

**ADMINISTRATIVE PROCEDURES**

|  |  |
| --- | --- |
| **50.02 Security Requirements for Information Resources**  | **Revised: May 17, 2022** |

1. GOVERNING REGULATIONS

1.1 This procedure is governed by the Texas Administrative Code, Title 1, Part 10, [Chapter 202](http://texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), Information Security Standards.

1.2 Definitions for key terms are included in Administrative Procedure [50.01](http://tfsfinance.tamu.edu/modules/finance/admin/admin_procedures/5001%20Resp%20for%20Electronic%20Info%20Resources.docx) Responsibilities for Information Resources

2. GENERAL

A designated department or person authorized to access a Texas A&M Forest Service information resource is a user. User access is controlled by means of identity management such as user accounts and access controls. Technical support staff, system administrators, database administrators, information security staff, and others require a higher level of privilege based on by their job duties. Such privileges necessitate the need for administrator accounts and special/service accounts. Passwords are a means of controlling authentication to user accounts, administrator accounts, special/service accounts, and vendor/third party accounts. Security of an information resource facility is also enhanced by controlling physical access.

3. PURPOSE

3.1 The purpose of these procedures is to:

a. Establish a process for creating, monitoring, controlling, disabling, and removing of user accounts, administrative accounts, special/service accounts, and vendor/third party accounts.

b. Establish a process for creating, changing, and safeguarding of passwords.

c. Establish a process for controlling, granting, and monitoring physical access.

3.2 These procedures apply to all individuals with authorized access to agency information resources.

4. USER ACCOUNTS FOR TFS E-MAIL AND NETWORK ACCESS

 4.1 User accounts are created by the Information Resources (IR) Department upon receiving the [Information Resources Account Activity Form](http://tfsfinance.tamu.edu/modules/finance/admin/procedures/Info%20Res%20Account%20Activity%20Form.docx) completed by the employee and approved by either the hiring supervisor or department head. The form is completed and approved as part of the hiring process.

 4.2 User accounts are created with a uniquely identifiable username and a temporary password that must be changed upon initial login. Please refer to section 7 for guidelines on creating and protecting passwords.

 4.3 User accounts that have not been accessed for more than 120 calendar days are disabled.

 4.4 User accounts have a password expiration that complies with the password guidelines (section 8).

 4.5 When an employee terminates employment with the agency, either the hiring supervisor or Employee Development will notify the IR Department two or more business days in advance whenever possible so that all access to information resources can be disabled in a timely manner. An e-mail to support@tfs.tamu.edu can be used for this purpose.

 4.6 Accounts that have been disabled more than 180 days are deleted.

 4.7 Supervisors who need access to the contents of an employee’s disabled account shall obtain prior written approval from the department head or associate director. The approved request may be submitted via e-mail to support@tfs.tamu.edu.

 4.8 Modifications to an existing employee’s access are requested by the immediate supervisor or the department head via e-mail to support@tfs.tamu.edu. Such modifications include name changes, file or folder permissions, database access and access to software or applications.

 4.9 Individual user accounts are not shared among users.

 4.10 The Networked System Administrator or other designated staff within the IR Department shall:

a. Process requests to create, modify, disable, or delete user accounts.

b. Review existing accounts for validity at least annually.

5. ADMINISTRATOR / SPECIAL ACCESS ACCOUNTS

5.1 Administrator accounts for server administration, database administration, security, and software or applications are reserved for IR Department staff.

5.2 Under special circumstances, administrative access to servers, databases, and applications may be given to authorized staff in other departments. Such requests must be approved in writing by the respective owner of the information resource and subsequently approved by designated IR Department staff.

5.3 Special access or service accounts are created with a specific expiration date to facilitate proper administrative control and are reserved for specific software installed on servers that require administrative access to run internal server processes, databases, and software or applications.

6. PHYSICAL SECURITY AND ACCESS

6.1 Physical security of and access to departmental information resource facilities are controlled and managed by the department head or designee. In doing so, the department head shall comply with building codes, fire codes, and other applicable regulations.

6.2 Physical security and access to the agency’s primary information resource facility located at the agency headquarters in College Station is controlled and managed by the IR Department.

6.3 Physical access shall be granted only to agency or other A&M System personnel whose job responsibilities require access to the facility.

6.4 Visitors, vendors, and contractors are allowed to access the information resource facility only when there is a business reason to grant access, and they are escorted by a designated staff member. Such access to sensitive areas requires logging of the details of the visit including but not limited to date and time of entry and exit, person and contact details.

7. PASSWORD GUIDELINES FOR EMPLOYEES

7.1 Passwords are confidential information and should never be shared with anyone. When working with authorized IR Department staff on technical issues that require direct account access, the following will be performed:

1. The account will be issued a temporary password.
2. The necessary technical or investigative work will be performed.
3. The user must change the password immediately after IR Department staff has finished using it.

7.3 Forgotten passwords are replaced, not reissued.

7.4 Procedures for setting and changing passwords include:

1. User identity must be verified before password is changed.
2. The password must be changed according to the password guidelines in section 9.1.
3. The user must change password at next login, where applicable.

7.5 If the security of a password is in doubt, the password shall be changed immediately. If the password has been compromised, the event shall be reported to the IR Department immediately.

7.6 Users shall not log in using a username and password assigned to any other user. The only exception is when IR Department staff is providing support to a user (section 7.1).

7.7 Users shall not circumvent password entry with auto logon, application remembering, embedded scripts or hard-coded passwords in client software. Users should always answer “NO” when prompted to have a password “remembered.” Exceptions may be made for specific applications (like automated backup) with the written approval of IR Department Head.

7.8 Users shall not write passwords on or near the computing device for easy access.

 7.9 Passwords must not be easy to guess. They must not be:

1. Your username
2. Your employee number
3. Your name
4. Your family member name
5. Your nickname
6. Your social security number or universal identification number (UIN)
7. Your birthday
8. Your license plate number
9. Your pet’s name
10. Your address
11. Your phone number
12. Name of your town or city
13. Name of your department
14. Street name
15. Make or model of a vehicle
16. Slang word
17. Obscenity
18. Technical term
19. School name, school mascot or school slogan
20. Any information about you that is known or easy to learn
21. Any popular acronym
22. Reverse character sequence of any of the above

7.10 Passwords must be easy to remember, but difficult to guess.

7.11 Substitute numbers or special characters for letters. Capitalization and substitution of characters are not easily predictable. Password phrases and spaces are also acceptable. For example, “greeneggsandham” is a weak password, but “Green Eggs & 42 Hams!” is better.

 7.13 Certain devices require password entry through a numeric keypad. In such case, avoid user telephone numbers, social security numbers, birthdates or portions thereof.

8. PASSWORD GUIDELINES FOR ADMINISTRATORS AND APPLICATION DEVELOPERS

8.1 All user and administrative account passwords shall conform to the following requirements:

a. A minimum of 14 characters,

b. At least one upper case letter, (A-Z)

c. At least one lower case letter, (a-z)

d. At least one number (0-9)

f. At least one special character or space. (!@#$%^&\*\_+=?;’”~<>|\)

8.2 All user and administrator accounts shall contain a history of at least the last four passwords used. New passwords must not be in the user or administrator account password history.

8.3 Changed passwords shall have a minimum lifespan of at least 24 hours.

8.4 Password protected information resources shall be programmed to require the users to change the passwords at least every 365 days.

8.5 A user account will be locked after five consecutive failed login attempts and will remain locked for a duration of at least 30 minutes unless otherwise reset by the IR Department according to section 7.4.

8.6 When developing software applications or deploying vendor acquired software packages, where the functionality exists, passwords shall comply with sections 7 and 8. Passwords shall not be stored in clear text within databases. Legacy applications that do not comply with this policy must have a plan to bring them into compliance or be granted a security policy exception.

8.7 Software applications utilizing password controls will be monitored continually and tested periodically by the IR Department to ensure compliance with password policies.

9. MULTI-FACTOR AUTHENTICATION (MFA) REQUIREMENTS

 9.1 All user accounts will be protected with MFA whenever possible.

9.2 All internal information systems that have login capabilities will require the use of MFA where technically feasible. Systems that store or process confidential information must have MFA enabled.

9.3 Legacy applications or platforms that do not have MFA functionality must have a plan to bring them into compliance or be granted a security policy exception.

9.4 Multi-factor authentication systems shall be configured to require re-authentication after a period of no more than five (5) days.

10. VENDOR/THIRD PARTY ACCESS

 Vendors/third parties play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and/or modify data, systems, and information resources. As a result, great care must be taken to prevent undue risk, loss of revenue or trust, or embarrassment to the agency.

10.1 Information resource owners, or designees, who provide vendors/third parties with access to mission critical or confidential information resources shall obtain formal acknowledgement from the vendor of their responsibility to comply with all applicable agency policies, rules, standards, practices, and agreements, including but not limited to:

1. Safety
2. Privacy
3. Security
4. Auditing
5. Software licensing
6. Acceptable use
7. Non-disclosure

10.2 To assure compliance with section 10.1, information resource owners or designees entering into a contract for services with a vendor/third party must obtain or create documentation indicating that the vendor will have access to mission critical information. Contracts must be processed through the Contracts Officer and should, at a minimum, address the following:

1. Description of information the vendor/third party must have access to.
2. How information is to be protected by the vendor.
3. Acceptable methods for the return, destruction, or disposal of information in the vendor’s possession at the end of the contract.
4. The identified vendor must use information and information resources for only the purpose of the business agreement.
5. Vendors/third parties must comply with terms of applicable non-disclosure agreements.
6. Any other information acquired by the vendor during the contract cannot be used for the vendor’s own purposes or divulged to others.

10.3 Access to mission critical and/or confidential information must not be given to anyone without the information resource owner’s or designee’s explicit authorization. Documentation of the access authorization must be maintained by the information resource owner or designee.

10.4 The information resource owner must also provide a point of contact for the vendor/third party. This point of contact will work with the vendor/third party to make certain the requirements set forth in this procedure are adhered to.

10.5 Each vendor/third party must provide a list of all employees working on the contract. The list must be updated and provided to the point of contact within one business day of staff changes.

10.6 Vendor/third party personnel must report all security incidents directly to agency personnel specified by the information resource owner or designee.

10.7 If vendor/third party management is involved in security incident management, the responsibilities and details must be specified in the contract.

10.8 Regular work hours and duties must be defined in the contract. Work outside of defined parameters must be approved in writing by the information resource owner or designee and if necessary to modify the scope of work in the agreement.

CONTACT: Information Resources Department Head, (979) 458-6607