DEPARTMENTAL REGULATION

Number: DR 3505-003

DATE: February 10, 2015

OPI: Office of the Chief Information Officer – Agriculture Security Operations Center

SUBJECT: Access Control for Information and Information Systems

Section | Page
---|---
1. Purpose | 2
2. Scope | 2
3. Special Instructions/Cancellations | 2
4. Background | 3
5. Policy | 3
6. Account Management | 4
7. Access Management | 8
8. Information Flow Enforcement | 10
9. Separation of Duties | 11
10. Least Privilege | 11
11. Unsuccessful Login Attempts | 12
12. System Use Notification | 12
13. Concurrent Session Control | 13
14. Session Lock | 13
15. Permitted Actions Without Identification or Authentication | 14
16. Remote Access | 14
17. Wireless Access | 15
18. Mobile Devices | 15
19. Use of Internal/External Data and Information Sharing | 16
20. Publicly Accessible Content | 17
21. Roles and Responsibilities | 17
22. Penalties and Disciplinary Actions for Non-Compliance | 21
23. Policy Exceptions | 22

Appendix A Definitions | A-1
Appendix B Acronyms and Abbreviations | B-1
Appendix C Authorities and References | C-1
1. PURPOSE

a. This Departmental Regulation (DR) establishes the logical access control policy of the United States Department of Agriculture (USDA or “Department”) for meeting the applicable laws, regulations, and standards of the Federal Government.

b. This policy establishes the access controls that agencies and staff offices shall implement and comply with to ensure the availability, integrity, and confidentiality of USDA information and information technology (IT) resources.

c. This DR documents USDA responsibility to comply with federal requirements to establish, implement, and support access control policies to manage risk to USDA systems.

2. SCOPE

a. This policy applies to all USDA agencies, staff offices, employees, appointees, contractors, and others working for or on behalf of the USDA.

b. This policy includes controls for access, audit and accountability, identification and authentication, media protection, and personnel security as they relate to components of logical access control.

c. This policy addresses all system access, whether accomplished locally, remotely, wirelessly, or through other means.

d. This policy does not apply to classified communications and systems.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

This policy supersedes the following Departmental directives and/or appendices, as specified:

a. DR 3505-003, Access Control Policy, August 11, 2009;


c. DM 3535-000, C2 Controlled Access Protection, May 11, 2005; and

d. DM 3535-001, USDA’s C2 Level of Trust, February 17, 2005.
4. BACKGROUND

   a. Subchapter II of the E-Government Act, entitled the Federal Information Security Modernization Act of 2014 (FISMA) section 3551, 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. The Office of Management and Budget (OMB) Circular A-130, Appendix III Security of Federal Automated Information Resources, defines adequate security as security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

   c. USDA DR 3140-001, USDA Information Systems Security Policy, defines adequate security as security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of, information. This includes ensuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.


5. POLICY

   a. Agencies and staff offices shall comply with this policy and establish additional internal policies if needed.

   b. Agencies and staff offices shall create and maintain procedures to implement this policy.

   c. Agencies and staff offices shall ensure that access to USDA information, IT resources, and systems is limited to those individuals with a need-to-know and based on least privilege access required to perform job functions and approved by system owners.


6. ACCOUNT MANAGEMENT

a. Agencies and staff offices shall establish, maintain, and fully document a user account management process to administer user accounts for all applicable agency and staff office information systems (e.g., mainframes, workstations, servers, databases, electronic mail, authentication, web, proxy, file, domain name systems (DNS), network components, mobile devices, firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors, operating systems, middleware, and applications) developed, maintained, or operated by USDA agencies, staff offices, employees, contractors, and others working for or on behalf of the USDA.

b. Agencies and staff offices shall manage information system accounts, including:

(1) Complying with the requirements for selecting, managing, and deactivating individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service identifiers as specified in the current revision of NIST SP 800-53;

(2) Identifying account types (e.g., individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service);

(3) Establishing conditions for group membership;

(4) Identifying authorized users of the information system and specifying access privileges;

(5) Requiring appropriate approvals for requests to establish accounts;

(6) Establishing, activating, modifying, disabling, and removing accounts;

(7) Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
(8) Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;

(9) Modifying or removing system access when the assignment, job responsibility, or business requirement for access changes or is no longer needed;

(10) Utilizing manual or automated processes to deactivate and delete temporary and emergency accounts that are no longer required, and accounts of terminated or transferred users;

(11) Granting access to systems upon verification of a valid access authorization, identification of intended system usage, and other attributes, as required by the agency or staff office or by associated mission or business requirements;

(12) Reviewing accounts in accordance with current United States Government Configuration Baseline (USGCB) standards;

(13) Identifying authorized users of the information system and the specification of access privileges consistent with the requirements in each system security plan (SSP);

(14) Ensuring users requiring administrative privileges on information system accounts receive additional scrutiny by agency and staff office system owners responsible for approving such accounts and privileged access;

(15) Ensuring that manual or automated mechanisms are employed to support the management of information system accounts;

(16) Ensuring that all account creation, modification, disabling, and termination actions are audited, including audit of the administrative accounts that conduct the actions;

(17) Ensuring that user system activity is recorded in system audit logs;

(18) Reviewing system audit records for indications of inappropriate usage and reporting findings in accordance with DR 3505-005, Cyber Security Incident Management Policy;

(19) Ensuring that account lockout and unlock timing is configured in accordance with the most current USGCB settings;

(20) Ensuring that user privileges and associated access authorizations are administered in accordance with access and functional requirements;

(21) Ensuring that administrator-privileged user accounts are established, tracked, and monitored in accordance with privileged role-based assignments;
(22) Ensuring that accounts enforce adequate separation of duties within the roles of the information system and establish compensating controls when a conflict of separation of duties is identified;

(23) Ensuring that inactive user accounts are suspended or permanently disabled in accordance with the timeframe identified under the most current USGCB recommendations;

(24) Ensuring that user accounts are automatically locked in accordance with the parameters identified under the most current USGCB recommendations for consecutive unsuccessful logon attempts;

(25) Creating, communicating, and enforcing password standards;

(26) Ensuring that password rules shall be adhered to:

(a) Ensure that passwords meet current USGCB settings for general and privileged users (e.g., system administrators, database administrators, security administrators, programmers, auditors, and engineers) for IT devices and servers;

(b) Ensure that password standards are consistent with the most current USGCB settings;

(c) Ensure that dictionary words are not used as passwords;

(d) Ensure that system security software is configured to enforce password history in accordance with current USGCB requirements; and

(e) Ensure that user account password iterations and password aging are set in compliance with current USGCB settings for IT devices and servers;

(27) Ensuring that systems are configured to obscure or mask feedback of authentication information to prevent unauthorized users from ascertaining the information;

(28) Ensuring, upon management approval, that system access be suspended or removed in advance of employee/contractor dismissal when the situation is not amicable;

(29) Ensuring that system access is disabled when a user fails to comply with any USDA requirement for retaining access which includes, but is not limited to:

(a) Timely completion of current annual security awareness training; and

(b) Successful background investigation has not been obtained and verified for the position;
(30) Ensuring that system access is executed using USDA approved methods, technologies, devices, and configurations, including the enforcement of multifactor authentication using either LincPass or AltLinc for USDA employees and contractors, and user enrollment in eAuthentication where applicable;

(31) Ensuring that encryption standards meet FIPS PUB 140-2, Security Requirements for Cryptographic Modules;

(32) Validating and reconciling current access authorizations to ensure they are appropriate and take action when inappropriate activity is detected;

(33) Create and follow agency and staff office standard operating procedures to establish, activate, modify, review, disable, terminate, and remove access accounts;

(34) Implement continuous monitoring processes to log and analyze both authorized and unauthorized access;

(35) Document access management processes, access methods, and approval/denial decisions in a manner that creates evidence of compliance that is available for approved audits, data calls, and continuous monitoring reviews;

(36) Supplement USGCB access standards and enforce additional access control guidance that applies when systems and/or users are physically located outside the United States or its territories;

(37) Control access to media maintained by or on behalf of USDA throughout the media’s lifecycle;

(38) Ensure that media are protected and physical access is controlled during storage and transport;

(39) Label media with appropriate handling caveats, based on the sensitivity of the information;

(40) Ensure that configuration settings enforce object re-use sanitization after logoff or between users;

(41) Sanitize media prior to decommissioning, redeploying, retiring, or disposal to ensure unauthorized users do not obtain access to data stored by the previous user; and

(42) Ensure that when an employee, contractor, volunteer, intern, or partner is terminated, all of their user identifications (IDs) and passwords or other means of accessing files or using computer resources shall be permanently disabled immediately prior to notice of termination.
c. Before a user account can be created, an agency or staff office approved access request form shall be completed, processed, and approved. Each form shall include at least the following:

(1) User first name, middle initial, and last name;

(2) ID;

(3) Description of the action requested;

(4) Description of the access and/or role being requested;

(5) List of information systems the individual is authorized to access and the roles authorized for each system;

(6) Verification of completed computer security awareness and privacy basics training, including date of completion;

(7) Supervisor’s signature and agency or staff office identification;

(8) Information system owner’s signature;

(9) Information Systems Security Officer (ISSO), Information Systems Security Program Manager (ISSPM), or delegated security representative signature;

(10) User’s signature verifying that the user has read and will abide by the system’s security rules; and

(11) Verification of background investigation, including date of completion for the level of clearance required for the position, in accordance with Executive Order 10450, Security Requirements for Government Employment, USDA Personnel and Security Document Division guidelines, and DR 4600-001 USDA Personnel Security Clearance Program.

7. ACCESS MANAGEMENT

The following conditions shall be met prior to obtaining access to systems operated by or on behalf of the USDA:

a. Users shall have a current, successful background investigation in accordance with DR 4600-001;

b. Users shall successfully complete annual training in information security awareness, personally identifiable information (PII), and rules of behavior;
c. Information systems shall enforce approved authorizations (e.g., identity-based, role-based, and attribute-based requirements for logical access to the system in accordance with this policy and the SSP);

d. The USDA mechanisms for two-factor authentication (e.g., access control lists, access control matrices, and cryptography) shall be implemented, documented, approved, maintained, and utilized by agencies and staff offices;

e. The USDA mechanisms for two-factor authentication shall be implemented at the application level to provide increased information security for agencies and staff offices;

f. Access authorization shall be employed and enforced at the information-system level;

g. Audited and explicit override of automated mechanisms in the event of emergencies or other serious events shall be implemented for all information systems owned or operated by or on behalf of USDA;

h. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used shall meet FIPS PUB 140-2 requirements;

i. The information system shall enforce multifactor authentication, in accordance with HSPD-12, FIPS PUB 201-2, and NIST SP 800-53 requirements and all applicable USDA policies;

j. The SSP shall outline discretionary access control (DAC), role based access control (RBAC), and mandatory access control (MAC), such that it:

(1) Allows users to specify and control sharing by named individuals or groups of individuals, or by both;

(2) Includes or excludes access to the granularity of a single user;

(3) Limits propagation of access rights;

(4) Establishes, uses, and monitors USDA departmentally sanctioned accounts for user, elevated privilege, and web services access; and

k. Individuals granted access to USDA information systems must first complete the USDA process mandated by HSPD-12 in accordance with applicable guidance, such as that set forth in OMB M-05-24, FIPS PUB 201-2, and DR 3640-001.
8. INFORMATION FLOW ENFORCEMENT

Information systems shall be configured to:

a. Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with NIST SP 800-53, NIST SP 800-100, NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, and USDA guidance, and the Oversight and Compliance Division standard operating procedure *OCD-SOP-004*, *USDA Six Step Risk Management Framework (RMF Process Guide)*;

b. Enforce information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions as applicable;

c. Enforce dynamic information flow control based on security policy that allows or disallows information flows based on changing conditions or operational considerations;

d. Prevent encrypted data from bypassing content-checking mechanisms;

e. Enforce configuration setting defined limitations on the embedding of data types within other data types, in accordance with NIST SP800-53;

f. Enforce information flow control on metadata;

g. Enforce one way data flow using hardware mechanisms as defined in the SSP;

h. Ensure that information flow control between systems is performed utilizing appropriate enforcement mechanisms (e.g., firewalls, gateways, proxies);

i. Enforce information flow control using security policy filters as a basis for flow control decisions, as defined in the SSP;

j. Enforce the use of human review when the system is not capable of making an information flow control decision, as defined in the SSP;

k. Provide the capability for a privileged administrator to enable/disable security policy filters, as needed once approved by the system owner;

l. Provide the capability for a privileged administrator to configure security policy filters to support different security policies as needed once approved by the system owner and change configuration board, as defined by the SSP;

m. Decompose information into policy-relevant subcomponents for submissions to policy enforcement mechanisms when transferring information between different security domains;
n. Implement policy filters that constrain data structure and content when transferring information between different security domains;

o. Automatically detect unsanctioned information and prohibit the transfer of such information when transferring information between different security domains, in accordance with the SSP, memorandum of understanding/agreement (MOU/A) or interconnection security agreement as outlined in **DM 3565-001, Annual Security Plans for Information Technology (IT) Systems**, the **RMF Process Guide**; and

p. Enforce security policies regarding information on interconnected systems to:

   (1) Uniquely identify and authenticate source and destination domains for information transfer;

   (2) Bind security attributes to information to facilitate information flow policy enforcement; and

   (3) Identify and track problems associated with the security attribute binding and information transfer.

9. SEPARATION OF DUTIES

a. Agencies and staff offices shall ensure the separation of duties of individuals as outlined in NIST SP 800-53 for all systems categorized as moderate or high under **FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems**;

b. Agencies and staff offices shall document separation of duties in each SSP;

c. Agencies and staff offices shall ensure separation of duties through assigned information system access authorizations; and

d. Agencies and staff offices shall separate duties of individuals assigned mission functions (e.g., system management, system programming, configuration management, quality assurance and testing, network security), as necessary, to prevent malevolent activity without collusion.

10. LEAST PRIVILEGE

a. Agencies and staff offices shall use the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
b. Agencies and staff offices shall explicitly authorize access to security functions deployed in hardware, software, firmware, and security relevant information for any system categorized as moderate or high under FIPS PUB 199.

c. Agencies and staff offices shall ensure that only privileged user accounts or roles are used to perform functions that require elevated privileges.

d. Agencies and staff offices shall audit use of privileged accounts or roles for all change activities made to USDA, agency, and staff office networks and systems.

e. Network access to privileged commands shall be used only for operational needs.

f. Agencies and staff offices shall limit authorization to privileged user accounts on the information system to designated system administration personnel.

11. UNSUCCESSFUL LOGIN ATTEMPTS

a. Agencies and staff offices shall enforce USGCB settings for account lockout after consecutive invalid login attempts by a user, and document the defined settings in the SSP.

b. When the maximum number of unsuccessful attempts is exceeded, the network, system, or applicable mobile devices shall be configured to automatically lock the account/node in accordance with the USGCB timeframe settings; the network/system lock shall remain in place until released by an administrator or when the USGCB defined timeframe has been reached. The control applies regardless of whether the login occurs via a local or remote network connection.

12. SYSTEM USE NOTIFICATION

a. A USDA approved notification banner shall be displayed before granting access to information systems owned or operated on behalf of USDA that provide privacy and security notices consistent with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance (e.g., OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 and the Privacy Act of 1974, 5 United States Code (U.S.C.) § 552a) and state:

"You are accessing a government information system; this system contains data belonging to the U.S. Government. This computer system, including all related equipment, networks, and network devices, and internet are provided only for authorized U.S. Government use. U.S. Government computer systems shall be monitored to ensure the availability, integrity, and confidentiality of its systems and information, to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational
security. Monitoring includes active attacks by authorized U.S. Government entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, subject to audit, and used for authorized purposes. All information, including personal information, placed or sent over this system is subject to monitoring.

Use of this computer system, authorized or unauthorized, constitutes consent to monitoring, recording of all activity. Unauthorized use is prohibited and may subject you to disciplinary actions, criminal prosecution, or civil penalties. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Use of this system implies understanding of these terms and conditions.”

b. The notification banner shall remain on the screen until users take explicit action to log on; refusal to accept terms outlined in the banner will mean denial of access to the USDA network and systems and termination of employment, unless system access is not a condition of employment.

c. For publicly accessible systems, the notification banner shall also:

(1) Display the system use information when appropriate, before granting further access;

(2) Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

(3) Include in the notice given to public users of the information system a description of the authorized uses of the system.

13. CONCURRENT SESSION CONTROL

a. USDA prohibits the establishment of concurrent local area network, wide area network, and virtual private network (VPN) connections and/or dual connects/split tunneling; and

b. Wireless capability shall be disabled on all agency or staff office laptop computers when connected to a wired network.

14. SESSION LOCK

a. Information systems categorized as moderate or high under FIPS PUB 199 shall prevent further access to the system by initiating a session lock in accordance with USGCB defined settings for system inactivity or upon receiving a request from a user; and
b. Information systems shall be configured to maintain session lock until the user reestablishes access using USDA established identification and authentication procedures.

15. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

a. The organization shall identify specific user actions that can be performed on the information system without identification or authorization; and

b. Provide documentation including supporting rationale in the SSP for the information system for user action not requiring identification and authentication.

16. REMOTE ACCESS

a. All of the provisions of this policy apply to remote access. Additionally, when agencies and staff offices authorize remote access, the remote access must be documented in their SSP and include, but not be limited to:

   (1) Compliance with applicable USGCB access standards;

   (2) Tools and devices for connectivity, including VPNs;

   (3) Control and management via a limited number of ports;

   (4) Multi-Factor Authentication as required by OMB 06-16; and

   (5) Encryption methodology and tools that meet FIPS 140-2, and other federal standards.

b. Agencies and staff offices shall document the allowed methods of remote access to the network and information systems in the SSP;

c. Agencies and staff offices shall disable networking protocols deemed to be unsecured except for explicitly identified components in support of specific operational requirements;

d. Agencies and staff offices shall protect information about remote access mechanisms from unauthorized use and disclosure;

e. Agencies and staff offices shall establish usage restrictions and implementation guidance for each allowed remote access method and document in the SSP;
f. Agencies and staff offices shall employ automated mechanisms to facilitate continuous monitoring and control of remote access methods and unauthorized access to the information system; and

g. Authorization of remote access to information systems shall be documented prior to connection in accordance with this policy.

17. WIRELESS ACCESS

In accordance with DR 3505-002, Wireless Networking Security Policy, agencies and staff offices shall:

a. Establish usage restrictions and implementation guidance for wireless access;

b. Disable wireless capability on any USDA laptop when it is connected to a wired network or when not intended for wireless use;

c. Prevent users from independently configuring wireless networking capability;

d. Confine wireless communications to controlled network boundaries;

e. Monitor for unauthorized wireless access on USDA networks and information systems;

f. Protect wireless access to the information system using approved authentication and encryption technologies;

g. Ensure wireless access to the network or information system is authorized prior to connection; and

h. Document the requirements for wireless connections in the SSP and enforce those requirements as documented for wireless connections to the network or information system.

18. MOBILE DEVICES

a. Usage restrictions and implementation of this policy for agency and staff office-controlled government furnished mobile computing devices shall be established in accordance with DR 3580-003, Mobile Computing and DM 3300-005, Policies for Planning and Managing Wireless Technologies in USDA;

b. Access to government furnished mobile computing devices shall be explicitly authorized and usage restrictions documented in agency and staff office procedures;
c. Monitoring and reporting of unauthorized connections to government furnished mobile
devices to USDA networks and information systems shall be in accordance with DR
3505-005;

d. Requirements for the connection of mobile devices to USDA, agency, and staff office
networks and information systems shall be enforced;

e. Information system functionality that provides the capability for automatic execution of
code on mobile devices shall be disabled without user direction; and

f. Use of government owned mobile devices while on international travel shall meet the
requirements outlined in DR 3580-003.

19. USE OF INTERNAL/EXTERNAL DATA AND INFORMATION SHARING

External information systems are information systems or components of information systems
that are outside the authorized boundary established by the USDA, agencies, and staff offices
where there is no direct supervision and authority over the application of required security
controls or the assessment of security control effectiveness.

a. Agencies and staff offices shall document, in an MOU/A, the terms and conditions for
sharing external data and information resources, the purpose of the interconnection,
identify relevant authorities, specify the responsibilities of each organization, define the
apportionment of costs, and identify the timeline for terminating or reauthorizing the
interconnection in accordance with NIST SP 800-100, NIST SP 800-53, NIST SP 800-47,
and the RMF Process Guide;

b. Agencies and Staff offices shall document the technical and security requirements for
establishing, operating, and maintaining interconnections, describe the security controls
that will be used to protect systems and data, and maintain a topological drawing of the
interconnection;

c. Agencies and staff offices shall only permit authorized individuals to use an external
information system to access the information system or to process, store, or transmit
organization-controlled information when:

(1) Implementation of required security controls on the external system as specified by
information security policy can be verified; or

(2) Approved information system connection or processing agreements with the hosting
entity have been established; and

d. Use of agency and staff office-controlled portable storage media on external information
systems shall be limited to authorized individuals only.
20. PUBLICLY ACCESSIBLE CONTENT

Agencies and staff offices shall:

a. Designate individuals authorized to post information onto agency and staff office information systems that are publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain non-public information;

c. Review the proposed content of publicly accessible information for non-public information prior to posting onto an agency or staff office information system;

d. Review monthly the content on publicly accessible agency and staff office information systems for non-public information; and

e. Remove non-public information from the publicly accessible agency and staff office information systems when discovered and maintain a log of information removed.

21. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) shall:

   (1) Provide leadership, authority, logistics, and oversight to ensure the information security program access control activities are implemented throughout the USDA; and

   (2) Provide the resources necessary to carry out assigned security duties.

b. The USDA Chief Information Security Officer (CISO) shall:

   (1) Perform information security duties as their primary duty;

   (2) Ensure the integration of FISMA, OMB, executive orders, NIST, and other applicable laws and regulations into the USDA information security program;

   (3) Ensure allocation of resources to operate and maintain the USDA information security program in accordance with federal information security requirements;

   (4) Ensure the USDA information security program is assessing risk and the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency or staff office;
(5) Ensure the USDA information security program develops, integrates, and maintains risk-based, cost-effective information security policies, procedures, and control techniques to address all applicable requirements;

(6) Ensure the USDA information security program has a process in place for the development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;

(7) Ensure compliance oversight of agency and staff office personnel, including contractors, to ensure they receive appropriate information security awareness training;

(8) Ensure compliance oversight to ensure that personnel with significant responsibilities for information security complete role-based training with respect to their security related responsibilities;

(9) Ensure the USDA information security program has a process in place to periodically test and evaluate the effectiveness of this policy;

(10) Provide oversight of USDA agencies and staff offices to ensure implementation of this policy;

(11) Monitor waivers to this policy and render decisions as necessary;

(12) Provide oversight and guidance to agencies and staff offices in implementing secure access controls for USDA systems;

(13) Collaborate with agencies and staff offices to provide training needed to effectively implement this policy; and

(14) Ensure compliance with this policy.

c. Agency and Staff Office CIOs shall:

(1) Establish internal policies, procedures, guidance, processes, and checklists, as appropriate, and assign responsibilities to support and implement this policy;

(2) Ensure staff is assigned, authorized, and appropriately trained to carry out the actions necessary for compliance with this policy;

(3) Ensure the resources needed to maintain secure local and remote access capability are included in agency and staff office IT budgets;

(4) Ensure system access is terminated or restricted based on the current risk or threat environments as needed to protect IT assets, especially from new or imminent threats;
d. Agency and Staff Office ISSPMs shall:

(1) Oversee compliance with this policy;

(2) Provide guidance on the implementation of policies, procedures, guidance, processes, and checklists developed to comply with this policy;

(3) Ensure access control requirements are documented and submitted to the office of the USDA CISO for inclusion in Departmentwide compliance reporting as needed;

(4) Ensure that staff involved with access control have been appropriately trained and authorized;

(5) Ensure compliance with USGCB;

(6) Recommend specific agency and staff office access control standards including methods, technology, devices, configurations, and tools in the absence of, or to augment USGCB access control standards and to support business needs;

(7) Implement and ensure compliance with agency and staff office access control standards as approved by the agency or staff office CIO;

(8) Review internal agency and staff office policy waiver requests and make recommendations to the appropriate signoff authority; and

(9) Facilitate development and completion of Departmental and agency waiver requests.

e. Agency and Staff Office ISSOs shall:

(1) Ensure system compliance with USGCB access control standards and their respective agency or staff office access control standards;

(2) Assist system owners with implementation of access control activities; and

(3) Ensure system compensating security controls are effective and removed when no longer needed, in accordance with DR 3565-003, Plan of Action and Milestones Policy.
f. Agency and staff office business owners, system owners, stewards, and persons who have been delegated authority to perform access control activities on their behalf, shall:

(1) Exercise DAC, RBAC, and MAC;

(2) Ensure access control tailoring, compensating security controls, and compliance are accurately documented in each system assessment and authorization package;

(3) Continuously monitor the effectiveness of access controls, compensating security controls, processes, and procedures to identify, mitigate, and/or eliminate vulnerabilities as needed;

(4) Document and submit to the USDA CISO any deviations from USGCB settings for desktops and servers, including the plan of action and milestone (POA&M) number(s) created in accordance with USDA requirements for tracking non-compliance with security requirements;

(5) Ensure that staff involved with access control have been appropriately trained and authorized;

(6) Pre-approve, authorize, monitor, suspend, and revoke user access to systems and assets over which they have authority;

(7) Apply the security concepts of need-to-know, least privilege, and separation of duties when creating or modifying user account accesses:

(8) Ensure that privileged accounts are associated with a specific user unless a shared account is required and authorized in writing and that auditing is enabled for all account activity; and

(9) Ensure that privileged users do not change or inactivate audit settings of privileged user accounts and that privileged users acknowledge this requirement in writing.

g. Agency and staff office managers and contracting officer representatives shall:

(1) Request new, modified, or terminated access for personnel, systems, and processes over which they have authority, as needed; and

(2) Apply the security concepts of need-to-know, least privilege, and separation of duties when creating or modifying user account accesses.

h. Agency and staff office system and network administrators shall:

(1) Implement access controls, in accordance with this policy, for the systems they support;
(2) Monitor the effectiveness of access controls, take corrective action when appropriate, and submit monitoring reports as required;

(3) Evaluate security features within their systems and recommend changes to improve security controls when applicable;

(4) Review system audit records for indications of inappropriate usage and report findings to designated agency and staff offices officials, as specified in internal procedures; and

(5) Generate and archive documentation upon request or as established in procedure to provide evidence of compliance with this policy.

i. Federal and non-federal USDA users shall:

(1) Have a current, successful background investigation in accordance with DR 4600-001;

(2) Complete and pass annual training in information security awareness, PII, and rules of behavior in order to maintain their system accesses;

(3) Complete annual role-based training specific to their duties, if designated as having significant security responsibilities;

(4) Review DR 4070-735-001, Employee Responsibilities and Conduct annually;

(5) Stay current with USDA access control policies, procedures, and standards;

(6) Notify their supervisor if an access control vulnerability or policy violation is discovered or suspected;

(7) Report any suspicious or unusual activity that could adversely affect access control for any USDA IT asset to their supervisor as soon as possible; and

(8) Ensure remote network access is conducted securely and in compliance with applicable USDA, agency, and staff office guidance.

22. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DM 3300-005, Policies for Planning and Managing Wireless Technologies in USDA, Chapter 3, sets forth USDA’s policies and standards on employee responsibilities and conduct relative to the use of wireless technologies.

DR 4070-735-001, 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, with further delineation provided in DR 3300-001, *Telecommunications & Internet Services and Use*, Section 3.

DR 4070-735-001, 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.

In addition, disciplinary or adverse action shall also be effected in accordance with other applicable laws and regulations, such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, OMB regulations, and Standards of Conduct for Federal Employees.

23. POLICY EXCEPTIONS

a. All USDA agencies and staff offices are required to conform to this policy. However, in the event that a specific policy requirement cannot be met as explicitly stated, agencies and staff offices may submit a waiver request. The waiver request shall explain the reason for the request, identify compensating security controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the policy requirement. Agencies and staff offices shall address all policy waiver request memoranda to the USDA CISO and submit the request to asoc.outreach@asoc.usda.gov for review and determination.

b. Unless otherwise specified, agencies and staff offices shall review and renew approved policy waivers every fiscal year. Approved waivers shall be associated with a NIST security control and tracked as a POA&M item in the Department’s FISMA data management and reporting tool.

-END-
DEFINITIONS

a. **Access Control.** The process of granting or denying specific requests to obtain and use information and related information processing services.
(Source: NIST Interagency or Internal Report (IR) 7298 Revision 2)

b. **Alt Link.** The name of the alternative smart card solution that USDA uses to credential short-term employees/non-Federal employees assigned to or associated with the agencies requiring limited access to federally controlled facilities and/or information systems for less than twelve months. This credential is a token that allows both logical and physical access and requires favorable fingerprint adjudication. This alternative solution meets the multifactor authentication required under HSPD-12.
(Source: USDA Office of Homeland Security and Emergency Coordination)

c. **Departmental Manual (DM).** Departmental Manuals are used for detailed, relatively lengthy technical guidance that is procedural in nature and Departmentwide in scope. Manuals generally are written for "specialist" audiences. They provide standards and guidance pertaining to a particular subject or administrative function, generally of the type that must be referred to on a daily or frequent basis. Some manuals implement an external agency directive series with USDA policy and procedural guidance.
(Source: DR 0100-001, Section 4a(2))

d. **Departmental Regulation (DR).** Departmental Regulations promulgate Departmental policy; delegate authority; establish responsibility; establish statutory or interagency committees; and prescribe procedures governing USDA activities and operations. DRs may also include selected material of an administrative nature that is published in the Federal Register or the Code of Federal Regulations.
(Source: DR 0100-001, Section 4a(1))

e. **Discretionary Access Control (DAC).** The basis of this kind of security is that an individual user, or program operating on the user’s behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user’s control.
(Source: NIST IR 7298 Revision 2)

f. **Least Privilege.** The security objective of granting users only those accesses they need to perform their official duties.
(Source: NIST IR 7298 Revision 2)

g. **LincPass.** The USDA branded smart card. The card “links” your personal identity to the card and to your ability to access Federal buildings and computer systems. LincPass meets all FIPS 201 standards, is produced by GSA’s Shared Services, includes USDA’s name and logo, and is used for access by USDA employees and affiliates.
h. **Multifactor Authentication.** An approach to authentication that requires the presentation of two distinct kinds of evidence to authenticate and grant access. The usual kinds of evidence are something known and something possessed.  
(Source: NIST IR 7298 Revision 2)

i. **Mandatory Access Control (MAC).** A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity.  
(Source: NIST IR 7298 Revision 2)

j. **Media.** Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.  
(Source: NIST IS 7298 Revision 2)

k. **Need-to-know.** A method of isolating information resources based on a user’s need to have access to that resource in order to perform their job but no more. The terms “need-to-know” and “least privilege” express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.  
(Source: NIST IR 7298 Revision 2)

l. **Role Based Access Control (RBAC).** A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.  
(Source: NIST IR 7298 Revision 2)

m. **Security Policy Filter.** The information system enforces information flow control using security policy filters as a basis for flow control decisions.  
(Source: NIST SP 800-53)

n. **Session Lock.** A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.  
(Source: NIST SP 800-53)

o. **Separation of Duties.** Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.  
(Source NIST SP 800-53)
p. **Split Tunneling.** A method that routes organization-specific traffic through the SSL VPN tunnel, but routes other traffic through the remote user's default gateway.  
(Source NIST SP 800-113)

q. **United States Government Configuration Baseline (USGCB).** The USGCB provides security configuration baselines for information technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a federal government wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security.  
(Source: NIST IR 7298 Revision 2)
# ACRONYMS AND ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>DM</td>
<td>Departmental Manual</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DR</td>
<td>Departmental Regulation</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Management Act</td>
</tr>
<tr>
<td>GSA</td>
<td>General Services Administration</td>
</tr>
<tr>
<td>HSPD</td>
<td>Homeland Security Presidential Directive</td>
</tr>
<tr>
<td>ID</td>
<td>User Identification</td>
</tr>
<tr>
<td>ISSPM</td>
<td>Information Systems Security Program Manager</td>
</tr>
<tr>
<td>IR</td>
<td>Interagency or Internal Report</td>
</tr>
<tr>
<td>ISSO</td>
<td>Information Systems Security Officer</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>MOU/A</td>
<td>Memorandum of Understanding/Agreement</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OCD</td>
<td>Oversight and Compliance Division</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
</tr>
<tr>
<td>POA&amp;M</td>
<td>Plan of Action and Milestones</td>
</tr>
<tr>
<td>PUB</td>
<td>Publication</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
<tr>
<td>SSP</td>
<td>System Security Plan</td>
</tr>
<tr>
<td>U.S.</td>
<td>United States</td>
</tr>
<tr>
<td>USDA</td>
<td>United States Department of Agriculture</td>
</tr>
<tr>
<td>USGCB</td>
<td>United States Government Configuration Baseline</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
APPENDIX C

AUTHORITIES AND REFERENCES

DM 3300-005, Policies for Planning and Managing Wireless Technologies in USDA, November 10, 2010

DM 3525-003, Telework & Remote Access Security, February 17, 2005

DM 3535-000, C2 Controlled Access Protection, May 11, 2005

DM 3535-001, USDA’s C2 Level of Trust, February 17, 2005

DM 3565-001, Chapter 13, Part 1, Annual Security Plans for Information Technology (IT) Systems, February 17, 2005


DR 0100-001, Departmental Directives System, September 16, 2011

DR 3140-001, USDA Information Systems Security Policy, May 15, 1996

DR 3300-001, Telecommunications & Internet Services and Use, March 23, 1999

DR 3505-002, Wireless Networking Security Policy, August 11, 2009

DR 3505-003, Access Control Policy, August 11, 2009

DR 3505-005, Cyber Security Incident Management Policy, October 31, 2013

DR 3565-003, Plan of Action and Milestones Policy, September 25, 2013

DR 3580-003, Mobile Computing, September 24, 2013

DR 3640-001, Identity, Credential, and Access Management, December 9, 2011

DR 4070-735-001, Employee Responsibilities and Conduct, October 04, 2007

DR 4600-001 USDA Personnel Security Clearance Program, July 02, 2013

DR 4620-002, Common Identification Standard for U.S. Department of Agriculture Employees and Contractors, January 14, 2009

Executive Order 10450, Security Requirements for Government Employment, April 27, 1953

FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 25, 2001

FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006

FIPS PUB 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013

HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

NIST IR 7298, Revision 2, Glossary of Key Information Security Terms, May 2013

NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996


NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Current version


NIST SP 800-113, Guide to SSL VPNs, July 2008

NIST, United States Government Configuration Baseline (USCGB)


OMB M-06-16, Protection of Sensitive Agency Information, June 23, 2006

SEM-33, Alternative Card for Short Term Employee, Interns, Volunteers, and Contractors, April 24, 2014