



## COLLEGE ADMINISTRATIVE PROCEDURE MANUAL

Procedure Title	Procedure Number	Page(s)	Date Adopted:
Technology Resources	CR - I	15	08/26/2025

### BASED ON BOARD POLICY

Section	Policy Title	Policy Number	Date Adopted:
C — Business and Support Services	Technology Resources	CR	08/26/2025

### PURPOSE

This procedure defines primary rights and responsibilities for all users of information and information resources that belong to, or are under the control of McLennan Community College (MCC).

This procedure applies to the use of information, electronic and computing devices, and network resources to conduct college business or interact with internal networks and business systems, whether owned or leased by MCC or a third party. All students, faculty, employees, contractors, consultants, temporary, and other workers at MCC and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with MCC policies, procedures and standards, and local laws and regulation. The purpose of the implementation of this information technology standard is to provide a set of measures that will mitigate information-security, privacy, and accessibility risks. This procedure applies to students, faculty, staff, contractors, consultants, and temporary and other workers at MCC, including all personnel affiliated with third parties.

### PROCEDURE

#### 1. ACCEPTABLE USE

##### 1.1. GENERAL

- 1.1.1. As an institution of higher learning, MCC encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. MCC recognizes the importance of information technology to students, faculty and staff in scholarly pursuits, professional development, service activities, class-related work activities, and personal development. In particular, access to networked electronic information (e.g., the Internet) supports the academic community by providing a link to electronic information in a variety of formats covering all academic disciplines.

- 1.1.2. As such, MCC makes available information resources (e.g., facilities, networks, hardware, software) and information for use by students, staff, faculty, and invited guests. Such use must be acceptable, i.e., it must comply with all relevant law and policy, including federal law (e.g., FERPA), state law (e.g., TAC 202, TAC 213), system policies and regulations, MCC rules and procedures, relevant IT standards, and MCC's General Conduct Policy.
- 1.1.3. The intention for publishing an Acceptable Use procedure is not to impose restrictions that are contrary to MCC's established culture of openness, trust, and integrity. MCC is committed to protecting its students, faculty, staff, and the college from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort involving the participation and support of all students, faculty, staff and/or any affiliate who deals with information and/or information systems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

## 1.2. ACCEPTABLE USE POLICIES

- 1.2.1. Only Authorized Use - A user shall not use or attempt to use MCC information-resources or MCC information unless and until the Owner of the information resource or information has authorized such use.
  - 1.2.1.1. A user shall use MCC information-resources or MCC information only in the manner authorized by the Owner. For example, if an Owner has authorized a user only to view certain information, then the user is not permitted to edit that information even if the user has the technical ability to do so.
- 1.2.2. Data Protection - MCC proprietary information stored on electronic and computing devices whether owned or leased by MCC, the employee, or a third party, remains the sole property of MCC.
  - 1.2.2.1. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of MCC proprietary information. This can be done by emailing [helpdesk@mclennan.edu](mailto:helpdesk@mclennan.edu) or calling (254) 299-8077.
- 1.2.3. Only Lawful Use - All use must comply with all relevant law and policy, including federal law, state law, system policies and regulations, and MCC rules, procedures, and standards. Under no circumstances is a student, faculty, or staff member of MCC authorized to engage in any activity that is illegal under local, state, federal

or international law while utilizing MCC owned resources.

- 1.2.4. Personal Use - Employees are responsible for exercising good judgment regarding the reasonableness of personal use. 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.
- 1.2.5. Protect Confidential and Controlled Information - Users must protect confidential and controlled information from unauthorized disclosure, modification, or deletion. See, for example, Family Educational Rights and Privacy Act ([FERPA](#)), Texas Public Information Act ([TPIA](#)), and the Payment Card Industry Data Security Standard ([PCI-DSS](#)).
- 1.2.6. No Indecent or Obscene Material - Users shall not use MCC information resources to intentionally access, create, store, or transmit material which MCC may deem to be indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the MCC official processes for dealing with academic ethical issues).
- 1.2.7. Passwords - System level and user level passwords must comply with the Password procedure. Providing passwords or sharing access to another individual, either deliberately or through failure to secure the password, is prohibited (e.g. Storing password on note taped to monitor, etc).
- 1.2.8. Physical Access - All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 5-minutes or less. You must lock the screen or log off when the device is unattended.
- 1.2.9. Respect Copyright - Intellectual property laws (e.g., copyright) apply to the electronic environment and users shall respect such laws. Users should assume that information (e.g., documents, messages, software) stored on or communicated by MCC information resources are subject to copyright unless specifically stated otherwise. Users shall not make unauthorized copies of copyrighted software or other copyrighted materials such as music, films, and textbooks.
- 1.2.10. Only Ethical Use - All use of MCC information resources and MCC information must be ethical.

1.2.11. Security Incident Reporting - Users shall report to the ISS Help Desk [[helpdesk@mclennan.edu](mailto:helpdesk@mclennan.edu) or (254) 299-8077] any weaknesses in the security of MCC's information resources, or any incidents of possible misuse or violation of this or any other policy or procedure related to the security of MCC's information resources.

1.2.11.1. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

## **2. UNACCEPTABLE USE**

2.1. The following activities are, in general, prohibited. Students, faculty, and staff may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

### **2.1.1. System and Network Activities**

2.1.1.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by MCC.

2.1.1.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which MCC or the end user does not have an active license is strictly prohibited.

2.1.1.3. Accessing data, a server, or an account for any purpose other than conducting MCC business, even if you have authorized access, is prohibited.

2.1.1.4. Exporting software, technical information, encryption software or

technology violating international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.

- 2.1.1.5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, macros, keyloggers, spyware, ransomware, etc.).
- 2.1.1.6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- 2.1.1.7. Using an MCC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- 2.1.1.8. Making fraudulent offers of products, items, or services originating from any MCC account.
- 2.1.1.9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- 2.1.1.10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- 2.1.1.11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student, faculty or staff member is not an intended recipient or logging into a server or account that the student, faculty, or staff member is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- 2.1.1.12. Port scanning or security scanning is expressly prohibited unless prior notification to ISS is made [[helpdesk@mclennan.edu](mailto:helpdesk@mclennan.edu) or (254) 299-8077].
- 2.1.1.13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- 2.1.1.14. Circumventing user authentication or security of any host, network, or account.
- 2.1.1.15. Introducing honeypots, honeynets, or similar technology on the MCC's network.
- 2.1.1.16. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- 2.1.1.17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- 2.1.1.18. Providing information about, or lists of, MCC's students, faculty or staff members to parties outside MCC.

#### 2.1.2 Email and Communication Activities

- 2.1.2.2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam, unless it directly relates to the employee's assigned responsibilities within the workplace or reasonably supports legitimate work-related communication and collaboration).
- 2.1.2.3. Any form of harassment via email, telephone or text messaging, whether through language, frequency, or size of messages.
- 2.1.2.4. Unauthorized use, or forging, of email header information.
- 2.1.2.5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- 2.1.2.6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

#### 2.1.3 Blogging and Social Media

- 2.1.3.1 Blogging by employees, whether using MCC's property and systems or personal computer systems, is also subject to the terms and restrictions set

forth in this procedure. Limited and occasional use of MCC's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate MCC's policy or procedure, is not detrimental to MCC's best interests, and does not interfere with an employee's regular work duties. Blogging from MCC's systems is also subject to monitoring.

- 2.1.3.2 MCC's Data Classification policy also applies to blogging. As such, Employees are prohibited from revealing any MCC confidential or proprietary information, trade secrets or any other material covered by MCC's Data Classification policy when engaged in blogging.
- 2.1.3.3 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of MCC and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by MCC's Non-Discrimination and Anti-Harassment policy and procedure.
- 2.1.3.4 Employees may also not attribute personal statements, opinions or beliefs to MCC when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of MCC. Employees assume any and all risk associated with blogging.
- 2.1.3.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, MCC's trademarks, logos and any other MCC intellectual property may also not be used in connection with any blogging activity.
- 2.1.3.6 Postings by employees from a McLennan Community College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of MCC, unless posting is in the course of business duties.

#### 2.1.4. Other Impermissible Use

- 2.1.4.1. Users shall not use MCC information resources or MCC information to purposely engage in activity that may: harass, threaten, or abuse others;

degrade the performance of MCC information resources; deprive an authorized user access to a MCC resource; obtain extra resources beyond those allocated; circumvent MCC information security measures.

- 2.1.4.2. Users shall not otherwise engage in acts against the aims and purposes of MCC as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

### **3. IT PRIVACY**

#### **3.1. GENERAL**

- 3.1.1. Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users in providing privacy in MCC information resources.
- 3.1.2. Users of MCC information resources have a basic right of privacy in 1) the files they own which are stored or communicated by MCC information resources, the activities they perform using MCC information resources. However, this privacy may be subject to limitations. As a public institution, MCC may be required to grant access or to disclose these files and activities to comply with law enforcement investigations, legal subpoenas, or Freedom of Information Act (FOIA) requests.
- 3.1.3. However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.
- 3.1.4. In particular, MCC has the right to examine all information stored on or passing through MCC information resources, and to monitor the activities of any user on MCC information resources so as to, e.g., ensure business continuity, ensure compliance with law and policy, or conduct authorized investigations.

#### **3.2. PRIVACY POLICIES**

- 3.2.1. A file may not be accessed, copied, or modified without prior authorization from the file Owner. This general right to privacy is subject to the following exceptions and limitations:



- 3.2.1.1. The file Owner's right to privacy in their files may be limited by other laws, policy, and procedure. For example, the Texas Public Information Act may require the disclosure of certain data under certain conditions.
- 3.2.1.2. A person in the file Owner's chain of command (i.e., the file Owner's supervisor, that supervisor's supervisor, etc.) may access or copy any of the file Owner's files as long as that person has the authorization of the appropriate person in their own chain of command. The Chief Information and Technology Officer (CITO), his or her designees, and resource Custodians may log, monitor, copy, and examine any information passing through or stored on any MCC information resource for which they are responsible for reasons including, but not limited to:
  - 3.2.1.2.1. Ensuring compliance with applicable law, policy, and procedure;
  - 3.2.1.2.2. Ensuring business continuity (e.g., making backups);
  - 3.2.1.2.3. Monitoring network performance and maintenance activities; or,
  - 3.2.1.2.4. Responding to authorized requests for information from, e.g., auditors or investigators.
- 3.2.2. A user's activities on or with an MCC information resource may not be tracked or recorded without first obtaining authorization from the user. This right of privacy in activities is subject to the following exceptions:
  - 3.2.2.1. The CITO, or designees, and resource Custodians may, without any notification to a user, monitor some, or all, of the user's activities on relevant information resources for MCC-business-related purposes. Examples of such monitoring include logging the phone numbers dialed by a user from their desk phone or recording the web sites a user visited using an MCC workstation.
  - 3.2.2.2. MCC may perform video and audio surveillance as defined in other procedure.

3.2.3. Individuals who have special access to information because of their position have the absolute responsibility not to take advantage of that access.

3.2.3.1. Such individuals should access only that information that is relevant to the particular task, and only so much of that information as is necessary to achieve the task.

3.2.3.2. If, however, in the course of performing the task such individuals find unrelated evidence of impermissible use or other wrongdoing, those individuals are obligated to report an incident.

3.2.3.3. If an individual inadvertently accesses information (e.g., seeing a copy of a test or homework) that could provide personal benefit, such individual has the responsibility to notify 1) the file Owner, 2) their own supervisor, and 3) the file Owner's supervisor.

- 3.2.4. Unless otherwise provided for, individuals whose relationship with MCC is terminated (e.g., student graduates; employee takes new job; visitors depart) are considered to cede ownership of, and hence the right to privacy in, all their files to the information resource custodian. MCC should determine what information is to be retained and delete all other.

## **4. ACCESS CONTROL**

### **4.1. Accounts and Permissions**

- 4.1.1. By default, users are not authorized to create accounts or to modify the permissions associated with any account. Only the Owner of an information-resource or information, or designees, may create an account for that information-resource or information, or modify the permissions associated with that account.

### **4.2. Sessions**

- 4.2.1. A user shall not 1) enable or permit the use of the user's session by a person other than the user without the user being present or 2) use a second user's session without the second user being present. For example, a user may not configure remote control software to permit another person to remotely access the user's session without the user being present.
- 4.2.2. A user shall not leave a session unattended on an MCC computer without enabling a password-protected screensaver.
- 4.2.3. An exception to the two previous provisions is when the user's session is being controlled by an authorized IT employee.

## **5. PROTECTION OF MCC INFORMATION**

### **5.1. Sharing of MCC Confidential Information.**

- 5.1.1. Users should constantly strive to minimize the amount of MCC



confidential information they share with others.

- 5.1.2. Users shall not share MCC confidential information with another entity unless authorized by the information's Owner.

## **6. SECURITY INCIDENT REPORTING**

- 6.1. Users shall report security incidents to the ISS Help Desk [[helpdesk@mclennan.edu](mailto:helpdesk@mclennan.edu) or (254) 299-8077].
- 6.2. The MCC Marketing and Communications office shall handle all interactions with public or private media related to any security incident involving MCC information resources and sensitive information. All MCC employees must refer any questions about these issues to this office.

## **7. HARDWARE AND SOFTWARE**

- 7.1. Users shall not install or use the following software on an MCC information-resource:
  - 7.1.1. Software with no valid license. Software for which the user does not have a valid license (including using personally licensed software for business purposes).
  - 7.1.2. Unsupported/Vulnerable. Commercial software for which the vendor is no longer supplying security patches (e.g., Windows 7, Adobe Acrobat Basic), or open-source software which has one or more known vulnerabilities.
  - 7.1.3. Block listed. Software which is widely recognized by the information-security community as malicious.
  - 7.1.4. Peer-to-Peer Filesharing. P2P filesharing software (e.g., BitTorrent).
  - 7.1.5. Security Software. Software for disabling, circumventing, or testing security measures, e.g., vulnerability scanners, password crackers, and packet sniffers.
  - 7.1.6. Anti-Virus/Anti-Malware. MCC installs anti-virus/anti-malware on all

its machines. Users shall not install additional anti-virus/anti-malware applications.

7.1.7. Encryption. Proprietary encryption software or encryption software that is weaker than AES 128-bit.

7.1.8. Cryptocurrency Mining. Any software for the mining of cryptocurrencies such as Bitcoin.

7.2. Users shall not make the following software changes on an MCC information-resource unless they are also a Custodian of the information resource, and the change is authorized:

7.2.1. Replace the operating system or boot the device from another operating system;

7.2.2. Disable or modify anti-malware and other security software;

7.2.3. Turn off whole disk encryption;

7.2.4. Change the domain to which the machine is attached; and,

7.2.5. Modify the network-interface configurations (e.g., IP address, protocols.).

7.3. Users shall not make the following changes to MCC hardware unless they are also a Custodian of the information resource, and the change is authorized:

7.3.1. Replace or remove internal hardware components, (e.g., network card, hard drive, etc.);

7.3.2. Format an MCC hard drive or other mass storage device;

7.3.3. Attach network extending devices (e.g., access points, routers) to the MCC network; and,

7.3.4. Modify, in any way, MCC network devices (e.g., routers, firewalls), or network cabling other than station cables.

## **8. COMPLIANCE**

8.1. Compliance Measurement. The Department of Information Systems & Services will verify compliance with this procedure and related policies through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

8.2. Exceptions. Any exception to this procedure must be approved by ISS in advance.

## **9. CONSEQUENCES FOR VIOLATIONS**

9.1. All users, including students, staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors, are required to adhere to this MCC procedure, and may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, and MCC policies.

9.2. Individuals found in violation of this procedure are subject to loss of access privileges to MCC information resources (e.g., servers, workstations, email, etc.) and could face disciplinary actions up to and including being expelled, terminated, and/or escorted from the MCC campus. In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

## **DEFINITIONS**

Affiliate – See Contractor.

Authenticators – Account names and passwords, security access cards, tokens, and keys associated with mechanisms that permit access to information resources.

Confidential information – Information that is exempted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records are confidential records. Examples of “Confidential” data include but are not limited to social security numbers, grades, credit card numbers, and personal health records.

Contractor – This refers to an individual, other than a student or employee, with a relationship to MCC such that they receive login granting access to electronic information resources governed by MCC. Other related terms include affiliate, contractor, and contingent worker.



Controlled information – Information that is not generally created for or made available for public consumption but that may be subject to public disclosure through the Texas Public Information Act or similar laws. Examples of controlled information include but are not limited to operational information; personnel records; information security procedures; research; internal communications.

Custodian (of information or an information resource) – A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

Information resources – The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Security Officer (“ISO”) – MCC employee designated by the President to be responsible for all college information-security. The Chief Information and Technology Officer has been designated as the ISO at MCC.

Malware – Software that is designed to operate in a manner that is inconsistent with the intentions of the user, and which typically results in annoyance or damage to the user's information systems, e.g., viruses, spyware.

Owner (of information or an information resource) – Person or entity authorized to decide which users may access the information resource and how. Not necessarily the owner in the sense of property.

Public information – Public information includes all information made available to the public through posting to public websites, distribution through email, or social media, print publications or other media. This classification also includes information for which public disclosure is intended or required.

Texas Administrative Code 202 (“TAC 202”) – Information security standards for information resources purchased by agencies and institutions of higher education in the State of Texas.

Texas Administrative Code 213 (“TAC 213”) – Electronic and information resources law for information resources purchased by agencies and institutions of higher education in the State of Texas.

User – An individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

Vendor – See Contractor.