

**ADMINISTRATIVE PROCEDURES**

|  |  |
| --- | --- |
| **50.03 General Computing** | **Revised: May 17, 2022** |

1. GOVERNING REGULATIONS

This procedure is governed by the following policies and regulations:

* 1. System Regulation [29.01.02](http://policies.tamus.edu/29-01-02.pdf), Use of Licensed Software

1.2 Texas Administrative Code (TAC), Title 1, Part 10, [Chapter 202](http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), Information Security Standards

2. PURPOSE

2.1 Information resources are strategic assets of the State of Texas that must be managed as valuable state resources. The purpose of this procedure is the following:

1. Establish prudent and acceptable practices regarding the use of information resources.

b. Educate users about their responsibilities.

2.2 This procedure applies to all users of Texas A&M Forest Service information resources.

3. ACCEPTABLE USE

3.1 Users will not attempt to access any data or programs contained on agency information systems for which they do not have authorization.

3.2. Users will not attempt to circumvent information security measures that are in place.

3.3 Users will exercise caution to protect their user accounts, passwords, etc., that are used for identification and authentication.

3.5 Users will not intentionally create, store, or transmit material that is offensive, indecent, or obscene.

3.6 Users will not intentionally transmit or make available for download material that is copyrighted (such as movies, videos, music, or photos) without permission from the material’s owner.

3.7 Users will not use agency information resources for personal gain or personal business.

3.8 Use of information resources for any unauthorized purpose may result in administrative or disciplinary actions or criminal prosecution.

4. INCIDENTAL USE

4.1 Incidental personal use of e-mail, internet access, fax machines, printers, copiers, and mobile devices is restricted to approved users; it does not extend to family members or other acquaintances.

4.2 Incidental use will not result in direct cost to the agency.

4.3 Incidental use will not interfere with normal departmental operations, nor with the performance of the employee’s work duties.

4.4 No files or documents may be created, sent, or solicited electronically that may cause legal action against or embarrassment to the agency. If you receive such files without your solicitation, delete them immediately.

4.5 Storage of personal e-mails and files within agency desktop computers, laptop computers, mobile devices, or networks must be nominal.

5. INTERNET/INTRANET USE

5.1 Users will not visit web sites that are obscene, indecent, malicious, or objectionable.

5.2 Incidental use of internet / intranet is subject to the incidental use and the acceptable use sections of this procedure.

5.3 Software for browsing the internet is provided to users for agency business only.

5.4 All software used to access the internet must be part of the agency’s standard software suite or approved by the Information Resources (IR) Department. This software must incorporate all security patches.

5.5 All files downloaded from the internet must be scanned for malware using the approved IR-distributed security solutions.

5.6 All websites accessed must comply with the acceptable use section of this procedure.

5.7 All web activity on information resource assets is subject to filtering, logging, monitoring, observation, and review.

5.8 Agency internet access must not be used for personal gain or personal solicitations.

5.9 Access to the internet from agency-owned, home-based computers or mobile devices must adhere to the same procedures that apply to use from within agency facilities.

5.10 When transmitting information of sensitive nature over the internet, ensure that the website is TLS secured. This can be verified by observing the padlock icon to the left of the address bar at the top of the browser.

6. E-MAIL USE

6.1 Employees must use their assigned e-mail address for all official e-mail correspondence within and outside of the agency.

6.2 Automatic forwarding of an employee’s e-mail to an external internet service provider account, or other non-agency account shall be established only after approval from the Associate Director for Finance and Administration.

6.3 All e-mail activity is subject to filtering, logging, monitoring, observation, and review.

6.4 An employee will not send, receive, or store sensitive (confidential or non-public) information through non-agency e-mail accounts. Examples of non-agency e-mail accounts include, but are not limited to Yahoo, Gmail, and e-mail provided by internet service providers.

6.5 An employee shall not store e-mails or attachments containing sensitive (or confidential) information on unencrypted portable computing devices. Examples of portable computing devices include, but are not limited to, laptops, flash drives, external hard drives, smart phones, tablets, and other cellular devices.

6.6 When sending e-mails or attachments containing sensitive information through the internet, users should encrypt the e-mail itself and ensure that the connection is TLS secured. This can be verified by observing the padlock icon to the left of the address bar at the top of the browser.

6.7 The following e-mail activities are prohibited:

a. Sending e-mail that is disparaging, intimidating, or harassing.

b. Using e-mail for conducting personal business.

c. Using e-mail for political lobbying or campaigning.

d. Violating copyright laws by inappropriately distributing protected works.

e. Posing as someone else when sending e-mail (spoofing), except when authorized to send messages for another when serving in an administrative support role.

f. Using unauthorized e-mail software.

g. Sending unsolicited messages to large groups, except as required to conduct agency business.

h. Sending or forwarding e-mail that is likely to contain malware.

7. USE OF DIGITAL MESSAGING PLATFORMS

7.1 Digital messaging services can be used as a means to exchange near real-time messages, see whether a co-worker is online and connected (presence) and share text, files, and images.

7.2 Employees will use the agency approved messaging service, Microsoft Teams.

7.3 When using the agency messaging service, employees will follow the same acceptable use practices found in Section 6 that also apply to e-mail use.

7.4 Employees should not use third-party or free messaging platforms to conduct business that would require content to be saved or discovered as an official record.

8. AUTHORIZED SOFTWARE

8.1 All agency computers are outfitted with a standard software suite by the IR Department. Non-standard software must be purchased only through the IR Department.

8.2 Software licenses are assigned to individual computers and not to an employee. Software licenses may not be replicated. They may be transferred only from one computer to another.

8.3 Users must neither make unauthorized copies of software nor transfer software to another computer without approval from the IR Department.

8.4 Users will not download, install, or run security programs or software utility programs that may reveal or exploit weaknesses in the security of an information system. For example, users will not install or run password cracking programs.

8.5 Each employee is responsible for reporting evidence of use of unlicensed or malicious software to the IR Department.

8.6 The IR Department has the following responsibilities related to unlicensed software:

a. Delete or destroy unlicensed installations and copies of software that are not needed, or immediately obtain a license for the package. Continually audit agency software licenses to determine usage and authorization.

b. Educate employees concerning (1) the boundaries of “acceptable use” of information resources to prevent the installation and use of unlicensed software and, (2) the responsibility for reporting evidence of willful misconduct in the area to the IR Department.

c. The Information Resources Manager (IRM) has overall responsibility for agency licensing compliance.

9. PORTABLE COMPUTING

9.1 Portable computing devices include notebook or laptop computers, handheld devices (smart phones, tablets), flash drives, external drives, etc. or any computing device that is capable of storing, receiving, and/or transmitting information.

9.2 Confidential information must not be stored on unencrypted portable computing devices. Any exceptions to this requirement must be approved by the Associate Director for Finance and Administration.

9.3 All portable computing devices will be password-protected to prevent unauthorized access.

9.4 Portable computing devices will be kept physically secure using appropriate means commensurate with the associated risk.

9.5 Confidential information must not be transmitted from portable computing devices unless approved encryption techniques (for example, transport layer security, encrypted e-mail, drive encryption) are utilized.

9.6 If a portable computing device is either lost or stolen, it must be reported to the IR Department immediately.

9.7 Where appropriate, portable computing devices must be equipped with agency approved endpoint security solutions.

9.8 All data stored on portable computing devices will be scanned for malware continually during usage.

10. SECURITY AWARENESS AND TRAINING

10.1 Computing devices such as desktop and laptop computers, tablets, smart phones, flash drives, and external drives are vital to the agency’s business operations. When any computing device is either missing or stolen, the information (or data) stored in the device may be more important than the device itself. Therefore, in addition to the physical security of these devices, precautionary measures must be taken to secure the data.

10.2 Flash drives and external storage media are portable, convenient, and can hold a large amount of data. Often these devices are stored along with laptops and are likely to be incidental to the theft. When such a device is either missing or stolen, valuable information is lost and cannot be replaced easily.

10.3 Please follow these simple steps to protect your data.

a. Ensure Windows and software updates and malware definitions updates are completed regularly.

b. Create strong passwords that are difficult to guess or crack, and change passwords periodically.

c. Be aware of malware and phishing when browsing the internet.

d. Do not write down username and passwords and post or store it near the device.

e. Do not store confidential information, such as social security numbers, banking information, credit card numbers or any information that is protected by various privacy laws and regulations. This information should be stored on encrypted devices and secure cloud providers (such as OneDrive for Business).

f. Do not transmit or store confidential information through unencrypted e-mail.

g. Do not give out personal information via e-mail or over the internet.

h. Do not click on internet links that are unfamiliar or are not from a reliable source.

i. Do not respond to e-mails that request your personal information, passwords, etc.

10.4 All agency employees (full-time, part-time, seasonal, and student worker) will complete information security awareness training during the new employee orientation and on a periodic basis during employment. (See Administrative Procedure [10.31](file:///Q:\admin_procedures\1031%20Required%20Employee%20Training.docx) Required Employee Training.)

11. PROTECTING COMPUTING DEVICES

11.1 Portable computing devices should be stored out of sight when not in use.

11.2 Users will not expose desktop, laptop, or other computing devices to environmental conditions such as extreme heat, humidity, cold, extended periods of direct sunlight, or magnetic fields.

11.3 Users will take precautionary measures to isolate computing devices from flammable materials.

11.4 When feasible, users should use an uninterruptible power supply or a surge protector to protect computers from power surges.

11.5 Users should exercise care when moving computers within offices or transferring computers between locations.

11.6 All desktop and laptop computers are preset to enable password protected screen saver after 30 minutes of inactivity. This security setting shall not be changed.

11.7 All agency applications, computers, and servers shall display the following disclaimer prior to a user logging in:

“This Computer System and all data herein are official State of Texas Resources and as such are available only for authorized purposes by authorized users. Use for any other purpose may result in administrative/disciplinary actions or criminal prosecution against the user. Usage is subject to monitoring and security testing. The user should have no expectation of privacy except as otherwise provided by applicable privacy laws.”

11.8 Personnel access to offices and buildings must be controlled through the established key control process at each office location for both digital and physical key systems.

12. BACKUP AND RECOVERY

12.1 All information considered of institutional value must be copied to one or more backup storage solutions on a regular basis (backed up) for disaster recovery and business continuity. All backup solutions should include an off-site component where technically feasible. Systems considered mission-critical shall be stored in a secure, off-site location.

12.2 Electronic backups are a means to enable the recovery of data and applications in case of events such as natural disasters, storage media failure, data corruption, data entry errors, or system operations errors.

12.3 Centralized systems, servers, and mission-critical applications maintained by the agency (for example databases web applications) will be backed up on a regular basis by the IR Department.

12.4 Desktops, laptops, and other computing devices at remote locations should be backed up by the personnel to whom they are assigned. Users are individually responsible for providing adequate primary backups to ensure the recovery of institutional data in the event of failure or loss. The agency provides each user with the ability to store and share data via an approved secure enterprise data storage service (such as OneDrive for Business).

The following steps should be used to back up the data:

a. Install and enable agency approved enterprise data storage software to perform the automatic backup of data (preferred).

b. Periodically run backups to an external device (optional).

c. Choose a backup frequency based on the criticality of the data. In general, it is recommended to perform a computer backup consisting of individual user profile data (i.e., desktop, documents, favorites, pictures, etc.) at a minimum. Using the agency approved enterprise data storage system, backup is continuous when connected to the network.

d. If utilized, external backup devices should be stored in a separate, secure location whenever feasible.

CONTACT: [Information Resources Department Head](mailto:cbryan@tfs.tamu.edu), (979) 458-6607