Texas A&M Veterinary Medical Diagnostic Laboratory Procedures

29.01.99.V0.05 | Information Technology Account Management Procedures

Approved: April 29, 2022

Next Scheduled Review: April 29, 2027

Click Here to View Revision History

PROCEDURE SUMMARY

This procedure establishes information technology (IT) account management procedures for all Texas A&M Veterinary Medical Diagnostic Laboratory (TVMDL) positions.

AgriLife Research, Texas A&M AgriLife Extension Service, and TVMDL 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.

Click **here** to view **Definitions**.

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 TVMDL information resources.

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

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 Identity 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.

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 (firstcall@ag.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 departmental account status dashboard provided within ALP should be reviewed for 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, <u>including any data associated with the account</u>. 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 At a minimum, account requests must include date, supervisor authorization, level of access, and account name.

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

6.1 Regional Center VPN access requests must be requested via ALP.

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

7.0 ACCOUNT PASSWORD MANAGEMENT AND LOCKOUT

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

7.2 Users should use the https://firstcallhelp.tamu.edu/knowledge-base/agnet-password-reset/ to remediate any lockout issues, password changes, or resets.

7.3 Users will receive automated email notifications every day for 30 days prior to their account password expiring with instructions for updating.

8.0 PASSWORD STANDARDS

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

1) Complex Passwords

a. Passwords will automatically expire every 2 years and must be changed.
b. Passwords are required to be a minimum of 12 characters.
c. Passwords must contain at least three of the following character groups [a-z] [A-Z] [0-9] [!@#$%^&*()+].
d. Passwords cannot contain any portion of your name, social security number, nickname, relatives, names, or birth date.
e. Passwords should not be dictionary words or acronyms.
f. Passwords should be unique and not used on other systems or services.
g. Passwords must not be publicly displayed or exposed to anyone.
h. Passwords must not be shared except when reviewed and approved by IT for special business purposes where risk has been reasonably mitigated.
i. If security of a password is in doubt, it should be changed immediately.
j. System administrators must not circumvent password guidelines for the sake of ease–of–use.

2) Long Term Passwords

a. Long term passwords may only be used when systems, applications, and/or process can support them and it is approved by IT management (some systems may not be able to support these)
b. Long Term Passwords must be 15 characters long or greater.
c. Long term passwords are required to be reset if a password expiration requirement is determined in the IT approval process or if it is determined there is an applicable risk that requires a reset.
d. Use passphrases which should include common punctuation characters to improve usability and increase variety.
e. Do not use common or general phrases that would be easily guessed.
f. NOTE: Service and Privileged Account passwords are examples where this may be utilized and may be shared among administrators with authorization and approval. The review and approval process will determine the password expiration requirement. All other applicable standards noted in the General Passwords section are also required.

9.0 ACCOUNT OWNER RESPONSIBILITIES

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

9.2 Account owners shall not disclose passwords to others.

9.3 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.

10.0 EMAIL ACCOUNTS

10.1 Email Account Termination

Email Accounts will be terminated upon the last day of employment.

10.2 Shared or Generic Email

All requests for generic or shared email accounts shall be submitted via AgriLife People (ALP) system.

10.3 Email Data Retention

The AgriLife People Identity Management system provides an option to send email account data to a supervisor upon termination of an employee. If no designation is made the data will no longer be accessible upon termination of the employee account after 14 days.

10.4 Texas A&M AgriLife does not provide email accounts for non-employees or for those with emeritus status.

10.5 Electronic Marketing Communications

Users or departments with mailing lists containing more than 100 external recipients should consider using a third-party electronic mailing service and comply with the provisions of the federal CAN-SPAM Act.

11.0 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 TVMDL Procedure 29.01.03.A0.01, *Information Resource Procedures*.

RELATED STATUTES, POLICIES, OR REQUIREMENTS

TVMDL Procedure *29.01.03.A0.01, Information Resource Procedures*

TVMDL Procedure *61.99.01.A1.01, Retention of State Records*

AgriLife People Management System

AgriLife Password Manager

DEFINITIONS

AgriLife People Manager (ALP) https://agrilifepeople.tamu.edu/: Texas A&M AgriLife Identity Management system used to provision, de-provision, and manage IT accounts for Texas A&M TVMDL, Texas A&M AgriLife Extension Service, Texas A&M Veterinary Medical Diagnostic Laboratory 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

Questions concerning this procedure should be referred to AgriLife Information Technology at 979-845-9689 or first-call@tamu.edu.

REVISION HISTORY

Approved: April 29, 2022

Next Scheduled Review: April 29, 2027