Information Technology Services

THE TEXAS A&M UNIVERSITY SYSTEM

Software/Hardware/Network Statement of Responsibility for Third Parties

Rev. 07/2022

I understand that I will be violating A&M System Policy, A&M System Offices (SO) rules, and state and federal law if I gain, or help others gain, unauthorized access to the SO computer network. I acknowledge that neither I nor anyone else possesses the authority to allow anyone to use my ID or password.

I also understand that if I violate state and federal laws by gaining, or helping others gain, unauthorized access to the SO network, I will be subject to criminal prosecution to the full extent of the law (Chapter 33, Section 1, Title 7 of the Texas Penal Code).

By logging on to any of the SO network computers, I acknowledge my responsibility for strictly adhering to The Texas A&M University System Policy concerning network access, the SO Information Resource Acceptable Use Standards (attached) and state and federal law. I am also aware that penalties exist for unauthorized access, unauthorized use or unauthorized distribution of information from SO computers.

I agree further not to attempt to circumvent the computer security system by using or attempting to use any transactions, software or resources I am not authorized to use.

I acknowledge that I have received and read The Texas A&M University System Offices Information Resources Acceptable Use Standards. I understand that I must comply with these Standards, including any changes to those policies, standards, and guidelines, when accessing and using SO Information Resources. My failure to comply with this Agreement may result in loss of access privileges to SO Information Resources or other disciplinary action up to and including termination for employees; termination or alteration of employment relations in the case of temporaries, contractors, or consultants; or dismissal for interns and volunteers. Furthermore, individuals could be subject to additional civil liability, and/or criminal charges.

I agree to complete The Texas A&M University System Offices Security Awareness Training promptly upon activation of my System Offices account.

Account User's Name (First Middle Last) _____ *Nickname (optional)* _____

Title or Position _____ A&M System Member or Contracting Company _____

Phone Number _____ Account Expiration Date (Not to Exceed 6 Months) _____

Email Address _____

UIN (if provisioned) _____ System Office Host Department _____

NetID (if provisioned) _____ System Office Department Head _____

User Signature _____ Date _____ Department Head Signature _____ Date _____

Scan and email ONLY THIS PAGE to helpdesk@tamus.edu and then give all 5 pages to the user.

301 Tarrow Street, Suite 371 • College Station, Texas 77840-7896
(979) 458-6450 • Fax (979) 458-6299 • www.tamus.edu

The A&M System Offices (SO) relies on networked computers and the data contained within those systems to achieve its mission. These Acceptable Use Standards are to protect these resources in accordance with A&M System Policy, SO rules, and federal and state law. These Standards do not supersede any state or federal laws or any other SO policies regarding confidentiality, information dissemination, or standards of conduct.

CONFIDENTIAL AND SENSITIVE INFORMATION

As an employee or sponsored user of The Texas A&M University System Offices, you may have access to confidential or sensitive information through use of SO Information Resources or through your associated activities with SO information systems. Confidential and sensitive information includes identifying information, federal tax information, personal health information, criminal justice information, or any information that is classified as confidential or sensitive by federal or state law, by SO policy, or is defined as "Personal Identifying Information" under Texas Business and Commerce Code §521.002(a)(1) or "Sensitive Personal Information" as defined by Texas Business and Commerce Code §521.002(a)(2).

Your System Offices computing account may have access to confidential and sensitive information related to:

- Customers, employees, users, contractors, and volunteers (e.g., records, conversations, applications, financial information). This may include any information by which the identity of a person can be determined, either directly OR indirectly.
- SO functions (e.g., information protected by the attorney-client and attorney work product privilege, financial information, employment records, contracts, federal tax information, internal reports, memos and communications.).
- Third parties (e.g., vendor information, customer information, contracts).

As a user of SO systems, you are required to conform to applicable laws and SO policies governing confidential and sensitive information as well as any changes to those policies.

Authorized Use	I UNDERSTAND THAT: • A&M System Offices (SO) Information Resources are provided for the express purpose of conducting the business and mission of The Texas A&M University System Offices; however, brief and occasional personal use (i.e., surfing, browsing, email, instant messaging (IM)) is allowed if the following Acceptable Use Standards are followed. Personal use should not impede the conduct of state business. For employees, only incidental amounts of time—time periods comparable to reasonable coffee breaks during the day—should be used to attend to personal matters using SO Information Resources. • All users of state networks and systems should be aware that when sending an email message or other electronic transmission of a personal nature, there is the danger of the SO user's words being interpreted as official SO policy or opinion. Therefore, when a SO user sends a personal email, especially if the content of the email could be interpreted as an official SO statement, the user should use the following disclaimer at the end of the message: "This message contains the thoughts and opinions of [user's name] and does not represent official A&M System Office policy." I AGREE THAT: • I will complete the SO Information Security Awareness Training promptly upon activation of my account and annually thereafter. • I will not use SO Information Resources to: engage in acts against the mission and purposes of the A&M System or any A&M System member, intimidate or harass, degrade performance, deprive access to a SO resource, obtain extra resources beyond those allocated, or to circumvent computer security measures. • I will not intentionally access, view, create, store, download, upload, transmit, print, copy, post, or share any racist, sexist, threatening, sexually explicit, obscene or otherwise objectionable material (i.e., visual, textual, or auditory entity) and doing so is strictly prohibited. • I will not use SO Information Resources to conduct a personal business or for any personal monetary interests or gain or use for the exclusive benefit of individuals or organizations that are not part of the A&M System. Any exceptions must be in support of the SO missions and require the prior written approval of an Executive Officer of the SO. • I will not copy, reproduce or download any illegal and/or unauthorized copyrighted content or licensed software except as expressly permitted by the software license, use unauthorized copies on SO-owned computers or use software known to cause problems on SO-owned computers. • I have no right to expect privacy in my use of SO Information Resources or in the content of my communications sent or stored in SO Information Resources. All user activity is subject to monitoring, logging, and review.
Ownership and Privacy	I UNDERSTAND THAT: • Internet, instant messaging, and peer-to-peer usage (P2P), electronic files or email created, sent, received, transmitted or stored on SO Information Resources owned, leased, administered, or otherwise under the custody and control of SO are the property of SO, are not private, and are subject to the Texas Public Information Act, and may be accessed at any time by SO IT employees or other appropriate personnel without knowledge of the SO Information Resources user or owner in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards. • Information concerning SO business is subject to the Texas Public Information Act regardless of where this information is stored. These storage locations include external email accounts (Hotmail, Gmail, etc.), a home computer, mobile device or personal storage device such as a thumb drive. • I have no right to expect privacy in my use of SO Information Resources or in the content of my communications sent or stored in SO Information Resources. All user activity is subject to monitoring, logging, and review.

Data Protection	I AGREE THAT: • I will access data on a need to know basis. • I will not attempt to access data or programs contained on systems for which I do not have authorization or consent. • I will save all critical SO data (electronic files) on network servers or on a SO computer that is using the automated backup system provided by Information Technology Services (ITS) to ensure backup of the data. All data should be backed up for disaster recovery reasons. • I will maintain all records (electronic or paper) in accordance with the SO Records Retention Policy.
Virus and Software Protection	I UNDERSTAND THAT: • Computers found to be infected with a virus or other malicious code will be disconnected from the SO network until deemed safe by Information Technology Services (ITS). I AGREE THAT: • I will not connect a non-SO-owned PC to the network using a Virtual Private Network (VPN). • I will not disable or bypass virus protection software except as required by the temporary installation of software or for other special circumstances.
Instant Messaging	I AGREE THAT: • I will not download/install or use any Instant Messaging (IM) software on SO computers without specific authorization. • Authorized IM may be used for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action. • I will not use IM to conduct state business that would require the content to be saved as a state record. • I will not use IM to document a statutory obligation or SO decision. • I will not use IM when the resulting record would normally be retained for recordkeeping purposes.
Peer-to-Peer	I AGREE THAT: • If authorized for usage on state systems, I will use Peer-to-Peer (P2P) for any routine official business communication that is not normally filed for recordkeeping, such as a communication that is temporarily needed only for an employee to complete an action. • I will not download/install any P2P software onto state computers, networks, or mobile computing device without specific authorization.
Electronic Mail	I UNDERSTAND THAT: • Delivery of electronic mail is not guaranteed. I AGREE THAT: • I will not use email for purposes of political lobbying or campaigning except as permitted by the A&M System Policy and Regulations. • I will not pose as anyone other than myself when sending email, except when authorized to do so by the owner of the email account. • I will not use another user's email unless authorized to do so by the owner of the email account, or as authorized by policy for investigation, or as necessary to maintain services. • I will not use email software that poses a significant security risk to other users on the SO network. • I will not send or forward “chain” letters. • I will not send unsolicited messages to large groups except as required to conduct SO business. • I will not send excessively large messages or attachments unless in performance of official SO business. • I will not send or forward email that is likely to contain computer viruses. • I will not violate copyright laws by inappropriately distributing protected works. • I will not subscribe to mailing lists or mail services strictly for personal use. • I will not send, forward or receive confidential or sensitive SO information through non-SO email accounts (e.g., Yahoo!, Gmail, or any other email service belonging to an Internet service provider).
Internet Use	I UNDERSTAND THAT: • Software for browsing the Internet is provided to authorized users for business and research purposes only. • Due to network maintenance, performance monitoring and to ensure compliance with applicable laws and policies, all user activity may be subject to logging and review. • Email or postings by users of SO network resources to news groups, “chat rooms” or Listserv® lists must not give the impression that they are representing, giving opinions, or making statements on behalf of SO, unless authorized. • Business related purchases are subject to A&M System Disbursement of Funds Guidelines. I AGREE THAT: • Only information for which public disclosure is intended or required can be posted in public places on the internet. Nonpublic information includes confidential and controlled information. Specific examples of nonpublic information are found in the Texas A&M University System Data Classification Standard. Public places include web sites, social media, internet forums, shared drives that are accessible from the internet and cloud file sharing without authentication. • I will not post personal commercial advertising on SO web sites. • I will not make non-business related purchases over the internet unless it is incidental and does not result in direct costs to the SO, nor expose the SO to unnecessary risks. • I will use Internet facilities on state networks or systems in ways that do not disable, impair, or overload

	performance of any other computer system or network, or circumvent any system intended to protect the privacy or security of another user. • I will not download entertainment software, games or any other non-business related software or files, such as music or movies. • I will not send or receive files or documents that may cause legal liability for or embarrassment to the SO.
Confidential and Sensitive Information	I UNDERSTAND THAT: • All confidential or protected information stored on a mobile device such as a laptop, tablet, smart phone, thumb drive or other portable storage media must be encrypted. • I have no right or ownership interest in any confidential or sensitive information referred to in this Agreement. The SO may revoke my access to confidential and sensitive information at any time and without notice. I AGREE THAT: • I will not transmit confidential or sensitive information unless approved transmission protocols and security techniques are utilized. • I will not send, forward or transmit through email any confidential or sensitive information except when I send a message from my SO email account to another SO email account (from @tamus.edu to @tamus.edu). • I will, at all times, safeguard and retain the confidentiality, integrity and availability of confidential and sensitive information. • I will only access confidential and sensitive information for business needs. • I will not in any way divulge copy, release, sell, loan, review, alter, or destroy any confidential or sensitive information except as authorized. • I will not misuse or carelessly handle confidential and sensitive information. • I will encrypt confidential and sensitive information when appropriate, including when emailing such information outside the SO and when storing such information on portable electronic devices and portable storage devices. • I will safeguard and will not disclose my password or other authorization I have that allows me to access confidential and sensitive information, except as permitted by law. • I will report activities by any other individual or entity that I suspect may compromise the confidentiality, integrity or availability of confidential and sensitive information. • My privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.
Access to Data	I AGREE THAT: • Proper authorization is required for access to all data owned by the SO, except data that has been authorized by for public access. • I will not attempt to access or alter any data that I am not authorized to access in the performance of my job duties. • Except as authorized by my job responsibilities, I will not use SO Information Resources to review, alter, or otherwise act to obtain access to information about myself, or any relative, friend, or business associate. • I will use appropriate measures to prevent others from obtaining access to SO data, such as securing my workstation either by logging off or using a password-protected screen saver. • Before leaving a workstation with access to files containing confidential or sensitive information, I will logoff or activate a password-protected screen saver. • If I receive a request for the release of SO information or data, I will follow SO's policies and procedures for the release of information.
Incidental Use of Information Resources	I UNDERSTAND THAT: • Incidental personal use of electronic mail, IM, P2P, and internet access is permitted by SO Standards, but is restricted to employees and sponsored users (it does not extend to family members or other acquaintances). It must not interfere with normal performance of an employee's duties, must not result in direct costs to SO, and must not expose the SO to unnecessary risks. • All messages, files and documents stored on SO computing resources, including personal messages, files and documents, are owned by the SO and are subject to SO review. • Storage of any non-work related email messages; voice messages, files and documents within the SO email system must be nominal (less than 5% of a user's allocated mailbox space). • Any files, messages or documents residing on SO computers may be subject to public information requests. Therefore, a SO email account should not be used for personal email correspondence that is confidential.
Security	I UNDERSTAND THAT: • Where technically feasible, all PC's, laptops, mobile devices and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less to prevent unauthorized access to the device. I AGREE THAT: • I will not download and/or use security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems, except as authorized by ITS. • I will not use password cracking programs, packet sniffers, or port scanners on SO Information Resources. • I will report any weaknesses in SO computer security or any incidents of possible misuse or violation of this agreement to the proper authorities by contacting my immediate supervisor, department head, or the SO Information Security Officer (ISO). • I will not remove SO Information Resources from SO property without proper prior authorization and approval of staff with appropriate authority.

	• I will immediately report all security incidents, including the loss or theft of any SO Information Resources or data, to SO management and to the SO ISO.
Use of File Storage	I UNDERSTAND THAT: • Files stored on network file servers and cloud storage and costs state resources. I AGREE THAT: • I will not store non-work related information on network file servers or cloud storage, including pictures, music and videos. • I will not store Outlook archive (PST) files or installation files (*.exe, *.msi, *.iso) files on network file servers or cloud storage regardless of whether these files are work-related or not, without the approval of ITS. • I will not store files past their record retention schedule. • I will delete files that are no longer needed.
Software	I AGREE THAT: • I will only install or use software on SO computers that has been properly licensed and approved by ITS for my use in accordance with SO policies and procedures. • If installing or authorizing the installation of software on SO computers, I will be responsible for ensuring that such software is only used in a manner that complies with the terms of the applicable software license agreement and all applicable SO policies and procedures.
Passwords	I UNDERSTAND THAT: • Each user of SO resources is responsible for all activities conducted using his or her account(s). • Physical security of unattended computing devices options include barriers such as locked doors or security cables. Logical security options include screen saver passwords and automatic session time-outs. I AGREE THAT: • I will not share SO computer/network account, password, any personal identification number (PIN), digital certificate, security token (i.e. Smartcard), or any other similar information or device used for identification and authorization purposes. • I will not divulge digital certificate passwords used for digital signatures. • I will not circumvent password entry through use of auto logon, application “remember password” features, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the SO ISO. Any exception situation must include a procedure to change the passwords and must adhere to security policies for password construction. (For more information, see the SO’s Password Guidelines.) • I will secure unattended computing devices from unauthorized access. • I will receive and will be required to use a personal security identification code (User ID and Password) to gain access to and to use SO Information Resources. • My user ID and password are security measures that must be used only by me and I will not disclose my password to anyone. • I will be held personally responsible for any transactions initiated, actions taken, or for any harm, loss, or adverse consequences arising from the use of my user ID and password, including any unauthorized use by a third party if such party gains access to my user ID and password due to my misconduct or failure to abide by SO policy.
Portable and Remote Computing	I UNDERSTAND THAT: • Remote computers are subject to the same rules and security related requirements that apply to SO-owned computers when accessing the SO network from a remote computer. • If it is determined that required security-related software is not installed on a remote computer or that a remote computer has a virus, is party to a cyber attack or in some way endangers the security of the SO, the network connection will be disabled. Access will be re-established once ITS determines the computer is safe. • All remote access (e.g., home or public internet connections) to confidential information from a portable computing device shall utilize encryption techniques, such as VPN, Secure File Transfer Protocol (SFTP), or Secure Sockets Layers (SSL). • If critical SO data is stored on portable computing devices, it must be backed up to a SO network server or cloud storage service provided by ITS for recovery in the event of a disaster or loss of information. • Any confidential or sensitive information stored on a portable device shall be encrypted with an appropriate encryption technique. Special care (such as file encryption, file-level password protection, etc.) should be taken to protect information stored on portable computing or storage devices, and in protecting such devices from theft. I AGREE THAT: • I will password protect all computers, portable-computing devices and portable storage devices using SO information resources, especially those which process, store, or transmit confidential information, by using the “strong” password standard adopted by SO. • I will change my passwords immediately if there is suspicion the password has been compromised. • I will conform to SO Information Security Standards that apply to access from within the local area network. • I will not transfer confidential information via wireless connection to, or from, a portable computing device unless encryption methods that appropriately secure wireless transmissions, such as VPN, Secure File Transfer Protocol (SFTP), or Secure Sockets Layers (SSL) or other secure encryption protocols are utilized. • I will physically secure, using means appropriately commensurate with the associated risk, any unattended portable computing or storage device containing confidential information.

	• I will keep portable computing devices patched/updated, install anti-virus software and a personal firewall, where appropriate.