APHIS REMOTE ACCESS MANAGEMENT POLICY

1. PURPOSE

There is an inherent security risk in allowing remote access to an enterprise network. This Directive establishes:

a. The policy for management of remote access to APHIS networks and systems from external sources.

b. The requirement for secure protection of APHIS networks and systems from external sources.

2. AUTHORITIES and REFERENCES

a. USDA Department Manual 3525, Telework and Remote Access Security.

b. National Institute of Standards and Technology Special Publication 800-46, Security for Telecommuting and Broadband Considerations.

c. National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems.

d. Government Accounting Office Federal Information Systems Control Audit Manual (FISCAM) AC3-2.

e. Office of Management and Budget Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

3. SCOPE

This Directive applies to:

a. All individuals who have been authorized to remotely access APHIS networks and systems, including APHIS employees, contractors, employees of other Federal agencies, employees of State and local Governments, public and private organizations, and private individuals.

b. The APHIS networks and systems covered by this Directive include all general support systems, information systems, applications, computer hardware and software, and telecommunications hardware and software that support APHIS business functions.

4. DEFINITIONS

a. Employee. Full or part time Government employee or contractor employed by APHIS.

b. External Sources. Sources external to the APHIS enterprise network. These sources are not managed by APHIS. Sources may include broadband Internet connections, dial-up connections, dedicated circuits, wireless connections, cellular telephones, aircards, software, and other sources.

c. Government-Owned Computer System. A system that is owned by the Government. Systems may include servers, laptops, desktops, handheld computers, and others.

d. Non-employee Account. The unique identity and credentials assigned to a non-APHIS user which allows the user to gain access to APHIS networks or systems.

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

f. Remote Access. The ability to get access to a computer system or a network from a remote location or a location that is external to the computer system or network.

g. Split Tunneling. The process of allowing a remote user to access a public network, most commonly the Internet, from the user's external source connection at the same time that the user is allowed a secure connection to resources on the APHIS network.

h. User. An individual or (system) process authorized to access a network or system.

5. POLICY

Management of remote access to APHIS networks and systems is critical to ensuring the integrity, availability, and confidentiality of APHIS systems, information, and network infrastructure. This Directive establishes APHIS requirements for remote access management as follows:

a. Authentication, encryption, and active monitoring mechanisms will be used for remote access systems to protect the integrity and confidentiality of APHIS networks and systems.

b. Two-Factor Authentication will be used for all users who remotely access APHIS networks and systems.

c. No Split-Tunneling will be allowed through remote access sessions.

d. All remote access will be managed and controlled through centrally managed resources.

e. Real time or near real time analysis of remote session events will be employed to detect system level alerts.

f. Remote access sessions will be automatically disconnected upon logout or session inactivity lasting longer than 30 minutes.

g. All users, both employees and non-employees, are required to use the APHIS-provided remote access client for remote access.

h. All users are to conduct only official and approved Government business through remote access.

i. Only employees with a valid APHIS domain account will be allowed to remotely connect to APHIS networks and systems. Technical security controls will be used to prevent authenticating on the APHIS network without a valid domain account.

j. Employees must use a computer system that is provided or approved by APHIS to remotely access the APHIS networks and systems.

k. Employees must have installed and running on their computer system the current APHIS issued:

(1) Agency standard operating system image;

(2) Patchlink agent;

(3) Personal firewall; and

(4) Anti-virus software and virus definition files.

l. Non-employees are not required to use Government-owned computer systems to access APHIS networks and systems; however, they must identify:

(1) A valid business reason for requiring remote access to APHIS networks and systems.

(2) The computer name of the system(s) requiring remote access.

(3) The operating system of the computer system(s) requiring remote access.

(4) The name and version of the active anti-virus software running on the computer system(s).

(5) The name and version of the local firewall protection on the computer system(s).

m. Requests for remote access for non-employees must be reviewed and approved by the APHIS program office authorizing official and the APHIS Telecommunications Manager for non-employees to gain remote access to APHIS networks and systems.

n. APHIS Form 516, Remote Access Account Control Form (see Attachment 1), will be used to request a remote access account or to request termination of a remote access account for non-employees.

o. APHIS Form 516 will be retained by the APHIS Telecommunications Manager for a period of 2 years from the date of issue. The APHIS program office authorizing official, the user, and the user's supervisor or representative should also retain a copy of the form.

p. All non-employee accounts for remote access will have a termination date that coincides with the cessation date of the work for which access was required.

q. No users with remote access privileges have rights to expect privacy in their use of APHIS networks and systems.

r. Remote access computers should not be used as servers (e.g., Web servers, private e-mail servers, File Transfer Protocol (ftp) sites, or chat servers).

6. RESPONSIBILITIES

a. The Chief Information Officer (CIO), Information Technology Division (ITD), will:

(1) Mandate the creation of, and compliance with, remote access management policies to ensure the availability, integrity, and confidentiality of APHIS networks and resources.

(2) Have the final approval regarding adequacy of the systems and security measures of the remote access systems.

(3) Provide guidance to program units on remote access standards and requirements.

(4) Ensure procedures are in place for the review and approval of non-employee requests for remote access.

(5) Ensure appropriate response and recovery actions are taken for suspected breaches or violations of APHIS networks and systems through remote access systems.

b. The Chief Technology Officer (CTO), ITD, will:

(1) Plan for remote access system expenses, maintenance, and upgrades.

(2) Ensure that contingency plans for remote access systems are developed, tested, and maintained to ensure the continual availability and performance of remote access for employees and non-employees.

(3) Ensure that technical and security controls are in place to authenticate and provide account management for remote access users.

(4) Ensure that operating procedures are developed for the security and operation of the remote access systems and functions.

(5) Ensure that personnel responsible for the operation, maintenance, and security of the remote access systems are properly trained for their respective roles.

(6) Ensure procedures are in place to address suspected network or system penetrations or violations through remote access connections.

(7) Ensure the review and recertification of non-employee accounts for remote access are completed.

c. The Telecommunications Manager, ITD, will:

(1) Ensure that development, implementation, maintenance, and security procedures for remote access systems are completed.

(2) Review all non-employee requests for remote access and provide approval/disapproval.

(3) Ensure that user accounts for non-employees are established upon approval of requests.

(4) Ensure that remote system audit trails are developed, implemented, maintained, and regularly reviewed for alerts, violations, suspected penetrations, or other abnormalities or intrusions that would prevent or hinder APHIS business operations.

(5) Establish procedures for responding to violations or incidents of APHIS remote access systems and procedures for promptly notifying the ITD CIO, CTO, and Information Systems Security Program Manager (ISSPM) of the violations or incidents.

(6) Be responsible for retention of all documentation pertaining to non-employee accounts for remote access, including APHIS Form 513, APHIS User Account Control Form (see Attachment 2), for a period of 2 years from date of approval or denial of the request.

d. The Enterprise Operations Services Branch Manager, ITD, will:

(1) Establish and maintain processes for providing centralized support with users on remote access connectivity or configuration issues.

(2) Provide oversight for the administration of user domain accounts with the appropriate level of internal access to APHIS systems and services.

(3) Ensure that APHIS-owned computer systems are imaged with the current APHIS operating system and services to include patchlink agent, personal firewall, and anti-virus software.

(4) Assist in the development of APHIS standards for computer systems used for remote access.

(5) Assist in identifying technical security risks and technical security controls applicable to APHIS computer systems used for remote access.

(6) Promote general guidance, awareness, and training on remote access usage and users' responsibilities.

e. The Information Systems Security Program Manager (ISSPM), ITD, will:

(1) Participate in developing remote access management policies that define how remote access will be allowed or explicitly denied, how remote access services will be used, the conditions for exception to this Directive, and rules used to design and implement the security for the remote access systems.

(2) Disseminate information on security postures and measures for remote access systems, including encryption and authentication methods and industry best practices and standards.

(3) Evaluate the compliance of remote access systems with policies or procedures.

f. The Information Systems Security Manager/Officer (ISSM) ITD, will:

(1) Investigate remote access system incidents or violations. He/she also will make initial and final reports of incidents and violations to the APHIS ISSPM.

(2) Update the overall Agency security plans to reflect remote access policies, as required.

g. The Deputy Administrators/Directors of Program Units and heads of major business offices will:

(1) Ensure employees in their program units/business offices are aware of and adhere to this Directive.

(2) Enforce the rules and regulations under their control for the protection of APHIS networks and resources.

(3) Ensure that procedures are in place to properly identify and document a non-employee's need to access APHIS networks and systems.

(4) Ensure that Government-owned computer systems are provided to employees approved to use such systems at remote locations.

(5) Ensure employees in their program unit are in compliance with the Government furnished computer system requirements listed in Section 5.k.

(6) Notify the APHIS CIO within 10 calendar days of a non-employee's termination or when there is no longer a need to provide remote access.

(7) Assist in identifying, investigating, and rectifying violations of this Directive and APHIS approved standards and procedures for remote access.

h. All users will:

(1) Follow the policies outlined in this Directive.

(2) Conduct only official and approved Government business using remote access.

(3) Be responsible for safeguarding their logon credentials as well as the networks and systems they are accessing.

(4) Not attempt to compromise, tamper, hinder, or break into any networks or systems, whether USDA, APHIS, or other Federal, State, public, or private networks and/or systems.

(5) Logoff or logout of their remote access session whenever they leave their computer systems for an extended period to include breaks, lunch, or at the end of their work day.

7. COMPLIANCE AND SANCTIONS

a. All users of APHIS networks and systems are individually and personally responsible for complying with Federal, USDA, and APHIS policies on remote access, as well as with the procedures and practices developed in support of this Directive.

b. Any user, whether employee or non-employee, that attempts to compromise, hinder, or invade in any way, APHIS networks or systems, will be denied access and disciplinary or legal actions may be taken.

8. EXCEPTIONS

a. Exceptions that reduce the requirements of this Directive require approval from Deputy Administrators/Directors for Program Units, the APHIS CIO, or the APHIS Administrator.

b. Exceptions must be made in writing to either the Deputy Administrators/Directors for Program Units, the APHIS CIO, or the APHIS Administrator with proper justification for the exception.

c. Any exceptions to this Directive must be technically and administratively supported by APHIS and must align with the APHIS business mission and functions.

9. INQUIRIES

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

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

/s/
Marilyn L. Holland
APHIS Chief Information Officer

Attachments