than the connections provided by ITU.

Likewise, unless ITU has approved in advance, users are prohibited from using new or existing Internet connections to establish new communication channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services.

Reporting Security Problems

ITU must be notified **immediately** when:

- Sensitive College information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.
- Unauthorized use of College information systems has taken place, or is suspected of taking place.
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
- There is any unusual systems behavior, such as missing files, frequent workstation crashes, misrouted messages.

Security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users must not attempt to probe computer security mechanisms at Mohave Community College campuses or other Internet sites. If users probe security mechanisms, alarms will be triggered and College resources will needlessly be spent tracking the activity.

Unless prior written authority has been obtained from ITU, files containing tools that could be used for unauthorized access to computer systems, or other suspicious material may be taken as *prima facie* evidence of unauthorized access activity and may expose the user to disciplinary procedures.

Penalties

Violations of these computer security policies can lead to withdrawal and/or suspension of system and network privileges and/or disciplinary action.

Information Privacy Principles

The following Information Privacy Principles are presented as guidelines for all members of Mohave Community College.

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and where appropriate, with the knowledge or consent of the persons involved.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data is collected should be specified not later than at the time of collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change or purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used, for purposes other than those specified in accordance with **Principle 7.3 except** with the consent of the person or persons involved; or by the authority of law.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and contact information of the data custodian.

Individual Participation Principle

An individual should have the right:

1. To obtain from a data custodian, or otherwise, confirmation of whether or not the custodian has data relating to that person;
2. To have communicated to the person, data relating to that person:

   a. within a reasonable time;
   b. at a charge (if any) that is not excessive;
   c. in a reasonable manner; and
   d. in a form that is readily intelligible;

3. To be given reasons if such request is denied, and to be able to challenge such denial; and
4. To challenge data relating to the person and if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

A data custodian should be accountable for complying with measures which give effect to the principles stated above.

Appendix E - Standards and Guidelines for Strategic Systems

1. Strategic System Platforms

1.1. Definition of 'Strategic'

A *strategic* system is one that meets *several* of the following criteria:

- Is critical to the mission of the College.
- Affects large parts of the College.
- Yields College-wide benefits.
- Is large.
- Is expensive.

Note: By this definition, the IRIS and Dental Hygiene systems qualify as strategic system platforms.

1.2. Management of Strategic Systems

The following policies apply in the management of strategic systems:

1. Strategic platforms will be managed and operated by ITU.

2. The designated custodian of the application will manage strategic Applications.
   a. The designated custodian (software owner) will be listed in the Server List maintained by ITU.

1.3. Physical Security

The following standards of physical security of strategic platforms must be met:

- Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.
- Air temperature and humidity must be controlled to within acceptable limits.
- Platforms must be electrically powered via UPS to provide the following:

    - Minimum of 15 minutes' operation in the event of a power blackout.
    - Adequate protection from surges and sags.
    - Trigger an orderly system shutdown when deemed necessary.

1.4. Physical Access

- Premises will be staffed and controlled by designated ITU staff.
- External doors will remain locked, preferably with electronic locks.
- There will be security screens on all external windows.

1.5. User Access to Network

1.5.1. New Users

New Network *userid*'s will be handled as follows:

- Written notification from HR (EAF) must be submitted to ITU for new employees.
- The HR notification form will be kept in the ticketing system for reference.
- The new employee *userid* and *temporary password* will be e-mailed.
- New students receive an e-mail indicating the student's *userid* and temporary password.
- The access level will be based on the principle of least privilege.

1.5.2. Terminating Users

The *userids* of persons leaving the College or no longer requiring access will be disabled.

- Human Resources personnel, via email, shall notify ITU within 24 hours of an employee leaving the employ of the College. All computer files related to that individual will be referred to the data custodian for disposition.
- *Userids* for students which have become inactive will be disabled immediately. The associated computer files will be referred to the system custodian for disposition.

1.6. Fire Detection and Control

- There will be smoke and thermal detectors on the premises.
- Under floor areas will have smoke and water detectors.

1.7. Data Integrity

- Security backups of all data will be made daily, weekly, or monthly depending on the system.
- The backup regime must meet the following criteria:

  - Enable recovery to the last backup for the affected system.
  - Provide at least one more level of backup to a previous time, to cover the case of the failure of the primary backup media.

- There should be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.

- There should be a validation of security backups at least once every six months.

1.8. Password Aging

If the Network Operating System provides the facility, automatic Password Aging should be enforced. The life of a password should be no more than 90 days.

1.9. Disaster Recovery Plan

There will be a Disaster Recovery Plan for strategic systems, this plan will be maintained by ITU and kept available to authorized personnel in the Disaster Recovery Cache.

1.10. Documentation

Procedures reflecting these policies are documented within the ITU *Internal Security Protocols* document.

2. Software Change Control

2.1. Definition

Software Change Control covers the control of all aspects of strategic systems software including the operating system, its associated packages and utilities, third party and College developed applications, together with any command procedures and documentation to support and run them.

2.2. General Obligations

When mid-level to major changes are required to systems software, associated packages and utilities, applications software, command procedures, or documentation, it is essential that the changes are:

- appropriately authorized and approved
- thoroughly tested
- sufficiently documented
- implemented at an appropriate time.

Any change must only be transferred into the production environment when approved by the appropriate System Custodian.

Sound software security management requires the procedures to manage the change control for applications and systems changes are clearly defined. There must be a set of Software Change Control Procedures to assist the process.

2.3. Change Control Responsibilities

Specific personnel will be given the responsibility for the implementation of changes by undertaking appropriate testing in the test environment, and, subject to the appropriate approvals, moving the changes to the production environment. All elements of the system will be subject to Software Change Control Procedures.

2.4. Change Control Environment

Where possible, three separate environments should be maintained for each strategic system:

- development
- testing
- production

Migration of software between environments should only be undertaken after obtaining the appropriate sign-offs as specified in the Software Change Control Procedures.

New software and changes to existing software should be prepared in the *Development Environment* by appropriately authorized development or applications support staff. Applications should be specified, designed and coded according to the College's systems development methodology (APT).

Once assessed as satisfactory, the new or modified software should be transferred to the *Testing Environment* for systems and acceptance testing by an appropriate testing group, according to an agreed test procedure. Changes to software are not permitted in the testing environment.

Following successful completion of testing and approval by the appropriate systems custodian, the new or modified software should be transferred to the *Production Environment* for implementation under the control of ITU Operations staff. A contingency plan to enable the software to be restored to its previous version in the event that the implementation is unsuccessful should be prepared where appropriate.

2.5. Documentation

<u>Change Control Procedures</u>

Procedures reflecting these policies must be documented in the ITU Software Change Control Procedures.

<u>Software Change Request</u>

No software change is to be undertaken without an appropriately authorized software Change Management request. The Change Management request is also the principal documentation to be completed for the software change management process.

Technical, Operations and End User Documentation

Appropriate documentation in respect of each software change must be completed in sufficient detail and accepted before the change is implemented in the production environment.

3. Communications

Network access can be categorized into three major areas:

1. Campus Local Area Network
2. External Access
3. Intercampus Network (between MCC campuses)

The College has varying degrees of control decisions affecting security management of these areas:

1. Total control over the campus LAN and Intercampus Network, given that ITU staff plan, install, manage, and maintain these systems.

2. No control over the Internet

3.1. Campus Local Area Networks

3.1.1. Physical Security

The following standards of physical security campus local area networks must be met:

- Premises housing network control equipment must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.
- External building ducts must conform to College standards of service reticulation.
- Internal building distribution of cables within ceiling, wall or floor cavities must be reticulated within protective conduits.
- Air temperature and humidity must be controlled to within equipment defined limits.
- Network electronics must be powered via Un-interruptible Power Supplies to provide the following:

1. Minimum of 15 minutes' operation in the event of a power blackout.
2. Adequate protection from surges and sags.

3.1.2. Physical Access

- Access to areas housing network electronics should be controlled by designated ITU staff only.
- Doors to areas housing network electronics will be locked with a unique key, the distribution of which will be determined by ITU staff and the Executive Director of Information Technology.

3.1.3. Data Integrity

3.1.3.1. Eavesdrop Protection

Subnet----With the present security strategy, users are categorized into security sub-groups (students, administrative staff, and general staff). However, the creation of each security sub-group requires a duplication of physical network infrastructure and increased central management. The end result of which is not always totally effective - e.g. the Admissions users are an isolated networking sub-group, but if admissions staff connect to the network from any other location on campus, then they forfeit all of the security of their designated sub-group.

By utilizing eavesdrop protection at the network hardware level, full network flexibility on campus is retained at the user end, with an unbreakable system of eavesdrop protection.

Mohave Community College Campus Local Area Networks are protected by a hardware level of eavesdrop protection.

3.2. Inter-campus Network

The inter-campus network consists of leased telecommunication lines connecting College campus locations to the College LAN. All policies and guidelines established for the central campus LAN apply to the extended campuses.

3.3. Regional and Wide Area Networks

Protection from illegal entry from public Regional and Wide Area networks is usually provided by network firewalls. However, with the diverse nature of the College's business and the public nature of the services that it delivers, firewall solutions are not sufficient. Many of the College's customers are external to the campus and use the public networks to access College teaching, research and library material. Also, academic staff can be highly mobile, requiring access to the College network from various external locations, often from overseas.

Because of the nature of Wide Area Networks (WAN) there are only limited security measures that can be taken. Security Policy for Strategic Systems must rely heavily on software applications and general computer controls. The risks of transmitting information over the WAN must be considered when:

- Determining the nature of information to be sent over the WAN.
- Granting approval for new applications, which involve the transmission of information over the WAN.

Appendix F – Standards and Guidelines for Desktop Computers

1. Desktop/Laptop Computer Security Guidelines

1.1. Definition

Desktop/laptop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units.

1.2. General Obligations

Users and custodians of desktop/laptop computers are subject to the “Conditions of Use” and “Code of Practice” sections specified in the College’s IT Security Manual.

1.3. Hardware Security

1. Lock offices. Office keys should be registered and monitored to ensure they are returned when the owner leaves the College.

2. Secure desktop/laptops in public areas. Equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case.

3. Secure hard disks. External hard disks should be secured against access, tampering, or removal and are required to be encrypted.

4. Locate computers away from environmental hazards.

5. Store critical data backup media in fireproof vaults or in another building.

6. Register all College computers on the domain.

1.4. Access Security

- Utilize password facilities to ensure that only authorized users can access the system. Where the Desktop/Laptop is located in an open space or is otherwise difficult to physically secure then consideration should be given to enhanced password protection mechanisms and procedures.
- Users will be assigned accounts on the appropriate domains in accordance with industry wide security standards.
- In order to maintain trusted login, no users should use more than one login except in the event of an emergency.
- Password guidelines:

  - Length should be **at least** 10 characters and contain at least one character from the following character sets: Uppercase, Lowercase, Numbers, and Symbols.
  - Avoid words found in the dictionary and include at least one numeric character. (Six-character passwords may suffice for non-dictionary words.)
  - Choose passwords not easily guessed by someone acquainted with the user. (For example, passwords should not be maiden names, or names of children, spouses, or pets.)
  - Do not write passwords down anywhere.
  - Change passwords every 90 days.
  - Do not include passwords in any electronic mail message.

1.5. Data and Software Availability

- Back up and store important records and programs on a regular schedule.
- Check data and software integrity.
- Request immediate assistance from Help Desk personnel to repair software problems.

1.6. Confidential Information

- Encrypt sensitive and confidential information where appropriate.
- Monitor printers used to produce sensitive and confidential information.
- Overwrite or “Wipe” sensitive files on fixed disks, floppy disks, or cartridges.

1.7. Software

Software is protected by copyright law. Unauthorized copying is a violation of College Copyright policy. Anyone who uses software should understand and comply with the license requirements of the software. The College is subject to random license audits by software vendors.

1.8. Viruses

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

To decrease the risk of viruses and limit their spread:

- Periodically run Anti-Virus software scans on your system to include "all files."
- Allow your virus software to update definitions daily.
- Contact ITU for assistance in installing software.
- Unplug computer from the network and contact the Help Desk immediately if you suspect virus contamination.

1.9. Computer Networks

Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks.

While ITU has responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment.

The following considerations and procedures must be emphasized in a network environment:

- Check all files downloaded from the Internet. Avoid downloading shareware files.
- Test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on College networks.
- Choose passwords with great care to prevent unauthorized use of files on networks or other personal computers and change them every 90 days.
- Always BACK-UP your important files.
- Use (where appropriate) encrypting/decrypting and authentication services to send confidential information over a College network.
- Never store College passwords or any other confidential data or information even temporarily.

Appendix G – MCC Copyright Policy

Mohave Community College details their Copyright Act Compliance policy in the Course Catalog. The current version of this document is available online at http://www.mohave.edu/print/244.asp.

Appendix H – MCC Intellectual Property Policy

Mohave Community College details their Academic Integrity policy in the Course Catalog. The current version of this document is available online at http://www.mohave.edu/print/244.asp.

Appendix I – Glossary of Terms

A

Access control: Measures that limit access to information or information processing resources to those authorized persons or applications.
Account harvesting: A method to determine existing user accounts based on trial and error. Giving too much information in an error message can disclose information that makes it easier for an attacker to penetrate or compromise the system.
Account number: The payment card number (credit or debit) that identifies the issuer and the particular cardholder account.
Acquirer: A bankcard association member that initiates and maintains relationships with merchants that accept Visa or MasterCard cards.
Asset: Information or information processing resources of an organization.
Audit Log: A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. Sometimes specifically referred to as a security audit trail.
Authentication: The process of verifying identity of a subject or process.
Authorization: The granting of access or other rights to a user, program, or process

B

Backup: A duplicate copy of data made for archiving purposes or for protecting against damage or loss.

C

Card-validation code:
The three-digit value printed on the signature panel of a payment card used to verify card-not present transactions. On a MasterCard payment card this is called CVC2. On a Visa payment card this is called CVV2.
Cardholder: The customer to whom a card has been issued or the individual authorized to use the card.
Cardholder data: All personally identifiable data about the cardholder and relationship to the Member (i.e., account number, expiration date, data provided by the Member, other electronic data gathered by the merchant/agent, and so on). This term also accounts for other personal insights gathered about the cardholder ‘i.e., addresses, telephone numbers, and so on).

Compromise: An intrusion into a computer system where unauthorized disclosure, modification, or destruction of data may have occurred.
Console: A screen and keyboard which allows access and control of the server / mainframe in a networked environment.
Cookies: A string of data exchanged between a web server and a web browser to maintain a session. Cookies may contain user preferences and personal information.

D

Database: A structured format for organizing and maintaining information that can be easily retrieved. A simple example of a database is a table or a spreadsheet.
Default accounts: A system login account that has been predefined in a manufactured system to permit initial access when the system is first put into service.
Default password: The password on system administration or service accounts when a system is shipped from the manufacturer, usually associated with the default account. Default accounts and passwords are published and well known.
Dual Control: A method of preserving the integrity of a process by requiring that several individuals independently take some action before certain transactions are completed.
DMZ (de-militarized zone): A network added between a private network and a public network in order to provide an additional layer of security.

E

Egress: Traffic leaving the network.
Encryption: The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption), against unauthorized disclosure.

F

Firewall: Hardware and/or software that protect the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet must have a firewall to prevent outsiders from accessing its own private data resources.

H

Host: The main hardware on which software is resident.

I

Information Security: Protection of information for confidentiality, integrity and availability.
Ingress: Traffic entering the network.

Intrusion detection Systems: An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
IP address: An IP address is a numeric code that uniquely identifies a particular computer on the Internet.
IP Spoofing: A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

K

Key: In cryptography, a key is a value applied using an algorithm to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.

M

Monitoring: A view of activity on a network.

N

Network: A network is two or more computers connected to each other so they can share resources.
Network Address Translation (NAT): The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network.
Non student users: Any user, excluding students, that accesses systems, including but not limited to, employees, administrators, and third parties.

P

Password: A string of characters that serve as an authenticator of the user.
Patch: A quick-repair job for a piece of programming. During a software product's beta test distribution or try-out period and later after the product is formally released, problems will almost invariably be found. A patch is the immediate solution that is provided to users.
Penetration: The successful act of bypassing the security mechanisms of a system.
Penetration Test: The security-oriented probing of a computer system or network to seek out vulnerabilities that an attacker could exploit. The testing involves an attempt to penetrate the system so the tester can report on the vulnerabilities and suggest steps to improve security.
Policy: Organizational-level rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.

Procedure: A procedure provides the descriptive narrative on the policy to which it applies. It is the “how to” of the policy. A procedure tells the organization how a policy is to be carried out.
Protocol: An agreed-upon method of communication used within networks. A specification that describes the rules and procedures products should follow to perform activities on a network.

R

Risk Analysis: Also known as risk assessment, a process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.
Router: A router is a piece of hardware or software that connects two or more networks. A router functions as a sorter and interpreter as it looks at addresses and passes bits of information to their proper destinations. Software routers are sometimes referred to as gateways.

S

Sanitization: To delete sensitive data from a file, a device, or a system; or modify data so that data is useless for attacks.
Security Officer: The person who takes primary responsibility for the security related affairs of the organization.
Security policy: The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Sensitive data: Data whose unauthorized disclosure may be used in fraudulent transaction.
Separation of duties: The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.
Server A computer that acts as a provider of some service to other computers, such as processing communications, file storage, or printing facility.
SQL injection: A form of attack on a database-driven Web site in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization’s host computers through the computer that is hosting the database.
SSL: An established industry standard that encrypts the channel between a web browser and Web server to ensure the privacy and reliability of data transmitted over this channel.

System Perimeter Scan: A non-intrusive test which involves probing external-facing systems and reporting on the services available to the external network (i.e. services available to the Internet).

T

Tamper-resistance: A system is said to be tamper-resistant if it is difficult to modify or subvert, even for an assailant who has physical access to the system.

Threat: A condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.

Token: A device that performs dynamic authentication.

Transaction data: Data related to an electronic payment.

Truncation: The practice of removing a data segment.

Two-factor authentication: Authentication that requires users to produce two credentials - something they have (e.g., smartcards or hardware tokens), and something they know (e.g., a password). In order to access a system, users must produce both factors.

U

UserID: A character string that is used to uniquely identify each user of a system.

V

Virus: A program or a string of code that can replicate itself and cause the modification or destruction of software or data.

Vulnerability: A weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

Vulnerability Scan: An automated tool that checks a merchant or service provider’s systems for vulnerabilities. The tool remotely reviews networks and Web applications based on the external-facing Internet protocol (IP) addresses. Scans identify vulnerabilities in operating systems, services, and devices that could be used by unauthorized individuals to target the company’s private network.

Revisions

Date	Revision No.	Type	Description
		Major	

Document Approval Procedures:
Document Submitted By:

Signature: ____________________________________ Date: _________________

Name: _______________________________ Title: _________________

Security and Compliance Review:

Signature: ____________________________________ Date: _________________

Name: _______________________________ Title: _________________

Institution Senior Management Approval - Final:

Signature: ____________________________________ Date: _________________

Name: _______________________________ Title: _________________