Texas A&M AgriLife Research Procedures

29.01.99.A0.05 | Information Technology Account Management Procedures

Approved: July 9, 2012
Revised: October 27, 2014

Next Scheduled Review: October 27, 2019

PROCEDURE STATEMENT

This procedure establishes information technology (IT) account management procedures for all Texas A&M AgriLife Research (AgriLife Research) positions.

REASON FOR PROCEDURE

AgriLife Research, Texas A&M AgriLife Extension Service (AgriLife Extension), and the Texas A&M University College of Agriculture and Life Sciences (College) currently use a centralized identity and authentication management system in addition to independently managed computing resources with localized solutions. The purpose of this document is to outline formal guidelines and procedures related to the management of computing resource access accounts within the centralized and local management systems. These procedures are established to achieve the following:

- ensure compliance with applicable statutes, regulations, and rules regarding computer resource account management;
- define required practices regarding creation and deletion of computer resource access accounts; and
- maintain computing resource access security controls and prohibit data leakage.

PROCEDURES AND RESPONSIBILITIES

1.0 GENERAL

1.1 Terms of use:

The confidentiality and integrity of data stored on agency computer systems must be protected by controls to ensure that only authorized users have access. This access must be restricted to only those capabilities that are appropriate to each user's job duties.

1.2 Violation of these procedures may result in the loss of access privileges for AgriLife Research information resources.

1.3 Any exceptions to the procedures contained herein must be approved in advance by the Director, AgriLife Research.

2.0 ACCOUNT MANAGEMENT PROCEDURES FOR ENTERPRISE DOMAIN ACCOUNTS (AGNET)

2.1 Creation of Employee Accounts

A. All employee access accounts must be created through the *AgriLife People Management* (ALP) system by an authorized unit account manager.

B. All employee domain accounts will be created in the form of *firstname.lastname* unless an alternative is required where a duplicate name exists.

C. All employee domain accounts will receive a *firstname.lastname@ag.tamu.edu* email account address unless one of the supported alternate domains is required (e.g. @tamu.edu).

2.2 Deletion of Employee Accounts

A. All requests for removal of accounts must be filed through the ALP system **prior** to the employee's last day of employment by the unit account manager.

B. All accounts will be deactivated at the close of business on the designated last day of employment provided in the ALP system.

C. If an alternate date is required for termination of IT services, the alternate service termination date must be set along with the stated business reason for the extension. All extensions must be approved in advance by the unit or center director prior to entry into the ALP system.

2.3 Changes to Employee Directory and IT Account Services

A. Any change in an employee's unit designation or position title must be made within the ALP system.

B. IT service changes shall be performed through the ALP system by the designated unit account manager.

C. Any changes in employee responsibilities impacting IT services or data access privileges shall be assessed and communicated to the departmental IT resource or the FirstCall Help Desk system (first-call@tamu.edu).

3.0 ACCOUNT REVIEW PROCESS

The following reviews shall be performed by all unit account managers to assist in the management of employee accounts within their respective units:

3.1 A monthly report will be provided to all unit account managers listing recent monthly employee payroll terminations by unit or center. This report shall be used to verify employees listed no longer have active accounts or listings in the ALP system.

3.2 A weekly inactive users report will be provided to account managers listing any employee accounts that have exceeded 90 days of inactivity. This report shall be used to review for any unused employee accounts and assess status of the employee.

4.0 INACTIVE ACCOUNTS

Inactive accounts are defined as accounts with 90 or more days of inactivity (e.g. no email access or workstation login). The following describes how inactive accounts will be managed.

4.1 Unit account managers and IT managers should engage with account owners to assess inactive accounts—90 days or older—to determine if the account can be closed.

4.2 Any inactive accounts with 120 days of inactivity will be automatically disabled within the Enterprise IT service domain. All other computer resources not using the AGNET domain should establish the same procedure.

4.3 Any disabled enterprise IT accounts will automatically be removed at 150 days, including any data associated with the account. Any data associated with the account is the responsibility of the data owner, and should be copied or handled as required prior to the account reaching 150 days of inactivity. All other computer resources not using the AGNET domain should establish the same procedure.

5.0 LOCAL UNIT OR CENTER SYSTEM IT ACCOUNTS

Some units and centers maintain computer resources that do not use the AgriLife Enterprise Active Directory for authentication. The following requirements must be performed to meet state guidelines related to account management:

5.1 Create a documented process that is updated and reviewed annually describing the method of account management for the computing resource(s).

5.2 Create and maintain a history of account activations and deactivations for any user accounts on the system(s).

5.3 At a minimum, account requests must include date, supervisor authorization, level of access, and account name.

5.4 Account management documentation must be maintained electronically for up to 6 years within the Laserfiche system.

6.0 COPIER/NETWORK DEVICE ACTIVE DIRECTORY ACCOUNTS

Accounts for Copiers and shared network devices must have an email address configured in the account for password expiration notification

7.0 VIRTUAL PRIVATE NETWORK (VPN) ACCOUNTS (REGIONAL CENTERS)

7.1 Regional Center VPN access requests must be sent via email to the FirstCall Help Desk (first-call@tamu.edu).

7.2 All VPN access will be removed automatically upon employee account termination.

8.0 ACCOUNT PASSWORD MANAGEMENT AND LOCKOUT

8.1 Account lockout will occur after 12 failed login attempts within 30 minutes. Users will be prohibited from logging in for 15 minutes after lockout has occurred.

8.2 Users should use the *AgriLife Password Manager* to remediate any lockout issues, password changes, or resets.

8.3 Users will receive automated email notifications 20, 7, and 1 day(s) prior to their account expiring with instructions for updating.

9.0 PASSWORD STANDARDS

All passwords must be constructed and maintained according to the following guidelines:

9.1 Passwords will automatically expire every 180 days, and must be changed.

9.2 Passwords are required to be a minimum of 8 characters.

9.3 Passwords must contain at least three of the following character groups [a-z] [A-Z] [0-9] [!@#$%^&*()+].

9.4 Passwords cannot contain any portion of your name, social security number, nickname, relatives, names, or birth date.

9.5 Passwords should not be dictionary words or acronyms.

9.6 Passwords should be unique and not used on other systems or services.

9.7 Passwords must not be publically displayed or exposed to anyone.

9.8 If security of a password is in doubt, it should be changed immediately.

9.9 System administrators must not circumvent password guidelines for the sake of ease–of–use.

10.0 ACCOUNT OWNER RESPONSIBILITIES

10.1 Account owners are responsible for all computer transactions that are made with his/her user ID and password.

10.2 Account owners shall not disclose passwords to others.

10.3 Account owners shall not circumvent any security controls and measures deployed on a computing resource inclusive of:

- anti–virus software;
- inactivity lockout;
- security login banners; and
- any other safeguards established to meet state–mandated IT security policies or IT management procedures.

11.0 SHARED OR GENERIC EMAIL ACCOUNTS

All requests for generic or shared email accounts shall use the *AgriLife IT Enterprise Services Shared or Generic Email Account Request* form, and be filed with the AgriLife IT FirstCall Help Desk when adding an account.

12.0 VENDOR ACCESS

All applicable rules and procedures regarding approval and acknowledgement of vendor access to computing resources shall be completed and authorized prior to requesting vendor access accounts to any system or service. See section 9.9 of AgriLife Research Procedure 29.01.03.A0.01, *Information Resource Procedures*.

12.1 All vendor access requests within the AgriLife Enterprise system must be sent to the FirstCall Help Desk (first-call@tamu.edu) a minimum of 5 days prior to the request date, and must be approved and authorized by the Director of AgriLife IT or designee.

12.2 All requests must include a start date, end date, and purpose for access.

RELATED STATUTES, POLICIES, OR REQUIREMENTS

AgriLife Research Procedure 29.01.03.A0.01, *Information Resource Procedures*

AgriLife Research Procedure 61.99.01.A1.01, *Retention of State Records*

AgriLife People Management System

AgriLife Password Manager

AgriLife IT Enterprise Services Shared or Generic Email Account Request Form

DEFINITIONS

AgriLife People Manager (ALP) http://agrilifepeople.tamu.edu—Texas A&M AgriLife Identity Management system used to provision, de-provision, and manage IT accounts for Texas A&M AgriLife Research, Texas A&M AgriLife Extension Service, and the Texas A&M University College of Agriculture and Life Sciences departments and units.

Authorized Unit Account Manager—Designated employee trained in the use of the *AgriLife People Manager* system that is authorized to perform account creation, deletion, and deactivation.

Enterprise Domain (AGNET) Account—A user account issued to employees, graduate students, or student workers providing for access to workstations, email, and other Texas A&M AgriLife IT services.

CONTACT OFFICE

For questions, contact AgriLife Information Technology at 979-845-9689 or first-call@tamu.edu.