COLLEGE OF AGRICULTURE AND LIFE SCIENCES GUIDELINES

INFORMATION TECHNOLOGY ACCOUNT MANAGEMENT PROCEDURES

Approved: July 9, 2012

Next Scheduled Review: July 9, 2014

PROCEDURE STATEMENT

This procedure establishes information resource account management procedures for Texas A&M College of Agriculture and Life Sciences positions.

REASON FOR PROCEDURE

The Texas AgriLife Extension Service, Texas AgriLife Research, and the College of Agriculture and Life Sciences currently use a centralized identity management system (Active Directory) 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 accounts within the centralized and local management systems. These procedures are established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and rules regarding computer resource account management;
- To define required practices regarding creation and deletion of computer resource access accounts;
- To 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 subject to loss of access privileges for Texas AgriLife Research information resources.

1.3 Any exceptions to the procedures outlined must be preapproved by the Dean of the College of Agriculture and Life Sciences.

2.0 ACCOUNT MANAGEMENT PROCEDURES FOR ENTERPRISE DOMAIN ACCOUNTS (AGNET)

2.1 Creation of Employee Accounts

A. All employee domain accounts must have an associated request record created within the APM 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 should be filed through the APM system prior to the last day of employment for an employee 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 APM 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 pre-approved by the unit or center director prior to entry into the APM 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 APM system.

B. Additional IT service changes should be directed to local unit IT resource or the AIT FirstCall Help Desk system (first-call@tamu.edu).

C. Any changes in employee responsibilities should be assessed with regard to impact to IT services or data access and communicated to the unit IT resource or the FirstCall Help Desk system (first-call@tamu.edu).

3.0 ACCOUNT REVIEW PROCESS

The following reviews should 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 should be used to verify employees listed no longer have active accounts or listings in the APM 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 should be used to review for any unused employee accounts and assess status of the employee.

3.3 Unit account managers will be required to certify unit account accuracy within the APM system, once every 90 days. An automated email reminder will be provided.

4.0 INACTIVE ACCOUNTS

Inactive accounts are defined as accounts with 90 or more days no activity (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 AGNET 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 Account requests must include date, supervisor authorization, level of access, and account name at a minimum.

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 VPN ACCOUNTS (REGIONAL CENTERS)

7.1 Regional Center Virtual Private Network 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. User will be prohibited from logging in for 15 minutes after lockout has occurred.

8.2 Users should use the AgriLife Password Manager (https://agrilifepass.tamu.edu) to remediate any lockout issues, password changes or resets.

8.3 Users will receive automated email notifications 20, 7 and 1 days 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 can not 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

All account owners have the following responsibilities:

10.1 Responsibility for all computer transactions that are made with his/her User ID and password.

10.2 Shall not disclose passwords to others.

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

- Anti-Virus Software
- Inactivity Lockout
- Security Login Banners
- 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 should use the form at (*http://ait.tamu.edu/forms/shared-genericmailbox.pdf*) and be filed with the AgriLife IT FirstCall Help Desk when adding an account.

12.0 VENDOR ACCESS

All applicable rules regarding approval and acknowledgement of vendor access to computing resources should be completed and authorized PRIOR to requesting vendor access accounts to any system or service. (See Texas A&M University Standard Administrative Procedure http://rules.tamu.edu/PDFs/29.01.99.M1.22.pdf)

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 request date and must be approved and authorized by the Director of IT or his designee.

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

DEFINITIONS

AgriLife People Manager - http://agrilifepeople.tamu.edu *(APM)*—The web application used to provision, de-provision, and manage IT accounts for the College of Agriculture and Life Sciences, Texas AgriLife Research and Extension Service Departments and Units.

Authorized Unit Account Manager—Designated employee trained in the use of the AgriLife People Management 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 IT services.

CONTACT OFFICE

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