U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	Number: DR 3505-003
SUBJECT: Access Control Policy	DATE: August 11, 2009
	OPI: Deputy Chief Information Officer (DCIO) for Policy & Architecture

1. PURPOSE

a. The policy in this United States Department of Agriculture (USDA) Departmental Regulation (DR) establishes the basis for implementing secure access control practices for protecting information systems and data within the United States Department of Agriculture (USDA).

b. This policy adheres to the guidance identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Appendix F as:

Identifier	Family	Class
AC-1	Access Control Policy and Procedures	Technical
AC-2	Account Management	Technical
AC-6	Least Privilege	Technical
IA-2	Identification & Authentication	Technical

2. SPECIAL INSTRUCTIONS/CANCELLATION

This regulation supersedes the Access Control policy included in Departmental Manual (DM) 3140-001.

3. BACKGROUND

a. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), mandates that all federal agencies develop, document, and implement an organization-wide program to provide security for the information systems that support their operations and assets.

b. In addition, Office of Management and Budget (OMB) Circular A-130 defines adequate security as security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

4. POLICY

a. Agencies will ensure that access to all Information Technology (IT) systems is in compliance with applicable Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) Special Publications and OMB standards (See Appendix C – Authorities and References).

b. USDA information systems shall uniquely identify and authenticate all users.

c. Each USDA agency must establish, maintain, and fully document a user account management program to administer user accounts for all agency information systems. This program must implement procedures to establish, activate, modify, review, disable, and remove user accounts.

d. Authorizations to access and use USDA information technology (IT) resources will be granted by business owners responsible for those resources and will be based on official business "Need to Know" and limited to the "Least Privilege" access required to perform job functions (see Appendix A- Definitions).

e. Agencies will implement dual factor authentication for all forms of remote access to agency information systems.

f. Individuals who will be granted access to USDA information systems must first undergo the Personal Identity Verification (PIV) process mandated by Homeland Security Presidential Directive-12 (HSPD-12) in accordance with applicable guidance such as that set forth in Office of Management and Budget (OMB) M-05-24 and Federal Information Processing Standards (FIPS) 201-1.

g. When an employee or contractor is terminated, all of their IDs and passwords or other means of accessing files or using computer resources must be disabled or removed within 48 hours of their departure. If the termination is not amicable, Agencies should remove all access prior to the employee or contractor's departure.

h. Agencies will ensure adequate separation of duties within the roles of the information system. Agencies will establish compensating controls when a conflict of separation of duties is identified.

i. All USDA information systems must display the USDA approved system use notification warning/terms of use banner before granting users system access.

j. Any exceptions that are granted will be temporary and expire at the end of each fiscal year. Agencies shall submit all policy exception requests directly to the Associate Chief Information Officer for Cyber and Privacy Policy Oversight (ACIO-CPPO).

5. PROCEDURES AND GUIDANCE

The policies in this regulation provide the framework for access control to USDA systems and will be further shaped by other USDA regulations and manuals that contain clarifying procedures. The USDA Departmental regulations and manuals can be found at: http://www.ocio.usda.gov/directives/index.html.

6. RESPONSIBILITIES

a. The DCIO for Policy and Architecture is responsible for:

(1) Establishing policy for security over wireless networks; and

(2) Enforcing the policy through compliance reviews, automated tools, and other means as necessary.

b. Agency CIOs are responsible for:

(1) Implementing this policy within their respective agency and/or office; and

(2) Providing proper evidence of compliance as necessary and upon request.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DR 4070-735-001 *Employee Responsibilities and Conduct*, Section 16, sets forth the USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of Computers and Telecommunications Equipment. In addition, Section 21, Disciplinary or Adverse Action, states:

a. A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action.

b. Disciplinary or adverse action shall be effected in accordance with applicable law and regulations.

-END-

APPENDIX A

DEFINITIONS

a. Least Privileged User Account - Users should run at all times with as few permissions as needed to perform actions, launch applications, and/or run services on a computer system.

b. Need to Know - Access to information necessary for conducting one's official duties.

c. Remote Access - Communication with a data process facility from a remote location or facility through a data link.

APPENDIX B

ABBREVIATIONS

CIO	Chief Information Officer
DM	Departmental Manual
DR	Departmental Regulation
FIPS	Federal Information Processing Standards
HSPD	Homeland Security Presidential Directive
ID	Identification
ISA	Interconnection Security Agreement
ISSPM	Information Systems Security Program Manager
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PUB	Publication
SP	Special Publication
USDA	United States Department of Agriculture

APPENDIX C

AUTHORITIES AND REFERENCES

Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

FIPS PUB 140-2 Annex A, *Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, December 2007.

FIPS PUB 201-1, Change Notice 1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.

Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, June 2007.

NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006.

NIST SP 800-63, Version 1.0.2, *Electronic Authentication Guideline*, April 2006.

NIST SP 800-88, *Guidelines for Media Sanitization*, September 2006.

Office of Management and Budget (OMB) M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005.

OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003.

OMB M-06-16, *Protection of Sensitive Agency Information*, June 2006.