APHIS USER ACCOUNT MANAGEMENT POLICY

1. PURPOSE

This Directive establishes APHIS policy for management of user accounts on APHIS-owned information systems.

2. REFERENCES

a. National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems. http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf

b. Federal Information Systems Controls Audit Manual (FISCAM), Volume 1: Financial Statement Audits.

c. OMB Circular A-123, Management Accountability and Control.

d. OMB Circular A-130, Management of Federal Information Resources.

3. SCOPE

a. This Directive applies to:

(1) All user accounts on all APHIS information systems, including major applications, general support systems, and APHIS domains.

(2) All individuals who use APHIS information systems, including APHIS employees, contractors, employees of other Federal agencies, employees of State and local governments, and authorized private organizations or individuals.

b. This Directive does not apply to:

(1) Local user accounts on desktop computers.

(2) USDA systems that use Form AD-1143, Corporate Systems Access Request Form.

4. DEFINITIONS

a. Concept of Least Privilege. A basic tenet of computer security which states that users should be granted the minimum level of security access required to accomplish their assigned responsibilities.

b. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

c. Non-privileged Account. A user account with no administrative rights on the system.

d. Privileged Account. A user account with administrative rights on the system.

e. Recertification. The process for confirming that a user account has been properly authorized and is still required by the user.

f. System Administrator. The individual possessing administrative rights to make changes for user and group accounts for a particular system.

g. System Owner. The individual responsible for establishing the rules for appropriate use and protection of the data/information within a system.

h. User. An individual or (system) process authorized to access an information system.

i. User Account. The unique identity and credentials assigned to a user, usually consisting of a "User ID" and password, which allows the user to gain access to the information system.

5. POLICY

Secure management of user access and accounts is vital to protecting APHIS computer systems and information. Documents referenced in Section 2 provide recommended security controls to accomplish this objective. This Directive establishes APHIS requirements and processes for the implementation of controls for management of user access, as follows:

a. Form 513, APHIS User Account Control Form, (Attachment 2) will be used to request initial access, modifications to access, and termination of access to all APHIS information systems, for the following user events:

(1) Work start date – form will be submitted 14 calendar days prior to work start date.

(2) Intra-Agency transfer or change of job duties – form will be submitted within 14 calendar days following these events.

(3) Termination – form will be submitted within 7 calendar days following employee or contractor termination, or cessation of work for which access was required.

b. APHIS authorizes all APHIS employees to have a non-privileged user account for the following systems, and grants an exemption from using Form 513 (Attachment 2) for requesting and granting non-privileged access to these systems. Please note that the exemption is for non-privileged accounts only; the use of Form 513 is required for privileged accounts.

(1) APHIS domain accounts.

(2) APHIS e-mail system.

(3) APHIS Instant Messaging system.

c. Accounts established for emergency or temporary access will be removed within 7 calendar days of the termination date specified on Form 513 (Attachment 2).

d. Accounts established for APHIS employees will be removed within 30 calendar days of employee termination.

e. User accounts will be disabled after 45 days of inactivity.

f. All user accounts will be recertified at least annually.

g. If the system or access level being requested requires a security clearance, credible documentation that the user possesses the security clearance required must be provided to the system owner or system administrator before the user account is created.

h. Generic accounts will not be created unless the request has been documented, reviewed, and approved.

i. Duplicate accounts will not be assigned to a user unless required for proper segregation of duties.

j. Supervisors, system owners, and system administrators will adhere to the concept of Least Privilege when authorizing, configuring, and managing user account access.

k. User account management documentation required by this Directive will be retained as follows:

(1) Authorizations and account modifications will be retained for the life of the account.

(2) Termination requests will be retained for 1 year.

(3) User Account Recertification documentation (Attachment 1) will be retained for 5 years, and will be retained and disposed of by calendar year (no incremental disposal).

6. RESPONSIBILITIES

a. The APHIS Chief Information Officer (CIO) will:

(1) Approve and ensure implementation of this Directive.

(2) Approve any modifications to this Directive.

b. Deputy Administrators/Directors of Program Units, and Heads of Major Business Offices will:

(1) Disseminate this Directive to their respective staffs.

(2) Ensure that appropriate procedures are developed and implemented to support implementation of this Directive within their program units.

(3) Assist in promptly identifying, investigating, and rectifying violations of this Directive.

c. APHIS Supervisors and Contracting Officer Technical Representatives (COTRs) for APHIS contractors will:

(1) Ensure that Form 513 (Attachment 2) is completed and forwarded to the appropriate system administrators to notify them of impacts to user accounts in conformance with the terms of this Directive.

(2) Authorize requests for user accounts to APHIS information systems by signing Form 513 (Attachment 2) and giving, mailing, or e-mailing it to the system administrator (if form is e-mailed, it must be sent from the supervisor's/COTR's e-mail account).

(3) Upon request from system administrator(s), promptly review lists of system user accounts, and recertify or provide corrections to system administrators.

(4) Ensure that system owners and administrators are adequately trained in the processes and requirements of this Directive.

d. Program Unit CIOs and/or Information System Security Managers (ISSMs) will:

(1) Ensure that annual and quarterly User Account Recertifications are performed in accordance with the terms of this Directive.

(2) Review and sign User Account Recertification Reports provided by system owners, as appropriate.

e. System Owners and/or System Administrators will:

(1) Manage user accounts in conformance with the terms of this Directive.

(2) Provide guidance and work collaboratively with supervisors and COTRs to identify and configure user accounts in line with the concept of Least Privilege.

(3) Annually perform a User Account Recertification (see Attachment 1 for process description) for all information system user accounts.

(4) Quarterly perform a User Account Recertification (see Attachment 1 for process description) for a random sample of user accounts, to ensure that the security controls for user access are functioning properly for the system.

(5) Prepare User Account Recertification Reports as described in Attachment 1, for review, approval, and signature by the Program Unit CIO or ISSM.

(6) Be responsible for the retention of all documentation pertaining to user accounts for the system, including Form 513 (Attachment 2), and User Account Recertification documentation and Reports (Attachment 1).

f. APHIS employees will follow the procedures outlined in this Directive when requesting creation, modification, or termination of user accounts.

7. INQUIRIES

a. Questions concerning the information and processes described in this Directive should be directed to the Manager, MRPBS, ITD, CSB.

b. This Directive can be accessed at ***www.aphis.usda.gov/library***

/s/
Gregory L. Parham
APHIS Chief Information Officer

2 Attachments