TEXAS A&M **INTERNATIONAL** UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.03.L0.01 Information Resource Acceptable Use

First Approved:	**October 8, 2020**
Revised:	**December 18, 2025**
	February 20, 2026
Next Scheduled Review:	**February 20, 2031**

Procedure Statement and Reason for Procedure

Texas A&M University System (**system) policies and regulations require** Texas A&M International University (TAMIU) to establish **rules and procedures consistent with system policy and regulation requirements. This procedure establishes** standards and responsibilities for **using** the **University's** information resources.

Procedures and Responsibilities

1. General

1.1 The rules and procedures specified are based on Federal, State, and TAMU System requirements. A complete list of all related requirements is in the resources area, Related Statutes, Policies, Regulations, or Rules, near the end of this document.

2. Responsibilities

2.1 The Chief Executive Officer (CEO) of each state institution of higher education is ultimately responsible for securing its information resources. The CEO of each institution or their designated representatives shall ensure that senior University officials and information owners, in collaboration with the Information Resource Manager (IRM), i.e., the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or Information Security Officer (ISO), support the provision of information security for the information systems used to support all operations and assets under their direct or indirect, e.g., cloud computing or outsourced control.

2.2 The CISO or ISO has the responsibility to:

2.2.1 develop and maintain information security policies and procedures that address the requirements set forth by Texas Administrative Code Chapter 202, Subchapter C, and the institution's information security risks.

2.2.2 develop and recommend policies and establish procedures and practices, in cooperation with the institution's CIO, information owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure.

2.3 "Information Owner Responsibilities" are defined in section 10.

2.4 "Information Custodian Responsibilities" are defined in section 11.

2.5 User Responsibilities" are defined in section 12 and apply to all who use institution resources.

3. User Sanctions

3.1 A user of information resources owned by the institution who fails to comply with Texas A&M System Regulation 29.01.03, Information Security, TAMIU and information security requirements outlined in this document are subject to disciplinary action, up to and including termination of employment, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, and suspension or expulsion for students. Additionally, individuals are subject to loss of information resource access privileges and civil and criminal prosecution.

4. Information Security Awareness

4.1 Users who utilize computer equipment for over 25 percent of their workday must have annual security awareness training (Texas Government Code § 2054.5191).

4.1.1 University employees must complete TrainTraq course number 3001, Information Security Awareness, as required by Texas A&M System Regulation 33.05.02, Reguired Employee Training and Texas A&M System Cybersecurity - Security Control Standards Catalog AT-2.

4.1.2 Any contractor with access to organizational information must complete a certified information security awareness training during the contract term and any renewal period per Texas Government Code § 2054.5192. Access is "any person given an account to access any state (or local) information system."

4.1.2.1 A list of certified training sources can be found on the Texas Department of Information Resources (TDIR) website.

4.1.2.2 The TDIR provides an annual YouTube video course for contractors with university access to complete and acknowledge its completion, which can be found on their website. The acknowledgment should be sent to the CISO, ISO, or CIO.

4.2 Users are required to read and understand this document.

4.3 Employees are responsible for keeping up with rules and procedural changes regarding information resources.

4.4 Employees agree to comply electronically with the Data Use Agreement during the security awareness training.

5. Required Reporting

5.1 Users must report any information security incident to the Information Technology Help Desk, CISO, ISO, or CIO using itsecurity@tamiu.edu. If a user receives a suspicious email, they shall send the original message as an attachment to preserve the email's metadata.

5.2 Report lost, stolen, or found equipment such as computers, laptops, USBs, cell phones, and storage devices.

5.3 Users will report any security violations, signs of wrongdoing, significant security issues discovered, and signs of unauthorized activity.

5.4 Users agree to report any security compromise that could lead to divulging confidential information online. Some examples are social security numbers, grades, date of birth (DOB), student IDs, etc.

5.5 Users shall report an insider threat if anyone with authorized access to information resources either wittingly or unwittingly attempts to inflict harm to the resources of the University.

5.6 Users observing or suspecting criminal activity shall contact the University Police Department (UPD) or other appropriate law enforcement agency. All further access to data on information resources must follow directives from law enforcement agencies. If law enforcement is notified, employees must also inform the CISO, ISO, or CIO using itsecurity@tamiu.edu.

6. Privacy

6.1 There is no expectation of privacy when using TAMIU-owned information resources, e.g., devices, email, instant messaging, etc., beyond that which is expressly provided by applicable privacy laws.

6.2 Users should not store private information, e.g., personal passwords, pictures, emails, etc., on institutional devices. Information can become the institution's property, be collected for legal use, or be subject to the Texas Public Information Act (TPIA) Chapter 552).

6.2.1 Information created, stored, or transmitted on information resources may be subject to disclosure under TPIA or through legal or administrative proceedings.

6.3 To manage the efficient operation of information systems, appropriate security practices, and issues relating to inappropriate or illegal use, the institution may log, review, and otherwise use any information stored on or passing through its information resources. All such actions shall follow the provisions and safeguards provided in the Texas Administrative Code § 202, Information Resource Security Standards, and other applicable rules and laws.

6.4 The institution collects and processes many types of information from third parties. Much of this information is confidential and shall be protected following all applicable laws and regulations, e.g., General Data Protection Regulation (GDPR), Gramm-Leach-Bliley Act (GLBA), and Texas Administrative Code § 206.

6.5 Users shall not attempt to access any data or information resources for which they do not have appropriate access, authorization, or explicit consent from the owner.

6.6 The ability to read a file does not imply authorization to read or alter it. Under no circumstances may a user change a file that does not belong to them unless the owner gives explicit consent.

6.7 Departmental heads own departmental data unless specifically delegated.

6.8 Information owners or custodians will provide access to information (requested by auditors) on the performance of their jobs. Notification to file owners will be sent as directed by the auditors.

6.9 Users with special access to information because of their position are responsible for not abusing that access. Suppose information is inadvertently gained, e.g., seeing a copy of a test or homework, which could provide personal benefit. In that case, the individual is responsible for notifying both the owner of the data and the organizational unit head.

6.10 Websites available to the general public shall contain a Privacy Policy and follow EIR accessibility requirements specified in Texas Administrative Code § 213.

7. Privacy of Regulated Data

7.1 Regulated data is information that federal, state, and system laws and regulations protect. Some examples of protected data include FERPA, GLBA, HIPAA, PCI, PHI, PII, CJIS, CUI, and more.

7.2 Computers and devices that access regulated data will be located on an isolated network segment. All traffic into and out of the network is logged. Access to specific internet sites may be restricted or forbidden.

7.3 Computers and devices that access regulated data are primarily for storing that information. Using the computer for personal business may be a violation.

7.4 No HIPAA-protected data may be saved outside the Electronic Medical Records (EMR) system, including the hard drives in the local system or externally attached storage.

7.5 All computers must begin with a known, clean image, free of malicious hardware/software, before any software with access to the EMR system is loaded. In the event of a data breach, hard drives in the affected machines will be removed and replaced with a new hard drive with a known, clean image.

7.6 End users will not be granted administrative access to any computer that can access regulated data and may not install, uninstall, or otherwise alter the computer's software unless the request is made through and approved by the CISO, ISO, or CIO.

7.7 System administrators must obtain approval from the CISO or ISO before installing any newly acquired software to prevent increasing the risk of an information breach.

7.8 Under HIPAA privacy rules, all medical information and any other individually identifiable health information in any form, whether electronic, hard copy, or oral, is considered protected health information (PHI). This includes information about an individual's past, present, or future physical or mental health or condition. Individually identifiable health information includes, but is not limited to:

7.8.1 names
7.8.2 addresses (including subdivisions smaller than a state such as street, city, county, and zip code)
7.8.3 dates (except years) directly related to an individual, such as DOB, admission/discharge dates, death dates, and exact ages of individuals older than 89
7.8.4 telephone numbers
7.8.5 fax numbers
7.8.6 email addresses
7.8.7 Social Security numbers
7.8.8 EMR and medical record numbers
7.8.9 health plan beneficiary numbers
7.8.10 account numbers
7.8.11 certificate and license numbers
7.8.12 vehicle identifiers
7.8.13 device identifiers and serial numbers
7.8.14 website URLs
7.8.15 IP addresses
7.8.16 biometric identifiers, including fingerprints, voice prints, iris and retina scans
7.8.17 full-face photos and other photos that could allow a patient to be identified
7.8.18 any other unique identifying numbers, characteristics, or codes

7.9 A person is subject to punishment under the law when they knowingly and in violation of the HIPAA Privacy Rule (42 USC 1320d-6)

7.9.1 use, or cause to be used, a unique health identifier

7.9.2 obtain individually identifiable health information relating to an individual or

7.9.3 disclose individually identifiable health information to another person.

7.10 All employees shall follow the FERPA requirements found at

7.10.1 https://www.tamiu.edu/registrar/ferpa.shtml

7.10.2 https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

7.10.3 https://studentprivacy.ed.gov/node/548/

8. Data Use

8.1 To use any data, the information owner must approve the use of the data under their responsibility.

8.2 The Vice President of Enrollment Management owns prospective student, recruit, and applicant data.

8.3 The Registrar is the owner of student data.

8.4 The Provost and VP for Academic Affairs (VPAA), and Human Resources own faculty data.

8.5 The Comptroller is the owner of financial data.

8.6 The Chief Human Resources Officer owns intern, employee, and student employee data.

8.7 Together, they will be responsible for maintaining the accuracy of their data and approving access requests to the data under their authority.

9. Information Owner Responsibilities

9.1 The information owner or their designated representatives are responsible for the following:

9.1.1 classify information under their authority, with the concurrence of the Chief Financial Officer (CFO) or their designated representatives, following the University's established information classification categories.
9.1.2 approve access to information resources and periodically review access lists based on documented risk management decisions.
9.1.3 formally assign custody of information or an information resource.
9.1.4 coordinate data security control requirements with the CISO or ISO.
9.1.5 convey data security control requirements to custodians.
9.1.6 provide authority to custodians to implement security controls and procedures.
9.1.7 document, justify, and account for exceptions to security controls—the information owner shall coordinate and obtain approval for exceptions to security controls with the CISO or ISO.
9.1.8 participate in risk assessments as provided under Texas Administrative Code § 202.75.

10. Information Custodian Responsibilities

10.1 Custodians of information resources, including third-party entities providing outsourced information resources and services to the University, shall:

10.1.1 implement controls to protect information and information resources that align with the Texas Department of Information Resources (TDIR) Security Control Standards Catalog and the system's Control Standards Catalog based on the classification and risks specified by the information owner or as specified by the policies, procedures, and standards defined by the University's information security program.

10.1.1.1 The system's required control standards listing is here: https://cyber-standards.tamus.edu/catalog/required-controls

10.1.2 provide owners with information to evaluate the cost-effectiveness of controls and monitoring.

10.1.3 adhere to monitoring techniques and procedures approved by the CISO or ISO for detecting, reporting, and investigating incidents.

10.1.4 provide information necessary to provide appropriate information security training to employees.

10.1.5 ensure information is recoverable following risk management decisions.

11. User Responsibilities

11.1 The user of an information resource has the following responsibilities:

11.1.1 use the resource only for the purpose specified by the institution or information owner.

11.1.2 comply with information security controls and institution policies and procedures to prevent unauthorized or accidental disclosure, modification, or destruction.

11.1.3 formally acknowledge that they will comply with the security policies and procedures in a method determined by the CEO or their designated representative.

11.2 Institution-owned information resources, designated for use by the public, shall be configured to enforce security policies and procedures without requiring user participation or intervention. Users must accept a banner or notice before using an information resource the institution provides.

12. Data Use Agreement

12.1 shall distribute a data use agreement and each update to that agreement to employees who handle sensitive information, including financial, medical, personnel, or student data. Each employee shall sign the distributed data use agreement and each update to the agreement (Texas Government Code § 2054.135).

12.2 Employees agree to electronically comply with the Data Use Agreement during security awareness training.

13. System Use

13.1 Resources may not be used for personal purposes except for incidental use defined by this document. The arbitrary use of institution resources for personal purposes must not (Texas A&M System Policy 33.04, Use of System Resources):

13.1.1 result in additional expense to the institution.

13.1.2 impede normal business functions.

13.1.3 be used for non-approved private commercial purposes.

13.1.4 be used for illegal activity.

13.1.5 be used to intentionally access, create, store, or transmit obscene materials.

13.1.6 be used to compete unfairly with private sector entities or private consultants.

13.1.7 result in embarrassment to the institution.

13.2 Incidental personal use of system computers (including, but not limited to, the internet and email), telephones, facsimile (fax) machines, and other means of communication must meet the requirements above. They must not unduly impede an employee's assigned responsibilities or the normal functioning of an office. The use of system telecommunication, email, and internet services for any illegal activity or to intentionally access, create, store, or transmit obscene materials, as defined in Texas Penal Code § 43.21 (other than in the course of academic research), is strictly prohibited, regardless of whether or not it results in an additional charge to the institution.

13.3 No employee shall entrust institution property or resources to any institution official or employee, or anyone else, to be used for any reason other than institution purposes (Texas Government Code § 2203.004). Employees shall not use equipment, property, or resources for their benefit unless it benefits the institution, has been approved in advance by the CIO or designees, and suitable arrangements have been made to pay the agreed-upon value for using such property or resources.

13.4 Electronic files are subject to the same records retention rules that apply to other documents and must be retained following records retention schedules.

13.5 Users must not attempt to access any data or programs on systems for which they do not have authorization or explicit consent.

13.6 Family members or other non-employees cannot access institution information systems.

13.7 Software or hardware purchased with institution funds may not be installed on non-institution systems or networks without prior authorization from the CIO.

13.8 Software or hardware purchased with personal funds may not be installed on institution-owned computers or networks without prior authorization from the CIO.

13.9 Desktops, laptops, and other information resources must remain on to allow patching and updating activities.

13.10 An information resource must be used only for the purpose specified by the institution, information, or resource owner.

13.11 The Logon Banner will read:

> Attention! This system is for official authorized use only. All content on this system is owned by Texas A&M International University and/or the State of Texas. Unauthorized use is prohibited, and misuse is subject to criminal prosecution. Usage may be subject to security testing and monitoring. Users have no expectation of privacy except as otherwise provided by privacy laws.

13.12 Use of the hardware, equipment, and manufacturers listed in the Statewide Plan of Preventing the Use of Prohibited Technology in State Agencies are prohibited.

14. Credential Use

14.1 Do not reuse any institution's password with any internet or external system.

14.2 Passwords must not be posted on or under a computer, monitor, or peripheral, e.g., keyboard, mouse etc., nor may they be left in any accessible location.

14.3 Passwords will expire.

14.4 Computing devices shall be secured by enabling a password-protected screensaver or automatic logoff.

14.5 Passwords must be treated as confidential information. Passwords shall not be revealed to anyone.

14.6 Passwords must never be transmitted in plaintext unless the account is used only for accessing publicly accessible data.

14.7 If the security of a password is in doubt, the password should be changed immediately.

14.8 If a password has been compromised, the incident should be reported to the CISO or ISO at itsecurity@tamiu.edu.

14.9 Users should not circumvent password entry with automatic logon, application remembering, embedded scripts, or hard-coded passwords in client software for systems that process/store controlled and confidential data. Exceptions may be made for specific applications, e.g., automated backups, with the approval of the information resource owner.

14.10 Hardware tokens must not be shared or loaned to others. If a hardware token is shared, lost, or stolen, it must be reported for deactivation immediately.

14.11 Security access codes, access cards, and keys to information system facilities must not be shared or loaned to others. If a revocable resource, such as a card or access code, is shared, it must be deactivated upon notification.

15. Network Use

15.1 Users are not to connect to or install any equipment, including computers, printers, and network management/control devices, to the network infrastructure without prior approval from Information Technology.

15.2 Users must not plug unknown devices into any institution's computer or network.

15.3 Information Technology is responsible for the University’s network infrastructure configuration.

15.4 Network management/control devices shall not be connected to network infrastructure without prior consultation with Information Technology. Network management/control devices include, but are not limited to, routers, gateways, switches, hubs, wireless access, devices, or software advertising or serving network services (including BOOTP, DHCP, DNS, IPv6 router, VPN, SMTP, ICS, OSPF or other routing protocols), devices or software transmitting multicast or broadcast traffic at high rates, etc.

15.5 Users are not permitted to install or run devices or software designed or intended to conduct network reconnaissance, vulnerability probing, reveal or exploit weaknesses, or conduct denial of service (DoS) or distributed denial of service (DDoS) attacks.

15.6 Users must not run password-cracking programs, packet sniffers, port scanners, or other unapproved hardware devices or software on information resources.

15.7 VPN implementers that backhaul data from a location to a central site, thus masking its actual location, are not allowable on the organization’s network. Contact Information Technology for allowable VPN use at itsecurity@tamiu.edu.

15.8 Users can use only those network addresses issued by Information Technology.

15.9 All connected devices are subject to monitoring and management.

15.10 Guest access is provided for conferences and similar meetings. The organizer should contact the Information Technology Help Desk for details as part of planning the event.

15.11 Users shall not alter or turn off institution network infrastructure devices or equipment.

15.12 All computers connecting to the network must run authorized malware protection software updated with current signatures and security patches.

15.13 Malware protection software must not be turned off or bypassed except as required for the temporary installation of software or other exceptional circumstances.

15.14 Computers infected with a virus or other malicious code will be disconnected from the network until deemed safe by Information Technology.

15.15 If a device causes any disruption, malware, vulnerability, or exploit to run on information resources or the network, the device will be disconnected until the problem is resolved.

15.16 Users must not purposely engage in activity that may harass, threaten, or abuse others, degrade the performance of information resources, deprive authorized users access to an institution resource, obtain extra resources beyond those allocated, or circumvent institution computer security measures.

15.17 Software or hardware purchased with institutional funds may not be installed on non-institution systems or networks without prior authorization from Information Technology.

16. Media Use

16.1 All removable media that contains confidential data shall be destroyed appropriately. Users must notify the help desk for the secure disposal of media and protect it until disposal occurs.

17. Software Use

17.1 Software must be used following license and contract agreements and applicable copyright laws. Such agreements should be maintained in the department that operates the system on which the software is installed. In cases where this is not feasible, individuals or departments should maintain documentation, e.g., End User License Agreements (EULA), purchase receipts, terms of service (ToS), etc., to validate that software or hardware is appropriately licensed.

17.2 The institution shall provide enough licensed copies of software so employees can fulfill their responsibilities expediently and effectively. Each department may make appropriate arrangements with the software vendors for additional licensed copies, if needed, for business activities, subject to the CIO's delegation of authority for contract administration.

17.3 It should be noted that some software licenses allow the user to make a copy for home use in conjunction with the business use of the software. A licensed software user should not assume this provision is in place but, instead, check with the license agreement before making copies for other machines.

17.4 Software not licensed to the institution shall not be installed on institution-owned systems, networks, or computers unless Information Technology approves; such unlicensed software will be removed unless the user can provide a license or authorization.

17.5 Licensed software may only be copied and used to the extent permitted under the license. Unauthorized copies or illegally distributed copyrighted software are prohibited.

17.6 Users, including cloud-based products, must not use non-standard software without the CIO's approval. Before purchasing or using, the CISO, ISO, or CIO must evaluate all software and services.

17.7 Users cannot install personal commercial, shareware, or freeware software until proof of ownership is supplied and the software is evaluated.

17.7.1 Software may require a license transfer by Information Technology.

17.7.2 Software must be assessed by Information Security (IS).

17.7.3 Software must be evaluated for Electronic Information Resources (EIR) accessibility.

17.8 If the software is deemed a security risk or duplicates the functionality of existing, approved software or hardware, the software will not be installed.

17.9 Software purchased with institutional funds may not be installed on non-institution systems or networks without prior authorization from Information Technology.

17.10 Peer-to-peer (P2P) software allowing content distribution in which digital files are transferred between "peer" computers is prohibited.

17.11 Systems may be scanned for unauthorized software.

17.12 Unapproved or unauthorized software will be removed unless proof of authorization from the rightful owners is provided, and it may require a license (or system) transfer.

17.13 Use of the software, applications, and developers listed in the Statewide Plan of Preventing the Use of Prohibited Technology in State Agencies is expressly prohibited.

18. Email Use

18.1 Email is considered an official means of communication.

18.2 Users required to conduct official business via email must do so with their assigned TAMIU email account. Email systems for the institution's business require appropriate security, backup, and records retention measures.

18.3 Requests to substitute non-institution email addresses for official communication will not be honored. Using non-approved email exposes that email to the Office of General Counsel's (OGC) legal collection and open records request per Texas Government Code § 552.004

18.4 Email is subject to the same policies regarding information disclosure as other methods of communication. The privacy of personally identifiable information (PII) must be protected under the laws and regulations provided by the Family Educational Rights and Privacy Act of 1974 (FERPA), Gramm-Leach-Bliley Act (GLBA), and the State of Texas. The confidentiality of email cannot be assured, and any confidentiality may be compromised by access consistent with applicable law or policy, including this procedure, by unintended redistribution, or due to current technologies inadequate to protect against unauthorized access.

18.5 Sensitive and confidential material must not be transmitted via email unless encrypted. Users must exercise extreme caution in using email to communicate confidential or sensitive matters and shall not assume that their email is private. Examples of confidential and controlled data can be found in the system's Cybersecurity Standards (Data Categorization).

18.6 Email must be used in a manner that achieves its purpose without exposing any technical, financial, or legal risks.

18.7 The following activities are prohibited:

18.7.1 Using personal email accounts for business purposes. Official emails shall not be forwarded from business email accounts to personal accounts.

18.7.2 Sending an intimidating or harassing email.

18.7.3 Using email for conducting non-approved private commercial purposes.

18.7.4 Using email for purposes of political lobbying or campaigning.

18.7.5 Violating copyright laws by inappropriately distributing protected works.

18.7.6 Posing as anyone other than oneself when sending an email, except when authorized to send messages to another individual while serving in an administrative support role.

18.7.7 Using unauthorized email software.

18.7.8 Sending or forwarding chain letters.

18.7.9 Sending unsolicited messages to large groups except as required to conduct University business.

18.7.10 Sending huge messages.

18.7.11 Sending or forwarding an email that is likely to contain computer viruses.

18.8 Users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any department unless appropriately authorized. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the University. An example of a simple disclaimer is: "The opinions expressed are my own and not necessarily those of my employer."

18.9 Storage of personal email, voice messages, files, and documents within institution-owned information resources must be nominal.

18.10 All users of institution networks and systems should not subscribe to mailing lists or mail services strictly for personal use and should not participate in electronic discussion groups, i.e., list servers, Usenet, IRC, news groups, chat rooms, for personal purposes.

18.11 Email messages will be retained on the mailbox server for a maximum of 180 days. Email messages in all folders, including the “Inbox,” “Sent Items,” and user-created folders will be automatically removed.

18.12 Messages in the “Deleted Items” folder will be permanently deleted after 180 days.

18.13 Calendar events will be automatically removed after 180 days.

18.14 Any email that constitutes an institution record must be retained according to the retention policy. Email messages must be filed in an appropriate system for retention. Individuals are responsible for making this designation by filing the information appropriately

19. Instant Messaging/Texting

19.1 The content and function of an instant message (IM) or short message service (SMS) message, i.e., text message, determines whether it is an institution record. Only IMs meeting institution records criteria are subject to records retention requirements. An IM is not an institution record unless the message uniquely documents system business and is NOT merely a convenience copy or transitory information. Any IM that is an institution record must be retained in an appropriate electronic records management system (not the IM account), following system records retention requirements.

19.2 TAMIU-provided IM services should be limited to sharing short-term messages requiring immediate action or confirmation of presence. Information of an enduring nature (in this case, needed after 48 hours) should be utilized in email messaging services or other storage provided by the system.

19.3 Use of non-approved IM applications exposes the information resource used to the Office of General Counsel’s legal collection and open records request per Texas Government Code § 552.004

20. Video Conferencing

20.1 Meeting solutions blend communications, collaboration, and content sharing to enable informal and formal meetings. These solutions may be part of a larger unified communications package or a standalone web conferencing product.

20.1.1 Limit meeting solutions for conducting business to those approved and centrally administered solutions.

20.1.2 Meeting access codes are only reused in recurring meetings when the meeting is protected by additional screening controls, e.g., waiting room, authenticated users.

20.1.3 Meeting hosts use a roll call or other means of identifying each meeting attendee when beginning the meeting and as additional attendees join.

20.1.4 Meeting hosts do not record the meeting unless necessary and only after informing each attendee that remaining in the meeting constitutes consent to the recording.

20.1.5 Meeting hosts or co-hosts monitor attendees to ensure unidentified participants do not enter the meeting.

20.1.6 Meeting hosts retrieve and delete recordings of meetings containing sensitive information from the meeting provider's platform immediately once the recording is made available.

20.1.7 Meeting hosts utilize user authentication or a lobby, pre-conference, or waiting room to identify attendees before admitting them to a meeting and lock the meeting room once all scheduled attendees have joined the meeting to prevent uninvited attendees from joining the meeting.

20.1.8 Meeting access codes, e.g., meeting or room ID, are protected with a passcode, password, or PIN.

20.1.9 Attendees are not permitted to enter the meeting room before the host begins the meeting.

20.1.10 The ability to share screen content is restricted to the meeting host or attendees explicitly permitted by the meeting host.

20.1.11 A lobby, pre-conference, or waiting room is enabled by default for all meetings.

20.1.12 When supported, hardened default meeting settings are locked by the account administrator and cannot be changed by meeting hosts.

21. Internet Use

21.1 All internet activity is logged and may be reviewed for inappropriate use.

21.2 Only officials expressly authorized to speak to the media or public on behalf of the University may represent the University via any electronic communication.

21.3 Supervisors should work with employees to determine the appropriateness of internet use for professional activities and career development. Written permission is needed and should be obtained for these activities, or the activities should be included in the employee's job description. All users of institution networks and information resources using the internet shall identify themselves honestly, accurately, and ultimately (including one's affiliation and function where requested) when providing such information.

21.4 Personal Internet use should not impede business conduct; only incidental use is allowed per Texas A&M System Policy 33.04, Use of System Resources. Users are responsible for exercising good judgment regarding the reasonableness of personal use, following all guidelines for the acceptable use of information resources.

21.5 The Information Security Office monitors for breaches of websites. If any user account has been compromised, a password reset of the user's local account will be issued. Users shall register a different password for every site/login.

21.6 Accessing, viewing, downloading, uploading, transmitting, printing, copying, posting, or sharing any racist, sexist, threatening, sexually explicit, obscene, or otherwise objectionable material, i.e., visual, textual, or auditory entity, is strictly prohibited.

21.7 Institutional Internet access must not be used for personal gain or solicitation.

21.8 Software shall scan all downloaded files to safeguard against malicious threats.

21.9 Sensitive or confidential information must not be posted publicly.

21.10 All confidential and controlled information transmitted over external networks, e.g., the Internet or shared externally, must be encrypted.

21.10.1 All sensitive or confidential data must only be shared using the document management system, network share, or secured Intranet site.

21.10.2 Third-Party Sharing – Contact the OIT Help Desk, AVPIT/CIO, or ISO for supplemental guidance at itsecurity@tamiu.edu.

21.11 Peer-to-peer software allowing illegal content distribution in which digital files are transferred between "peer" computers is not permitted.

21.12 All files downloaded from the internet must be scanned for malware using the approved malware/virus detection software.

21.13 Personal internet use should not incur a direct cost in addition to the general overhead of an internet connection; consequently, users are not permitted to print or store personal electronic files or material on the network.

22. Artificial Intelligence

22.1 You may not enter sensitive, restricted, or otherwise protected data into any generative AI tool or service. This information includes, but is not limited to:

22.1.1 FERPA-protected or regulated information, such as:
22.1.1.1 TAMIU IDs or photos
22.1.1.2 TAMIU directory data
22.1.1.3 TAMIU non-directory data such as student ID numbers
22.1.1.4 Student names and grades
22.1.1.5 Disability-related information

22.1.2 Health information protected by HIPAA

22.1.3 Information related to employees and their performance

22.1.4 Intellectual property not publicly available

22.1.5 Material under confidential review, including research papers and funding proposals

22.1.6 Information subject to export control

22.2 You may not direct AI tools or services to generate or enable content that facilitates sexual harassment, stalking, or sexual exploitation or that enables harassment, threats, defamation, hostile environments, stalking, or illegal discrimination, including, but not limited to:

22.2.1 Sexual harassment, stalking, dating violence, and domestic violence.

22.2.2 Depicting a person's voice or likeness without their consent or other appropriate rights, including unauthorized impersonation and non-consensual sexual imagery.

22.2.3 Harming or abuse of a minor, including grooming and child sexual exploitation.

22.2.4 Harassing, harming, or encouraging the harm of individuals or specific groups, including discrimination or harassment based on a protected class.

22.2.5 Discrimination based on disability or defects.

22.3 Protecting sensitive information and complying with applicable state and federal privacy and security laws and regulations and with university policies is imperative.

22.4 Access to protected institutional data must be authorized and managed to protect individual privacy, maintain promised confidentiality, and ensure appropriate access and use.

22.5 You may not upload any data that could be used to help create or carry out malware, spam, phishing, or other scams. IT resources may not be used to disseminate unauthorized email messages.

22.6 You may not use AI tools or services to generate content that helps others break federal, state, or local laws, institutional policies, rules, guidelines, licensing agreements, or contracts. IT resources may not be used to violate laws, policies, or contracts.

22.7 You may not use AI tools or services to infringe copyright or other intellectual property rights.

22.8 You must not use AI tools to produce academic work not expressly permitted in the course curriculum or syllabus. Getting caught passing off AI output as your work could result in penalties, including academic probation and expulsion.

22.8.1 Any individual or member who learns of a potential breach, data leakage, or confidentiality loss—including through generative AI—must report the incident to the CIO, CISO, or ISO at itsecurity@tamiu.edu.

23. TAMIU-Owned Portable Computing

23.1 Confidential or controlled data stored on portable computing devices shall be encrypted. Information Technology will maintain a list of suitable encryption mechanisms.

23.2 Users must use an approved VPN connection when remotely connecting to the institution's network.

23.3 Confidential or controlled data shall not be transmitted via a wireless connection to or from a portable computing device unless appropriately secure wireless encryption methods are utilized, e.g., Transport Layer Security (TLS) or Remote Desktop Protocol (RDP) over VPN.

23.4 Remotely accessing, e.g., dial-in services, cable/DSL modem, etc., confidential information from a portable computing device shall utilize approved encryption techniques, such as Secure File Transfer Protocol (SFTP), TLS, or VPN.

23.5 Unattended portable computing or storage devices containing confidential information shall be kept physically secure using means commensurate with the associated risk.

23.6 Export control regulation may apply when traveling outside the U.S. Contact the export control officer (ECO) for further information. Additional resources regarding export control at TAMIU are provided at the link below.

23.6.1 https://www.tamiu.edu/orsp/ExportControls.shtml

24. Bring Your Own Device (BYOD)

24.1 Employees, contractors, and network users must not send, forward, store, or receive confidential information on unencrypted or unsecured mobile devices, e.g., cell phones or tablets. Only encrypted devices authorized by the Information Technology Department, CISO, or ISO may receive and store confidential information.

24.2 It is not advisable to use a personal device for business use. Doing so could expose the personal device to litigation procedures (copying of data) or Public Records Requests. TAMIU is not liable for any damage incurred through an individual's use of personal devices for business purposes. The user retains all risk; however, the institution will not be at risk.

24.3 Multi-factor authentication (MFA) verification is not considered business use; therefore, using MFA for identity confirmation on a personal device is acceptable.

24.4 BYOD equipment and personal computers are only allowed on the wireless "guest" network, and appropriate authentication is required.

24.5 The University reserves the right to require any device accessing the institution's infrastructure to be subject to existing and future security policies and standards established by the Information Security Office. Security policies may include but are not limited to, device requirements for mobile anti-malware/anti-virus, mobile device firewall, secure communications, encrypted file folders including storage cards, strong passwords, MFA, and destruction and disabling in the event of a lost or stolen device or termination. Costs for any mobile security measures will become the financial responsibility of the device owner.

24.6 A current or former officer or employee of a governmental body who maintains public information on a privately owned device shall (Texas Government Code § 552.004):

24.6.1 forward or transfer the public information to the governmental body or its server for preservation.

24.6.2 preserve the public information in its original form in a backup or archive and on a privately owned device.

25. Computer Labs

25.1 Users shall log out after each session.

25.2 Copying or distributing unauthorized content is prohibited.

25.3 Software in the labs is subject to copyright licensing agreements. Copying or removing software from the labs is considered theft and is a violation of U.S. copyright laws.

25.4 Abuse of computing resources is considered a severe offense that may result in disciplinary action by the organization and loss of computing privileges. Responsible use of computing resources includes:

25.4.1 Using hardware and software properly.

25.4.2 Respect other users' privacy; do not try to access any files belonging to another user.

25.4.3 Respecting other users who want to be in a quiet environment free of interruptions, i.e., no cell phone use in the labs.

25.4.4 Backing up your data and protecting your information.

25.5 Devices and systems must not be moved or disconnected.

25.6 Devices, systems, software, and other lab materials shall not be removed.

25.7 Devices and systems may not connect or authenticate outside of the lab.

25.8 Personal devices used to connect to the lab or the organization domain are prohibited.

25.9 Unauthorized use of the following is prohibited: installing or running devices or software designed or intended to conduct network reconnaissance, vulnerability probing, revealing or exploiting weaknesses, or conducting denial of service (DoS) or distributed denial of service (DDoS) attacks.

26. Cybersecurity Lab

26.1 The rules in the Computer Lab section above shall be followed in addition to the following procedures.

26.1.1 Backing up personal data shall not prevent University backups from running, nor shall any University data be taken outside the computer or cybersecurity lab area, including backups, copies, packet captures, analytic, network- and locally captured data.

26.2 Users must conduct activities as standard users and elevate privileges only when needed.

26.3 Devices and systems may only be moved when instructed by faculty or staff.

26.4 Lab devices, servers, laptops, or workstations must not be added to the organization's domain.

26.5 No device or system shall be reimaged without appropriate authorization.

26.6 Users shall not conduct penetration testing, vulnerability scans, or other reconnaissance activities outside the cybersecurity lab.

27. Third Party Use

27.1 All network infrastructure connections to third-party networks require consultation with Information Technology before the purchase/installation of any software, hardware, or associated service.

27.2 Information owners must approve data sharing, e.g., FERPA, Directory Data, PII, HIPAA, PHI, PCI, with a third party.

27.3 The institution collects and processes many types of information from third parties. Much of this information is confidential and shall be protected following all applicable laws and regulations, e.g., GLBA, Texas Administrative Code § 202.

27.4 Third parties must adhere to EIR Accessibility standards outlined in Texas Administrative Code § 213 and TAMUS Policy 29.01.04.

27.5 When the department is the owner or custodian of the system hosting software or hardware, the department is responsible for ensuring End-User License Agreements (EULAs) are appropriately stored and maintained.

27.6 System owners must review access and remove user accounts of individuals who no longer require access or do not use the system.

27.7 System owners and custodians are required to perform, at a minimum, annual account reviews for access.

28. Web Publishing

28.1 All websites must meet the requirements of Texas Administrative Code § 206 and the Security Control Standards Catalog (AC-22).

28.2 The University's primary website is considered a public site, and all materials are shared. Information on the public website does not require any permission to access.

28.3 No confidential information may be posted on the public website. Hidden links are not an acceptable method of preventing information from being accessible, i.e., security through obscurity. Search engines will automatically discover and catalog, i.e., crawl, all content on the primary website unless controlled by a robots.txt file.

28.4 TAMIU must publish a privacy notice that meets the minimum requirements of the system's AC-8 control standard.

28.5 Domain names should be purchased through, or with the coordination of, Information Technology.

28.6 Before deploying an internet website or mobile application that processes confidential information, a vulnerability and penetration test must be reviewed and approved by the CISO or ISO (Texas Government Code § 2054.516).

28.7 Websites must adhere to EIR Accessibility standards (TAMUS Policy 29.01.04).

29. Clean Desk Requirements

29.1 Employees must ensure that all confidential information in hard copy or electronic form is secured in their work area at the end of the day and when they are expected to be gone for an extended period.

29.2 Computer workstations must be locked when not in use or unattended.

29.3 Computer workstations should be logged off at the end of the workday.

29.4 Any confidential information must be removed from the desk and secured in a drawer or locked office when not in use or unattended.

29.5 File cabinets containing confidential information must be closed and locked when not in use or unattended.

29.6 Keys used to access confidential information must be secured at all times.

29.7 Passwords shall not be left on sticky notes anywhere, nor may passwords be in an accessible location.

29.8 Upon disposal, confidential documents must be shredded in the official shredder bins or placed in the locked, confidential document disposal bins.

29.9 Whiteboards containing confidential information should be erased immediately after use.

29.10 Treat mass storage devices such as CD-ROMs, DVDs, BDs, or USB flash drives as confidential, and secure the media in a locked drawer or cabinet.

29.11 Printers and fax machines must be cleared of papers as soon as they are printed. This helps to ensure confidential documents are not left in printer trays for unauthorized persons to pick up or view.

30. Payment Card Acceptance

30.1 The Comptroller, Director of Purchasing, and Vice President for Finance and Administration, in coordination with the Information Security Officer, must approve any acceptance of payment methods by credit or debit card following university financial guidelines.

Related Statutes, Policies, Regulations, or Rules

31. Federal

31.1 U.S. Department of Education FISMA, NIST SP 800-171 R2

31.2 U.S. Department of Education FERPA

31.3 Gramm-Leach-Bliley Act (15 U.S. Code § 6801)

31.4 Health Insurance Portability and Accountability Act (HIPAA)

31.5 Payment Card Industry (PCI) Data Security Standard (DSS)

32. State of Texas

32.1 Texas Government Code, Chapter 552. Public Information

32.2 Texas Government Code, Chapter 2054. Information Resources

32.3 Texas Administrative Code Chapter 202, Subchapter C, Information Security Standards for Institutions of Higher Education

32.4 Texas Administrative Code Chapter 206, Subchapter C, Institution of Higher Education Websites

32.5 Texas Administrative Code Chapter 213, Subchapter C, Accessibility Standards for Institutions of Higher Education

32.6 Texas Administrative Code Chapter 216, Subchapter C, Project Management Practices for Institutions of Higher Education

32.7 DIR Acceptable Use of the Internet Policy

32.8 DIR Security Control Standards Catalog

32.9 DIR Prohibited Technologies

33. Texas A&M System

33.1 System Policy 29.01 Information Resources

33.2 System Regulation 29.01.01 Information Resources Governance

33.3 System Regulation 29.01.02 Use of Licensed Software Link to System

33.4 System Regulation 29.01.03 Information Security

33.5 System Regulation 29.01.04 Accessibility of Electronic and Information Resources

33.6 System Regulation 33.04 Use of System Resources

33.7 Texas A&M University System Cybersecurity Control Standards

33.8 Texas A&M Information Security Controls Catalog

33.9 System Regulation 29.01.05 Artificial Intelligence

Contact Office

Office of Information Technology, 956-326-2310