TEXAS A&M INTERNATIONAL UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.03.L0.01 Information Resource Acceptable Use

First Approved: October 8, 2020
Revised: October 8, 2020
Next Scheduled Review: October 8, 2025

Procedure Statement and Reason for Procedure

In accordance with The Texas A&M University System (System) Regulation 29.01.03, *Information Security*, Texas A&M International University (TAMIU) is required to establish an information security program to protect TAMIU information and information resources. The purpose of this SAP is to establish standards and responsibilities for the acceptable use of information resources.

Procedures and Responsibilities

1. General

The procedures specified in this SAP are based on Federal, State, and System requirements. A complete list of all related requirements are located under "Related Statutes, Policies, Regulations, or Rules" at the end of this SAP.

2. Responsibilities

2.1 The Chief Executive Officer (CEO) is ultimately responsible for the security of information resources. The CEO or their designated representative(s) shall ensure that senior TAMIU officials and information owners, in collaboration with the Information Resources Manager (IRM), i.e., the Associate Vice President for IT/CIO (AVPIT/CIO), and 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. [Texas Administrative Code §202.70(c)(3)]

2.2 The ISO has the responsibility to:

2.2.1 develop and maintain information security policies and procedures which address the requirements set forth by Texas Administrative Code §202, Sub-Chapter C and TAMIU's information security risks.

2.2.2 develop and recommend policies and establish procedures and practices, in cooperation with TAMIU's AVPIT/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 of this SAP.

2.4 "Information Custodian Responsibilities" are defined in Section 11 of this SAP.

2.5 "User Responsibilities" are defined in Section 12 of this SAP and apply to all individuals using TAMIU resources.

3. User Sanctions

Users of information resources owned by TAMIU who fail to comply with System Regulation 29.01.03, *Information Security* and System and TAMIU information security requirements outlined in this SAP 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/or suspension or expulsion for students. Additionally, individuals are subject to loss of information resource access privileges as well as civil and criminal prosecution.

4. Information Security Awareness

4.1 Users who utilize computer equipment more than 25% of their workday are required to annually complete information security awareness training. [Texas Government Code §2054.5191]

4.1.1 Any contractor with access to organizational information must complete information security awareness training during the term of the contract and any renewal period. [Texas Government Code §2054.5192]

4.2 Users are required to read and understand this document.

4.3 Employees are responsible for keeping up-to-date on rules and procedural changes regarding information resources.

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

5. Required Reporting

5.1 Users must report any information security incident to the Office of Information Technology (OIT) Help Desk, information security, or the ISO by email using itsecurity@tamiu.edu. If a user receives a suspicious email, they shall send the original email as an attachment (versus forwarding it) to preserve the email's metadata.

5.2 Users must report lost, stolen, or found equipment such as computers, laptops, USBs, and any mobile or storage device.

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 compromise of security that could lead to divulging confidential information, including but not limited to posting social security numbers, grades, dates of birth (DOB), etc., to the Internet.

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 TAMIU resources.

5.6 If criminal activity is suspected, the University Police Department (UPD) or other appropriate law enforcement agency must be notified. All further access to data on information resources must be in accordance with directives from law enforcement agencies. If law enforcement is notified, employees must also notify the ISO or AVPIT/CIO using itsecurity@tamiu.edu.

6. Privacy

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

6.2 Users should not store private information (e.g., personal passwords, pictures, and emails, etc.) on TAMIU devices. Information can become the property of TAMIU, be collected for legal use, or be subject to the Texas Public Information Act (TPIA). [Texas Government Code §552]

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

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

6.5 TAMIU collects and processes many different types of information from third-parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations (e.g., General Data Protection Regulation (GDPR), the Gramm-Leach-Bliley Act (GLBA), Texas Administrative Code §206).

6.6 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.

6.7 The ability to read a file does not imply authorization to read or alter it. Under no circumstances may a user alter a file that does not belong to them, unless given explicit consent by the file's owner.

6.8 Department heads own departmental data unless specifically delegated.

6.9 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.

6.10 Users who have special access to information because of their position have the absolute responsibility for not abusing that access. If information is inadvertently gained, e.g., seeing a copy of a test or homework, which could provide personal benefit, the individual has the responsibility to notify both the owner of the data and the organizational unit head.

6.11 Websites available to the general public shall contain a Privacy Policy and follow Electronic Information Resources (EIR) accessibility requirements as specified in Texas Administrative Code §213.

7. Privacy of HIPAA and PHI Data

7.1 Computers and devices that access (Health Insurance Portability and Accountability Act) or HIPAA-protected data or personal health information (PHI) will be located on an isolated network segment. All traffic into and out of the network is logged. Access to certain Internet sites may be restricted or forbidden.

7.2 Computers and devices that access HIPAA-protected data or PHI are primarily for HIPAA-protected data or PHI. The use of a TAMIU computer for personal business may be a violation.

7.3 No HIPAA-protected data or PHI may be saved outside of the Electronic Medical Records (EMR) system, including the hard drive(s) in the local system or externally-attached storage.

7.4 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.

7.5 End users will not be granted administrative access to any computer that can access HIPAA-protected data or PHI and may not install, uninstall, or otherwise alter the computer's software unless the request is made through and approved by OIT.

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

7.7 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 PHI. This includes any information related to the past, present, or future physical or mental health or condition of an individual. Individually-identifiable health information includes, but is not limited to:

7.7.1 names
7.7.2 addresses (including subdivisions smaller than state such as street, city, county, and zip code)
7.7.3 dates (except years) directly related to an individual, such as DOB, admission/discharge dates, death dates, and exact ages of individuals older than 89
7.7.4 telephone numbers
7.7.5 fax numbers
7.7.6 email addresses
7.7.7 Social Security numbers
7.7.8 medical record numbers
7.7.9 health plan beneficiary numbers
7.7.10 account numbers
7.7.11 certificate and license numbers
7.7.12 vehicle identifiers
7.7.13 device identifiers and serial numbers
7.7.14 website URLs
7.7.15 IP addresses
7.7.16 biometric identifiers, including fingerprints, voice prints, and iris/retina scans
7.7.17 full-face and other photos that could allow a patient to be identified
7.7.18 any other unique identifying numbers, characteristics, or codes

7.8 A person is subject to punishment under the law when they knowingly and in violation of the HIPAA Privacy Rule:

7.8.1 use, or cause the use of, a unique health identifier;
7.8.2 obtain individually-identifiable health information relating to an individual; or
7.8.3 disclose individually-identifiable health information to another person.

8. Privacy of FERPA Data

8.1 All employees shall follow the Family Educational Rights and Privacy Act of 1974 (FERPA) requirements found at:

8.1.1 https://www.tamiu.edu/registrar/ferpa.shtml
8.1.2 https://www.tamiu.edu/registrar/ferpa_faculty.shtml
8.1.3 https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
8.1.4 https://studentprivacy.ed.gov/node/548/

9. Data Use

9.1 To use any data, the information owner must approve the use of the data under their responsibility. Together, all are responsible for maintaining the accuracy of their data and approving access requests to the data under their authority.

9.1.1 The Director of Recruitment and School Relations is the owner of prospective students, recruits, and applicant data.
9.1.2 The University Registrar is the owner of student data.
9.1.3 The Provost and VP for Academic Affairs (VPAA) is the owner of faculty data.
9.1.4 The Comptroller is the owner of financial data.
9.1.5 The Director of Human Resources is the owner of employee and student employee data.

10. Information Owner Responsibilities

10.1 The information owner or their designated representative(s) are responsible for:

10.1.1 classifying information under their authority, with the concurrence of the Chief Financial Officer (CFO) or their designated representative(s), in accordance with TAMIU's established information classification categories;
10.1.2 approving access to information resources and periodically reviewing access lists based on documented risk management decisions;
10.1.3 formally assigning custody of information or an information resource;
10.1.4 coordinating data security control requirements with the ISO;
10.1.5 conveying data security control requirements to custodians;
10.1.6 providing authority to custodians to implement security controls and procedures;
10.1.7 documenting, justifying, and accounting for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the ISO; and
10.1.8 participating in risk assessments as provided under Texas Administrative Code §202.75.

11. Information Custodian Responsibilities

11.1 Custodians of information resources, including third-party entities providing outsourced information resources and/or services to TAMIU, shall:

11.1.1 implement controls required to protect information and information resources required by Texas Department of Information Resources (DIR) Security 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 TAMIU's information security program;

11.1.2 provide owners with information to evaluate the cost-effectiveness of controls and monitoring;

11.1.3 adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents;

11.1.4 provide information necessary to provide appropriate information security training to employees; and

11.1.5 ensure information is recoverable in accordance with risk management decisions.

12. User Responsibilities

12.1 The user of an information resource has the responsibility to:

12.1.1 use the resource only for the purpose specified by TAMIU or information owner;

12.1.2 comply with information security controls and TAMIU rules and procedures to prevent unauthorized or accidental disclosure, modification, or destruction; and

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

12.2 TAMIU-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 are required to accept a banner or notice prior to using an information resource provided by TAMIU.

13. Data Use Agreement

13.1 TAMIU shall distribute a Data Use Agreement, and each update to the 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]

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

14. System Use

14.1 Resources may not be used for personal purposes except for incidental use, in accordance with this SAP and System Regulation 33.04, *Use of System Resources*. The incidental use of TAMIU resources for personal purposes must not:

14.1.1 result in additional expense to TAMIU;
14.1.2 impede normal business functions;
14.1.3 be used for non-approved private commercial purposes;
14.1.4 be used for illegal activity;
14.1.5 be used to intentionally access, create, store, or transmit obscene materials;
14.1.6 be used to compete unfairly with private sector entities or private consultants; or
14.1.7 result in embarrassment to TAMIU.

14.2 Incidental personal use of system computers, including but not limited to the Internet, email, telephones, facsimile (fax) machines, and other means of communication, must meet the requirements above and 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 TAMIU.

14.3 No employee shall entrust TAMIU property or resources to any TAMIU official or employee, or to anyone else, to be used for any reason other than TAMIU purposes. [Texas Government Code §2203.004] Employees shall not use equipment, property, or resources for their benefit unless it benefits the TAMIU, has been approved in advance by the CFO or designee(s), and suitable arrangements have been made in advance for payment of the agreed-upon value for the use of such property or resources.

14.4 Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with the records retention schedules.

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

14.6 Family members or other non-employees are not allowed to access TAMIU information systems.

14.7 Software or hardware purchased with TAMIU funds may not be installed on non-TAMIU systems or networks without prior authorization from OIT.

14.8 Software or hardware purchased with personal funds may not be installed on TAMIU-owned computers or networks without prior authorization from OIT.

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

14.10 An information resource must be used only for the purpose specified by TAMIU or information or resource owner.

14.11 Logon Banner – "Texas A&M International University. Use of this system constitutes acknowledgement of the following: Unauthorized use is strictly prohibited; All usage is subject to security monitoring and testing; Misuse is subject to criminal prosecution; [There is] (n)o expectation of privacy."

15. Credential Use

15.1 Passwords must not be inscribed on sticky notes posted on or under a computer, monitor, or peripheral (i.e., keyboard, mouse, etc.), nor may they be left written down in any accessible location.

15.2 Passwords will expire.

15.3 Computing devices should not be left unattended without enabling a password-protected screensaver or automatic logoff.

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

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

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

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

15.8 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 mission-critical and/or confidential data. Exceptions may be made for specific applications (e.g., automated backups) with the approval of the information resource owner.

15.9 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 as soon as possible.

15.10 Security access codes, access cards, and/or 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.

16. Network Use

16.1 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 OIT.

16.2 Users must not plug any unknown device(s) into any TAMIU computer or network.

16.3 OIT is responsible for TAMIU's network infrastructure configuration.

16.4 Network management/control devices shall not be connected to network infrastructure without prior consultation with OIT. 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 broadcasting traffic at high rates; etc.

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

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

16.7 VPN implementers which backhaul data from a location to a central site, thus masking its true location, are not allowed on TAMIU's network. For allowable VPN use, contact OIT at itsecurity@tamiu.edu.

16.8 Users are permitted to use only those network addresses issued to them by OIT.

16.9 All connected devices are subject to monitoring and management.

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

16.11 Users shall not alter or disable TAMIU network infrastructure devices or equipment.

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

16.13 Malware protection software must not be disabled or bypassed except as required for the temporary installation of software or other special circumstances.

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

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

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

16.17 Software or hardware purchased with TAMIU funds may not be installed on non-TAMIU systems or networks without prior authorization from OIT.

17. Media Use

17.1 All removable media that contains confidential data shall be properly destroyed. The user must contact the OIT Help Desk for secure disposal of media.

17.2 The user must protect the media until it can be disposed.

18. Software Use

18.1 Software must be used in accordance with license agreements, contract agreements, and applicable copyright laws. Where feasible, 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 enough documentation (e.g., End User License Agreements (EULA), purchase receipts, terms of service (ToS), etc.) to validate software or hardware is appropriately licensed.

18.2 TAMIU shall provide enough licensed copies of software so employees can fulfill their responsibilities in an expedient and effective manner. Each department must receive approval from OIT before purchasing software or services.

18.2.1 The information owner of each information system is responsible for appropriately licensing the software.

18.3 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 user of licensed software should not assume this provision is in place but instead check with the license agreement before making copies for other machines.

18.4 Software not licensed to TAMIU shall not be installed on TAMIU-owned systems, networks, or computers unless approved by OIT. OIT will remove such unlicensed software unless the user can provide a license or authorization.

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

18.6 Users must not use non-standard software without OIT management approval.

18.7 Privately acquired commercial, shareware, or freeware software will not be installed until proof of ownership is supplied and an evaluation of the software is performed.

18.7.1 Software may require a license transfer by OIT.
18.7.2 All software must be assessed by OIT Information Security (IS).
18.7.3 All software must be evaluated for EIR accessibility.

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

18.9 Software purchased with TAMIU funds may not be installed on non-TAMIU systems or networks without prior authorization from OIT.

18.10 Peer-to-peer (P2P) software that allows content distribution in which digital files are transferred between "peer" computers is not permitted.

18.11 Systems may be scanned for unauthorized software.

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

19. Email Use

19.1 Email is considered an official means of communication.

19.2 Users required to conduct official business via email are required to do so with their assigned TAMIU email account. Email systems used to conduct the business of TAMIU require appropriate security, backup, and records retention measures.

19.3 Requests to substitute non-TAMIU email addresses for purposes of official communication will not be honored. Use of non-approved email exposes that email to Office of General Counsel's (OGC) legal collection and open records request. [Texas Government Code §552.004]

19.4 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 FERPA, the 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 SAP, by unintended redistribution or due to current technologies inadequate to protect against unauthorized access.

19.5 Sensitive and/or 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 or confidential. Examples of confidential and controlled data can be found in the Data Classification Standard.

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

19.7 The following activities are prohibited:

19.7.1 Using personal email accounts for business purposes. Official emails shall not be forwarded from business email accounts to personal accounts.
19.7.2 Sending an intimidating or harassing email.
19.7.3 Using email for conducting non-approved, private commercial purposes.
19.7.4 Using email for purposes of political lobbying or campaigning.
19.7.5 Violating copyright laws by inappropriately distributing protected works.
19.7.6 Posing as anyone other than oneself when sending an email, except when authorized to send messages on behalf of another individual while serving in an administrative support role.
19.7.7 Using unauthorized email software.
19.7.8 Sending or forwarding chain letters.
19.7.9 Sending unsolicited messages to large groups, except as required to conduct TAMIU business.
19.7.10 Sending excessively large messages.
19.7.11 Sending or forwarding an email that is likely to contain computer viruses with intent to do harm.

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

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

19.10 Users of TAMIU 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 server, Usenet, IRC, news groups, chat rooms) for personal purposes.

19.11 Email messages will be retained on the mailbox server for a maximum of 365 days. Email messages in all folders, including the inbox, sent items, and user-created folders will be automatically removed.

19.12 Messages in the “Inbox” and “Sent” folder will be removed after 30 days.

19.13 Messages in the “Deleted Items” folder will be permanently deleted after 2 days.

19.14 Calendar events will be retained on the calendar server for a maximum of 30 days. Calendar events on all calendars will be automatically removed.

19.15 Any email that constitutes a state or TAMIU record must be retained according to the retention policy. This requires email messages to be filed in an appropriate system that will allow for retention. Individuals are responsible for making this designation by filing the information appropriately.

20. Instant and Text Messaging

20.1 All use of instant messages (IM) at TAMIU is to be for non-TAMIU records or temporary communication only. All TAMIU record communication shall be recorded through other means. IMs will be retained for 24 hours or less.

20.2 Use of short message service (SMS) (i.e., text messages) at TAMIU for business is not permitted. All TAMIU record communication shall be recorded through other means.

21. Video Conferencing

21.1 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 stand-alone web conferencing product.

21.2 The use of meeting solutions for conducting business must be limited to those solutions that are approved and centrally administered.

21.3 Meeting access codes shall only be reused, such as in cases of recurring meetings, when the meeting is protected by additional screening controls (e.g., waiting room, authenticated users).

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

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

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

21.7 Meeting hosts must retrieve and delete recordings of each meeting containing sensitive information from the meeting provider's platform immediately after the recording is made available.

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

21.9 Meeting access codes (e.g., meeting or room ID) shall be protected with a passcode, password, or PIN.

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

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

21.12 Lobbies/pre-conference/waiting rooms are enabled by default for all meetings.

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

22. Internet Use

22.1 All Internet activity is logged and may be reviewed for inappropriate use.

22.2 Only officials who are expressly authorized to speak to the media or to the public on behalf of TAMIU may represent TAMIU via any electronic communication.

22.3 Supervisors should work with employees to determine the appropriateness of using the Internet 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 TAMIU networks and information resources using the Internet shall identify themselves honestly, accurately, and completely (including one's affiliation and function where requested) when providing such information.

22.4 Personal Internet use should not impede the conduct of business. Only incidental use is allowed as the Information Resources Access Standard and System Policy 33.04, *Use of System Resources*. Users are responsible for exercising good judgment regarding the reasonableness of personal use, in accordance with all guidelines associated with acceptable use of information resources.

22.5 The ISO monitors for breaches of websites. If the ISO identifies that any user account has been compromised, a password reset of the user's local account will be issued. It is recommended that all users register a different password for every site/login.

22.6 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.

22.7 TAMIU Internet access must not be used for personal gain or solicitation.

22.8 All downloaded files shall be scanned by software to safeguard against malicious threats.

22.9 Sensitive or confidential information must not be posted publicly.

22.10 All sensitive or confidential information transmitted over external networks (e.g., Internet) or shared externally must be encrypted.

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

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

22.11 Do not reuse any TAMIU password with any Internet or external system.

22.12 Peer to peer (P2P) software allowing illegal content distribution in which digital files are transferred between "peer" computers is not permitted.

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

22.14 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.

23. TAMIU-Owned Portable Computing

23.1 All sensitive or confidential data stored on portable computing devices shall be encrypted. OIT will maintain a list of suitable encryption mechanisms.

23.2 Users must use the approved Virtual Private Network (VPN) connection when remotely connecting to the TAMIU 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 (i.e., Transport Layer Security (TLS) or Remote Desktop Protocol (RDP) over VPN) are utilized.

23.4 All remote access (e.g., dial in services, cable/DSL modem, etc.) to confidential information from a portable computing device shall utilize approved encryption techniques, such as Virtual Private Network (VPN), Secure File Transfer Protocol (SFTP), or Transport Layer Security (TLS).

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. TAMIU provides additional export control resources at 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, such as two-way pagers, personal digital assistants (PDAs), cell phones, or tablets. Only devices authorized by OIT or the ISO may receive and store confidential information that must be encrypted.

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 a public records request. TAMIU is not liable for any damage incurred through an individual's use of a personal device(s) for business purposes. All risk is retained by the user, and TAMIU will not be put at risk.

24.3 Two-factor authentication (2FA) verification is not considered business use. Therefore, it is acceptable to use 2FA for identity confirmation on a personal device.

24.4 BYOD equipment and personal computers are only allowed on the wireless (guest) networks, and appropriate authentication is required.

24.5 TAMIU reserves the right to require any device accessing TAMIU's infrastructure be subject to existing and/or future security policies and standards established by the ISO. 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, two-factor authentication, and/or 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 a governmental body server to be preserved; or

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

25. Third-Party Use

25.1 All connections of the network infrastructure to third-party networks requires consultation with OIT prior to the purchase/installation of any software, hardware, or associated service.

25.2 Information owners must approve the use of data sharing (e.g., FERPA, Directory Data, PII, HIPAA-PHI, PCI) with a third-party.

25.3 TAMIU collects and processes many different types of information from third-parties. Much of this information is confidential and shall be protected in accordance with all applicable laws and regulations (e.g., the Gramm-Leach-Bliley Act, Texas Administrative Code §202).

25.4 Third-parties must adhere to EIR accessibility standards outlined in Texas Administrative Code §213 and System Policy 29.01.04, *Accessibility of Electronic and Information Resources*.

25.5 In instances where 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.

25.6 System owners are required to review access and disable and/or remove any user accounts of individuals who are terminated or transferred and who no longer need access or who no longer use the system.

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

26. Web Publishing

26.1 All websites must meet the requirements of Texas Administrative Code §206.

26.2 TAMIU's primary website is considered a public website, and all materials are considered public. Information on the public website does not require any permission to access.

26.3 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). All content on the primary website will be discovered and catalogued by search engines automatically.

26.4 TAMIU must publish a privacy notice that describes applicable provisions of its privacy policy on its homepage and all key public entry points or its site policies page. [Texas Administrative Code §206.72]

26.5 Domain names should be purchased through or with the coordination of OIT.

26.6 Before deploying an Internet website or mobile application that processes confidential information, a vulnerability and penetration test must be reviewed and approved by the ISO. [Texas Government Code §2054.516]

26.7 Websites must adhere to EIR accessibility standards outlined in System Policy 29.01.04, *Accessibility of Electronic and Information Resources*. The EIR officer may be contacted for additional information at accessibility@tamiu.edu.

27. Clean Desk Requirements

27.1 Employees are required to 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.

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

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

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

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

27.6 Keys used for access to confidential information must not be left at an unattended desk.

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

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

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

27.10 Mass storage devices (such as CD-ROM, DVD, BD, or USB drives) shall be treated as confidential, and the media shall be secured in a locked drawer.

27.11 All 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.

28. Payment Card Acceptance

The Comptroller, in coordination with the ISO, must approve any acceptance of payment methods by credit or debit card, in accordance with TAMIU financial guidelines.

Related Statutes, Policies, Regulations, or Rules

Federal
U.S. Department of Education, FISMA, NIST SP 800-171 R1
U.S. Department of Education, Family Educational Rights and Privacy Act (FERPA)
Gramm-Leach-Bliley Act (15 U.S. Code §6801)
Health Insurance Portability and Accountability Act (HIPAA)
Payment Card Industry (PCI) Data Security Standard (DSS)

State of Texas
Texas Government Code, Chapter 552. Public Information
Texas Government Code, Chapter 2054. Information Resources
TAC, §202, Sub-Chapter C, Information Security Standards for Institutions of Higher Education
TAC, §206, Sub-Chapter C, Institution of Higher Education Websites
TAC, §213, Sub-Chapter C, Accessibility Standards for Institutions of Higher Education
TAC, §216, Sub-Chapter C, Project Management Practices for Institutions of Higher Education
Texas Department of Information Resources, Acceptable Use of the Internet
Texas Department of Information Resources, Security Control Standards Catalog

The Texas A&M University System (System)
System Policy 29.01, *Information Resources*
System Regulation 29.01.01, *Information Resources Governance*
System Regulation 29.01.02, *Use of Licensed Software*
System Regulation 29.01.03, *Information Security*
System Regulation 29.01.04, *Accessibility of Electronic and Information Resources*
System Policy 33.04, *Use of System Resources*
The Texas A&M University System - Information Security Standards
The Texas A&M University System - Configuration Management Standard
The Texas A&M University System - Data Classification Standard
The Texas A&M University System - Identity Management Standard
The Texas A&M University System - Contingency Planning Standard
The Texas A&M University System - Electronic Media Protection Standard
The Texas A&M University System - Incident Management Standard
The Texas A&M University System - Information Resource Access Standard
The Texas A&M University System - Physical and Environmental Protection Standard
The Texas A&M University System - System Development and Acquisition Standard
The Texas A&M University System - Information System Monitoring Standard
The Texas A&M University System - Information Integrity Standard
The Texas A&M University System - Standards: Preservation Holds (January 3, 2006)

Contact Office

Office of Information Technology, 956-326-2310