| ALVIN COLLEGE | ADMINISTRATIVE PROCEDURE MANUAL | |
|---|---|---|
| Section Title:<br>**Acceptable Use of Technology - Employee** | Number: cr-05 | Page: 1 of 12 |
| **BASED ON BOARD OF REGENTS POLICY** | | |
| Policy Title: TECHNOLOGY RESOURCES | Policy Number: CR | |
| Local | Date Adopted: 12/12/2017<br>Last Revised: 8/25/2026 | |

## PURPOSE

Alvin College provides computer and Internet resources to its employees as a means of enhancing efficiency and productivity. Commercial uses are specifically excluded. **All employees are responsible for seeing that these computing resources are used in an effective, efficient, ethical, secure, and lawful manner.** This standard establishes rules and prohibitions that define acceptable use of these computing systems. Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as discipline or legal sanctions under Federal, State, and local law.

## USERS AGREEMENT

All employees of Alvin College computing resources must read, understand, and comply with this Standard, as well as any additional procedures and guidelines established by the administrators of each system. **By using any of these computing systems, users agree to comply with this Standard. Annually, all users are required to acknowledge receipt and understanding of this Standard and agree in writing to comply with such Standard and supporting procedures and guidelines.**

## RIGHTS and PRIVILEGES

The computer systems, facilities, and accounts are owned by and operated by Alvin College. The College reserves all rights, including termination of service without notice, to the information systems which it owns and operates.

Access to the College's network system and the Internet is a privilege, not a right. Access and privileges on Alvin College information systems are assigned and managed by the administrators of the specific systems. A system administrator is the person or persons appointed by the College administration to monitor information systems in a selected area or areas. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system.

All access to the College information systems, including the issuance of passwords, must be approved by the data owner of the information system. Alvin College Information Technology Services provides custodial and administrative oversight at the direction of the information system's owner and the head of Information Technology.

As a State of Texas public community college, all communications utilizing the College's information resources are subject to public information requests, as applicable through the Public Information Act.

Upon approval of the College President, supervisors may be granted access to employee communications for review.

## MULTI-FACTOR AUTHENTICATION

"Multi-Factor Authentication (MFA)" is a method of computer access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

Alvin College employees are required to register a device or alternative contact to provide a secure method for systems to contact you during the login process for email, business-critical applications, and remote access. Depending on the MFA type and supported application, the device or alternative contact type may be a mobile device that can receive texts, an authentication app on a mobile device, a non-College email address, or a land-line telephone. The recommended and most secure method is an authentication app installed on a personal mobile device.

## CONFIDENTIALITY

No user is to disclose confidential information unless disclosure is a normal requirement of that user's position and has been so authorized. All users with access to confidential data are to safeguard the accuracy, integrity, and confidentiality of that data by taking precautions and following procedures necessary to ensure that no unauthorized disclosure of confidential data occurs. Such precautions and procedures include the secure storage of data backups and the protection of sensitive data with passwords.

## THIRD-PARTY CONTRACTOR ACCESS

Requests for third-party accounts and access must be submitted to the Alvin College IT Service Desk and approved by the appropriate information system owner(s) and head of Information Technology. Third-party / contractor accounts must be created for specifically named individuals with a specified expiration date. Third parties and contractors must agree to the Technology Use Standard and Agreement – Third Party and complete cybersecurity training before credentials may be delivered.

## ELEVATED ACCESS

Users with elevated permissions or administrative access should only use those accounts for official college business. Use of administrative access should be consistent with an individual's role or job responsibilities as assigned by the administrative tasks assigned to their job descriptions. Administrative access or elevated permissions must not be used to satisfy personal curiosity about an individual, system, practice, department, or other type of entity.

## USAGE

### Accounts and Files

All accounts, including email, are the property of Alvin College. As such, any information associated with these accounts is not private, and is subject to open records requests as outlined by the Public Information Act.

Access to College networks is restricted to Alvin College faculty, currently enrolled students, and staff. Community members and others who do not meet these requirements are allowed access to Internet-based resources from Alvin College's Library, or via a guest Wi-Fi network.

All authorized users are solely responsible for managing their files (including the files that constitute a web course) and their email.

Accounts are marked for deletion when employment is terminated or at the discretion of the Administration of the College and/or the discretion of the administrator of the network. The college is under no obligation to recover or protect user files from deleted accounts.

Users are to take precautions to prevent the unauthorized use of their passwords. In choosing passwords, users are to avoid the use of common words, proper names, readily associated nicknames or initials, and any other letter and/or number sequences that might be easily guessed. Passwords should contain a mix of uppercase, lowercase, numeric characters, and special characters. Users will be held accountable for all actions performed under their passwords, including those performed by individuals as a result of user negligence in protecting the password. If an account becomes compromised, users are to immediately change their password and contact the IT Service Desk.

Users are not to attempt to access, search, or copy technological and information resources without the proper authorization. No one is to use another individual's account, and active sessions are not to be left unattended. Users are not to test or attempt to compromise internal controls, even for purposes of systems improvement. Such actions require the advance and written approval of the authorized administrator or must be included among the security evaluation responsibilities of one's position. Violations must be reported to the head of Information Technology, the employee's supervisor, and the Office of Human Resources.

Users with access to student and personnel systems are not allowed to modify or add approvals to their own records. Users whose primary role is to modify such records must notify their supervisor should any such change be necessary to their record and are expected to follow standard college approval procedures.

Upon separation from the College, for business continuity purposes, all employee files and emails are transferred to the employee's immediate supervisor, or upon request, the supervisor's designee.

## EMAIL

Email is a critical mechanism for business communications at Alvin College. All employees are assigned an Alvin College email address to use throughout their employment. This Alvin College email address is the official means of electronic communication when representing the college in any capacity. Use of Alvin College's electronic mail system and services is a privilege, not a right; and therefore, must be used with respect and in accordance with the goals of Alvin College. Email sent, received, or stored on the College's systems is a state record and may be subject to the Texas Public Information Act (Texas Government Code Chapter 552) and to the records retention requirements.

### Email Account Activation / Termination

All Alvin College employees are assigned an email account. Employee email access will be terminated upon separation from the College. Email account naming conventions must differ in relation to the user's role with the College. Alvin College is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment or has ceased. Upon separation from the College, for business continuity purposes, all employee files and emails are transferred to the employee's immediate supervisor, or upon request, the supervisor's designee.

Email accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include auditors or contractors. Applications for these temporary accounts must be submitted to the IT Service Desk and approved by the appropriate information system

owner(s) and head of Information Technology. All terms, conditions, and restrictions governing email use must be in a written and signed agreement.

**General Expectations of End Users**

Important official communications are often delivered via email. As a result, employees of Alvin College with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important college announcements and updates, as well as fulfilling business- and role-oriented tasks.

Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove him or herself from the list, and is responsible for doing so in the event that their current email address changes.

Email users are also expected to comply with normal standards of professional and personal courtesy, and conduct.

**Email Content – Do NOT include PII**

Employees should NOT include any personally identifiable information (**PII**) in an email message body or in an unencrypted attachment. Information regarding the encryption of email is shared on the College Intranet portal.

Examples of **PII** include, *but are not limited to* the following:

Social Security Numbers
Bank Account Numbers
Health Status or information
Credit Card numbers
Driver's license number
Mother's Maiden Name
Birthdate
Employment date or retirement eligibility date
Race, ethnic, religion, or sexual orientation
Home address and telephone number

## THE INTERNET

Alvin College's Internet resources, including the World Wide Web, electronic mail, and networking protocols provide information beyond the confines of the campus. It allows access to ideas, information, and commentary from around the world. While the Internet offers a wealth of material that is personally, culturally, and professionally enriching to individuals of all ages, it also enables access to material that may be offensive or disturbing to others, inaccurate, or illegal under U.S. law. Alvin College cannot police the global network and takes no responsibility for its content. Rather, all users must assume responsibility and exercise sound judgement for their own activities on the Internet.

The use of the Internet must be consistent with the mission of Alvin College, the policies of the College, State, and Federal law. Access to the Internet over college computers is a privilege granted to users, and the College reserves the right to suspend and control this privilege if a user violates any acceptable use clause.

## COPYRIGHT CONCERNS

Copyright is a form of protection that the law provides to the authors of "original works of authorship" for their intellectual works that are "fixed in any tangible medium of expression", both published and unpublished (Title 17, United States Code). It is illegal to violate any of the rights provided by the law to the owner of the copyright. Alvin College respects the ownership of intellectual material governed by copyright laws. All users of Alvin College technology resources are to comply with the copyright laws and the provisions of the licensing agreements that apply to software; printed and electronic materials, including documentation, graphics, photographs, multimedia, including musical works, video productions, sound recordings, and dramatic works; and all other technological resources licensed and/or purchased by Alvin College or accessible over network resources provided by the College

In compliance with the requirements of the Digital Millennium Copyright Act of 1998 (DMCA), any user of Alvin College technology resources who violates the digital copyright laws for the first time will be reminded of the laws, and the software or licensing violation will be removed. A second violation will result in removing the software or licensing violations, retraining the user in copyright procedures, and taking appropriate disciplinary action. A third violation will require Alvin College to remove the user's network and Internet access and take further disciplinary action, which may include termination of employment.

## AI AND MACHINE LEARNING

Artificial Intelligence (AI) and Machine Learning (ML) are technologies that allow computer systems to perform tasks that normally require human judgment, such as analyzing data, generating text or images, and supporting decision-making. AI and ML can enhance work, research, and instruction, but employee use must be consistent with CRB-01, Acceptable Use of Artificial Intelligence, Employees, this procedure, and applicable law (see Legal and Regulatory References).

### AI Training

Employees who are required to complete annual cybersecurity training under this procedure must also complete an annual AI awareness training program certified by the Texas Cyber Command, as required by state law (see Legal and Regulatory References). This training is designed to build an understanding of how AI technology may be used in relation to an employee's job duties and to teach best practices for the safe, effective, and responsible use of AI systems. Information Technology Services will identify the College's designated AI training program and notify affected employees of the training assignment and deadline. An employee who has completed a Texas Cyber Command-certified AI awareness program at another Texas public entity within the current annual cycle may submit documentation of that completion in place of retaking the training, subject to verification by Information Technology Services. See CR-04, Cybersecurity and AI Training Programs, for the full training cycle and non-compliance process.

### Additional Guidance

For the College's full AI Code of Ethics, permitted and prohibited uses of AI, and the process for requesting human review of an AI-influenced decision, see CRB-01, Acceptable Use of Artificial Intelligence, Employees.

## SOCIAL MEDIA STANDARDS AND GUIDELINES

Social media has changed the way we communicate, offering a new model to engage with students, alumni, and the world at large. The Alvin College Marketing department has created and maintains a dynamic set of standards and guidelines that will be adjusted as new mediums, issues, and practices, in conjunction with the overall communication goals of the college, arise.

By participating in college-affiliated social media profiles and websites officially administered by Alvin College accounts, it is understood that user-generated content on college-affiliated social media accounts profiles or websites does not reflect the opinions or interests of Alvin College or its offices and must not be

inappropriate in nature. All participation and user-generated content appearing on Alvin College's college-affiliated social media profiles is subject to this agreement. *All college-affiliated Alvin College social media profiles must include a member of the Alvin College Marketing department as an administrator.*

All participants on Alvin College in college-affiliated social media profiles and website accounts must act appropriately and respectfully with the other participants in our online community. We ask that all participants in Alvin College's social media provides refrain from derogatory content which includes but is not limited to: Content which is illegal, blatantly profane, violent, sexual, pornographic, discriminatory, or otherwise defamatory. All content deemed inappropriate will be removed at the discretion of Alvin College Marketing administrators.

All content posted on college-affiliated accounts, pages and websites administered by Alvin College is subject to applicable copyright laws. Users may only post content of which they are the owner(s) or have written or licensed permission from the copyright owner to share the content (i.e., under an attribution Creative Commons license).

Alvin College accepts no responsibility or liability for any data, text, software, images, videos, messages, audio, or other content, which is generated by and posted publicly by users other than Alvin College in its official capacity. Alvin College accepts no liability or responsibility whatsoever for the content of any target third-party site linked from this page.

The entirety of Alvin College's Social Media Standards and Guidelines are available through the Marketing department, and must be reviewed and accepted prior to engaging in any social media activity which may be construed as being on behalf of the college.

Artificial intelligence tools may be used to assist with content generation, editing, proofreading and planning for Alvin College social media accounts. Any AI-assisted content must follow the standards and guidelines outlined above, comply with the entirety of this Acceptable Use Policy for AI and reflect the college's official voice.

## TELEPHONE AND VOICEMAIL ACCEPTABLE USE STANDARD

Telephone communication is an essential part of the day-to-day operations of Alvin College. Telephone and voicemail services are provided to employees of the College in order to facilitate performance of the College's work. Adjunct Faculty are not assigned a voicemail box.

As with all Alvin College resources, the use of telephones and voicemail should be as cost-effective as possible and in keeping with the best interests of the College. All employees must operate within the following basic standard guidelines:

- All telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of Alvin College.
- Information Technology Services is responsible for installation and repair of all college telephony equipment and administration of telephone and voicemail accounts.
- If a voicemail box is full, no further messages can be recorded.
- If you will be away from the office for more than one business day, you are expected to change your voicemail greeting to reflect this fact and direct callers to alternate contacts if applicable.
- Use of directory assistance (i.e., 411) should be avoided since a fee is incurred with each use.

## WI-FI ACCESS

Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment at Alvin College does not automatically guarantee the granting of wireless access privileges.

Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data.

Addition of new wireless access points within college facilities will be managed at the sole discretion of Information Technology Services in conjunction with key functional and instructional areas of the College. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organizational campus, are strictly forbidden and may result in the seizure of that equipment.

## VIDEO CONFERENCING AND CHAT SERVICES

Video call, video conferencing, and chat services are in use at Alvin College through a variety of software platforms. These services provide the ability to remotely engage with individuals and groups for a wide variety of purposes.

### General Expectations of End Users

Users are expected to comply with normal standards of professional and personal courtesy and conduct when utilizing video conferencing and chat services. Office or personal environments that may be captured with a webcam view should be professional and not distracting to viewers. If this is not possible, virtual backgrounds should be used.

## REMOTE ACCESS

Remote access is defined as any connection to Alvin College's network and/or other applications from off-site locations, such as the employee's home, a hotel room, conference, airports, cafes, satellite office, and wireless devices.

All remote access will be centrally managed by Alvin College Information Technology Services and will utilize encryption and strong authentication measures.

Based on positions within the college, certain employees are automatically granted remote access privileges. Any other employee requiring the use of remote access for business purposes must request access through their supervisor and clearly outline why the access is required and level of service needed. Requests must be approved by the employee's dean, director, or vice president before submission to Information Technology Services. Please contact the IT Service Desk for more information.

## BACKUPS

It is the responsibility of the information systems data owner to direct an appropriate backup and retention strategy. IT Services shall assign an appropriate administrator or network administrator to ensure that appropriate procedures and resources are in place to back up data as directed. Backups are to be stored in a location that is physically secure to protect the confidentiality of the data. It is the responsibility of the user to perform any actions necessary to comply with these procedures.

It is important to note that only networked drives are included in the normal backup processes. Data stored on users' desktops or local hard drives are not backed up and may not be recoverable in the event of a system failure. All college data must be stored in the employee's assigned storage or departmental networked drive.

## PROTECTING COLLEGE DATA

Alvin College Information Technology utilizes a number of networked devices and strategies to protect college data from cyber related attacks. However, it is every employee's responsibility to safeguard their network credentials and college data. Employees should be alert to various attempts and strategies that may inadvertently allow malicious attempts to gain access to data. Any suspicious email or computer activity should be immediately reported to the IT Service Desk.

### Cybersecurity Training

While IT Services maintains network and email firewalls, spam filters, anti-malware software, and other mechanisms to restrict access to College and student data, employees are the last line of defense against those that attempt to gain access to data for malicious purposes. To help employees recognize these attempts, and in accordance with Texas Administrative Code 202, Information Security Standards and the 2025 Texas House Bill 150, employees with access to College resources must complete annual cybersecurity training that is certified by the Texas Cyber Command. More information is available in CR-04, Cybersecurity and AI Training Programs.

### Viruses and Malware

Malware, traditionally known as a 'computer virus', is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Malware may be transmitted via email, instant messaging attachments, downloadable Internet files, and removable media, including mobile devices. Malware is usually disguised as something else, and so its presence is not always obvious to the computer user. A malware infection can be very costly to Alvin College in terms of lost data, lost staff productivity, financial loss, and loss of institutional reputation.

Alvin College has anti-malware software licensed per individual computer. If an employee detects any suspicious activity, email, notifications, or computer behavior, it must be reported immediately to the IT Service Desk. Report the following information if known: what caused the alert or suspicion, activity at the time of detection, source of detection, and potential recipients of infected material.

### Rules for Malware Prevention

- Run the standard anti-malware software provided by the College. Contact the IT Service Desk immediately for assistance.
- Never open any files from an unknown source.
- Be suspicious of email messages containing links to unknown websites.
- Never copy, download, or install files from unknown sources.
- Regularly update virus protection on personally owned home computers that are used for business purposes.

### Phishing, SMishing, and Vishing

Phishing email messages and websites are designed to steal money or obtain access to data. Phishing attempts most often mimic an official looking email or website and request the user's ID and password. Once a user fails to recognize the attempt and provide this information, cybercriminals can install malware on your computer or steal or encrypt and hold for ransom personal and college information off of your computer and networked drives Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. SMishing is a

similar attempt using texting/SMS applications. Vishing is an attempt to gain access to your information over the phone.

**Tips for Recognizing Phishing Attempts**

- Don't trust the display name of the sender of an email. Check the email address in the header form – if it looks suspicious, don't open the email.
- Look but don't click – hover your mouse over any links embedded in the body of the email. If the link address looks suspicious, don't click on it.
- Check for spelling mistakes – These are often a good sign that the email is not legitimate.
- Beware of urgent or threatening language in the subject line – Invoking a sense of urgency is a common phishing tactic. Beware of phrases such as "account will be suspended", or "mailbox is at the limit".
- Never give out personal information – legitimate companies will never ask for personal credentials via email.
- Don't believe everything you see - Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it's legitimate. Be skeptical when it comes to your email messages—if it looks even remotely suspicious, don't open it.

**Laptops, Tablets, and Mobile Devices**

If issued a college laptop, or using a mobile device to conduct college business, employees must take adequate care to protect and secure it. Be aware of your surroundings and any suspicious persons. The device should never be left in an unsecured area in an automobile, hotel, or conference event. If circumstances require storing in a vehicle, the device must be kept in the trunk or completely out of sight. Employees who are assigned college-owned devices are solely responsible for their care. College data should never be stored on a mobile device; remote access should be utilized to securely access college networked data. Employees who are issued a laptop or other mobile device must accept a Mobile Technology Assignment Agreement.

## PHYSICAL SECURITY

All users are responsible for the physical security of their technological and information resources. Administrators are to help ensure physical security by instituting procedures for the use of locked doors and/or for the use of security devices made available by Alvin College for the protection of the equipment. To avoid loss by fire or theft, backups of important data are not to be stored in the same location as the originals. Adequate power regulators and surge suppressors are to be used.

## GENERAL PROVISIONS

The following actions (including but not limited to) will result in disciplinary action including but not limited to the suspension of computer privileges:

- Damage or destruction of equipment, software, or data belonging to the College or to other users, including adding, altering, or deleting files on College workstations and/or servers.
- Altering of system settings or Internet browser settings on College computers without express permission of an instructor or an authorized member of Information Technology Services.
- Reproduction of materials protected by copyright without permission of the copyright owner.
- Violating software license agreements.
- Violating or attempting to violate computer system or network integrity, including attempts to bypass network security functions, or to obtain restricted passwords for system administration.
- Using College technological resources to harass or intentionally offend others.

- Utilizing the Internet and/or College equipment for unauthorized material/commercial gain or profit.
- Using the Internet or any College technological resource for any activity prohibited by Federal, State or International Law.
- Attempting to utilize computing resources to which you do not have access or approval.
- Sharing your personal password with others or using another person's password.
- Neglecting to protect and safeguard network IDs and passwords, including phishing attempts and other cybercriminal methods.
- Impersonating another user via any form of electronic messaging.
- The production of and/or intentional dissemination of self-replicating or similar nuisance program (e.g., virus, Trojan horse), whether or not they are destructive in nature.

## MAINTENANCE

The responsibility for maintaining the campus computing environment rests with Information Technology Services. To ensure the smooth functioning of computer equipment, all employees must observe the following:

- Only authorized software may be installed on any College computer. Information Technology Services is responsible for determining what software may or may not be installed, based on technical specifications and licensing.
- Only authorized personnel may repair College computer equipment.
- Maintenance requests for labs should be submitted in a timely fashion, i.e., at least two weeks in advance. A list of all required software and proof of licensing may be requested by IT Services before any work is performed.

## LEGAL AND REGULATORY REFERENCES

This procedure is governed by, at minimum:

- Texas Administrative Code 202 (TAC 202), Information Security Standards;
- Texas Government Code Chapter 2063 (Texas Cyber Command), as amended by House Bill 150 (89th Legislature), which requires annual cybersecurity training;
- Texas Government Code §2054.5191 (House Bill 3512, 89th Legislature), which requires designated employees to complete annual, Texas Cyber Command-certified AI awareness training;
- Texas Government Code Chapter 2054, Subchapter S (Senate Bill 1964), which requires an AI Code of Ethics and minimum risk-management standards for AI systems;
- 1 Texas Administrative Code Chapter 219, which implements Senate Bill 1964, including the AI Code of Ethics (§219.11) and the risk assessment and impact assessment required before deploying a "heightened scrutiny" AI system used as a controlling factor in a consequential decision, such as admissions, grading, discipline, or an employment action (§§219.20–219.24);
- Texas Government Code §2054.5192, which requires designated contractors to complete annual cybersecurity training;
- The Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), and the Payment Card Industry Data Security Standard (PCI DSS), which govern how College systems and AI may handle student, financial, and payment card data;
- The Texas Public Information Act, Texas Government Code Chapter 552; and
- The Digital Millennium Copyright Act of 1998 (DMCA) and Title 17, United States Code, which govern copyright.

## VIOLATIONS

An employee's computer use privileges may be suspended immediately upon the discovery of a possible violation of this procedure. Suspected violations will be confidentially reported to the appropriate system administrator, the employee's supervisor, and the Office of Human Resources.

Violations of this Standard will be dealt with in the same manner as violations of other College policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including the loss of computer use privileges, termination from the College, and legal action. Violations of some of the above standards may constitute a criminal offense.