5.275	Information Technology	5.275

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

Members of the MCC community are expected to use these resources in a responsible, ethical and legal manner. Examples of technology resources include, but are not limited to, central computing services, the college-wide data network, electronic mail, Internet access, voice mail, classroom and library computing, online college resources, sensitive data, shared network resources, and system and data security and reliability.

While MCC takes reasonable measures to ensure network security, it cannot be held accountable for unauthorized access to its technology resources by other users, both within and outside the MCC community. Moreover, MCC cannot guarantee users protection against loss due to system failure, fire, etc., or against loss of content or hardware damage on personal computers.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-A	Information Technology Privacy	5.275-A

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

Electronic messaging, Internet access via an MCC network and other college-owned technology systems are Mohave Community College's property and are intended for business purposes. Employees do not have any express or implied privacy rights in any matter created, received or sent through the college's technology systems including' but not limited to, emails, voice mails, and sites visited on the internet. Contents of emails, both work-related and personal, and the history of internet sites visited are subject to monitoring.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-B	Information Technology	5.275-B
	Acceptable Use Standards – Principles, Purpose, Scope	

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

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 the Acceptable Use Standards 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 MCC students, faculty, and staff.

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

Purpose:

The standards set forth 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 the security standards set forth, 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. These standards are in place to protect the MCC community and to ensure the smooth, secure operation of MCC's information technology systems.

Scope:

The standards apply 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.

5.275-B	Information Technology	5.275-B
	Acceptable Use Standards – Principles, Purpose, Scope	

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-C	Information Technology	5.275-C
	Acceptable Use – Generally Prohibited Conduct	

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

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. Failing to use good judgement with respect to personal use of IT resources. 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.

5.275-C	Information Technology	5.275-C
	Acceptable Use – Generally Prohibited Conduct	

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-D	Information Technology	5.275-D

Acceptable Use – Security and Proprietary Information

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

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.

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 8 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.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-E	Information Technology	5.275-E
	Acceptable Use – System and Network Access	

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

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.

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.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-F	Information Technology	5.275-F
	Acceptable Use – Email and Electronic Communications	

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

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.

Email and Electronic Communications

1. Use of MMC 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.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

Acceptable Use Standards - Compliance

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

Compliance

The Information Technology department will verify compliance to these standards through various methods, including but not limited to business reports, internal and external audits, audit tools, and security related hardware and software tools.

The Information Technology team routinely monitors inbound, outbound, and internal network traffic for the purposes of compliance and network maintenance. Mohave Community College reserves the right to audit systems and network traffic to ensure compliance with the standards.

Exceptions to the Acceptable Use Standards must be approved by the Chief Information Officer in advance, and in writing.

Faculty or staff found to be in violation of the standards may be subject to disciplinary action as outlined in the Policy and Procedure Manual.

Students found to be in violation of the standards may be subject to disciplinary action under the Student Code of Conduct in the Student Handbook.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-H	Information Technology Disaster Recovery	5.275-H

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

Disaster Recovery

It is the intention of Mohave Community College to provide, as allowed by the IT infrastructure in place, an ability to:

- Perform backups of critical data systems that consist of a duplicate copy of data, configuration, and operating systems made for archival purposes or to protect against damage or loss.
- Support availability of these backups that will allow affected systems to be brought back online to support the college
- Communicate status of these efforts to systems staff responsible for bringing these affected systems back online
- Communicate status of recovery to system users on efforts bring affected systems back online

The college shall prepare Information Technology Disaster Recovery plans for the following classes/tiers of systems in use at the college.

- Tier 1 systems are deemed mission critical systems for the college and are installed at remote sites
- Tier 2 systems are deemed mission critical systems for the college and are installed on the various college campuses
- Tier 3 systems are deemed non-critical and systems used for initial testing, training and future implementation.

The Information Technology Disaster Recovery Plan shall support business continuity planning for the college as a whole as well as planning at the department and campuses level.

The non-confidential portions of the Information Technology Disaster Recovery Plan are available at MCC Information Technology Disaster Recovery Plan.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-I	Information Technology Security Processes	5.275-I

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

Security Processes

It is the intention of Mohave Community College 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. These efforts are documented in the Information Technology Security Manual.

The manual:

- Defines the elements that constitute Information Technology security at Mohave Community College.
- Explains the need for Information Technology security.
- Specifies the various categories of Information Technology data, equipment, and processes subject to this policy.
- Indicates, in broad terms, the Information Technology security responsibilities of the various roles in which each member of the College may function.
- Indicate appropriate levels of security through standards and guidelines.

The scope of the Information technology Security manual includes

- Confidentiality of Information
- Integrity of Information
- Accessibility of information
- Information Technology physical/virtual assets
- Efficient and Appropriate Use
- System Availability

The non-confidential portions of the Information Technology Security Manual are available at MCC Information Technology Security Manual.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*

5.275-J	Information Technology Permission Processes	5.275-J

The college shall maintain the institution's information technology systems in support of instruction and college business at a level as close to state-of-the-art as possible within the constraints of funding and ability to benefit (ARS 15-1445).

Permissions Processes

In order to ensure the integrity and security of employee and student data, Mohave Community College assigns data system (currently Jenzabar EX) permissions to each individual position control number (PCN) whereby permissions follow a position rather than a person. Jenzabar module managers, individually and collectively in conjunction with supervisors, decide which permissions each position needs to perform their job duties. A review of the permissions assigned to each position is administered annually.

Assigning Permissions

There are four methods by which an employee/worker can obtain permissions to Jenzabar:

1. The first method is by being hired or having a position transfer. In this instance, the already established assigned permissions from the PCN attach to the permissions of the new hire/transfer.

2. The second method is upon request of an employee's supervisor, with a statement that an employee with this PCN needs additional permissions to complete the tasks assigned to the position. These added permissions become a part of the PCN regular permissions, and transfer to other PCN holders. These requests must be approved by the supervisor, the meta-module managers (those ove3rseeing several or critical modules), and the chief information officer.

3. The third method is upon the request of an employee's supervisor, with a statement that an employee is performing tasks temporarily outside the permissions needed by the PCN and thus needs additional permissions. The third method is generally time-restricted, where the additional permissions are needed temporarily. These added permissions do not become a part of the PCN regular permissions and will be removed either at a stated date or at the time the employee is no longer assigned that PCN. These requests must be approved by the supervisor, the meta-module managers, and the chief information officer.

4. The fourth method occurs when a new position/PCN is created. When a new position and subsequent PCN is created by the human resources department, module managers (those overseeing several, or critical modules) review the position description special permissions in collaboration with the supervisor, and, with the approval of the chief information officer, PCN permissions are assigned.

Permissions Reduction

Supervisors will also use this process to reduce permissions where they determine that a position/PCN does not need all the permissions assigned. In this instance, the chief information officer will approve the reduction and the Chief Human Resources Director will be notified of the change.

Workers with no PCN

Two categories of MCC workers are not assigned PCNs: Student workers and Temporary Workers. In these cases, Permission Groups are established and permissions are approved through the same approval process.

Permissions Request Form and Details

Details of the permissions request process, including objections, work flow, electronic signatures and time stamps are addressed on the permissions request form.

Date of Adoption: *Adoption of Manual*

References: *ARS 15-1445*