

PREFACE TO SELECTED INFORMATION DIRECTIVES

CIO Transmittal No.: 15-010	CIO Approval Date: 06/12/2015
-----------------------------	-------------------------------

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005*

CHIEF INFORMATION OFFICER MEMORANDUM

SUBJECT: Chief Technology Officer (CTO) Responsibilities in Selected Information Directives

Re-assigned CTO responsibilities

Effective immediately, CTO responsibilities detailed in the selected information directives (i.e., Information Policies, Procedures, Standards, and Guidance) listed in Appendix A are re-assigned to the OEI Office of Technology, Operations, and Planning (OTOP) Director and the Senior Agency Information Security Officer (SAISO) as detailed. The re-assignment does not change any requirements in the selected information directives.

The OEI Information Directives Program Manager is directed to attach this memorandum and Appendix A as a Preface to each of the Information Directives listed. OEI will then update the Roles and Responsibilities section of each Information Directive in accordance with the normal review and update cycle.



Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2104.1 Software Management and Piracy Policy	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy and manage enterprise software licenses.	OTOP Director
CIO 2104-P-01.0 Software Management and Piracy Procedure	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy, manage enterprise software licenses, and provide covered users within their office with training and awareness on the Software Management and Piracy Policy through the annual Cybersecurity Awareness Training.	OTOP Director
CIO 2121.1 System Life Cycle Management (SLCM) Policy	Establish and publish procedures, technical operational procedures and standards (TOPS), and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2121-P-03.0 SLCM Procedure	Establish and publish procedures, TOPS, and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2122.1 Enterprise Architecture (EA) Policy	Issue procedures, guidance, and technical standards associated with the EA with a specific focus on the technology architecture, chair the Quality Technology Subcommittee (QTS), and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-01.1 EA Governance Procedures	Issue procedures, guidance, and technical standards associated with the EA, with a specific focus on the technology architecture, chair the QTS, and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-03.0 Information Technology Infrastructure Standard Procedure	Recommend to the CIO a specific IT standard, product or specification to be added to the official Agency IT Standards Profile with consultation from the Quality Information Council (QIC) and the QTS, and develop and maintain the Agency's Technology Architecture.	OTOP Director
CIO 2122-S-02.0 Personal Computer Configuration and Management Standard	Review and approve requests for waivers in regard to this standard.	OTOP Director
CIO 2123.1 Configuration Management Policy	Provide procedures, standards, and guidance to senior level managers in support of the Agency's Configuration Management Policy; institute change management processes; and provide a change management database.	OTOP Director

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2150-P-01.1 Information Security - Interim Access Control Procedures	Approve all methods of dial-up access, approve all wireless connections, establish, document, authorize, and monitor all methods of remote access to an information system; delegate to Regions and other entities, as appropriate; and address co-management responsibilities for the Agency Security Architecture.	OTOP Director
CIO 2150-P-08.1 Information Security - Interim Incident Response Procedures	Determine Operational Status Categories during Alerts and Risks (OSCAR) 5 level (page 7).	SAISO
	Be available when the Computer Security Incident Response Capability (CSIRC) must report and coordinate incidents (page 16). Be available to meet with the Director of Cyber Security Staff (CSS) when senior managers are informed of incidents, occurrences and their status (page 18).	OTOP Director
CIO 2150-P-14.1 Information Security - Interim Risk Assessment Procedures	Approve the use of and, as appropriate, acquire and deploy enterprise vulnerability management technology. Consult with the SAISO to determine the coverage and compliance of enterprise vulnerability management technology with respect to federal and Agency requirements, including use of these tools to meet assessment requirements of other control families in NIST 800-53A, Revision 1, and to ensure the most cost effective, complete and accurate results.	OTOP Director
CIO 2150-P-15.1 Information Security - Interim System Services Acquisition Procedures	For the procurement of external information system services where a sufficient level of trust cannot be established, be available to confer regarding risks associated with the network and the Agency.	OTOP Director
CIO 2150-P-16.1 Information Security - Interim System and Communications Protection Procedures	Approve use of mobile VoIP-enabled units.	OTOP Director
CIO 2150.4 Mobile Computing Policy	Oversee policy and procedure implementation regarding use of mobile computing technologies. Approve mobile computing technology and device deployment.	OTOP Director
CIO 2150-P-01.1 Mobile Computing Management Procedures	Oversee policy and the implementation of the procedures. Approve enterprise mobile device types to be deployed. Review and approve requests for waivers in regards to the procedures.	OTOP Director

EPA Classification No.:	CIO-2150.3-P-01.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005*

**INFORMATION SECURITY –
INTERIM ACCESS CONTROL PROCEDURES
V3.2
JULY 13, 2012**

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Access Control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

These procedures cover all EPA information and information systems to include those used, managed, or operated by a contractor, another agency, or other organization on behalf of the agency.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all offices within the Agency meet the minimum security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems. All EPA information systems must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the family of access controls found in NIST SP 800-53, Revision 3.

5. AUTHORITY

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- E-Government Act of 2002, Public Law 107-347, Title III, *Federal Information Security Management Act (FISMA)* as amended
 - Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
 - Clinger-Cohen Act of 1996, Public Law 104-106
 - Paperwork Reduction Act of 1995 (44 USC 3501-3519)
 - Privacy Act of 1974 (5 USC § 552a) as amended
 - USA PATRIOT Act (P.L. 107-56), October 2001
 - Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—*Employees Responsible for the Management or Use of Federal Computer Systems*, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
 - Office of Management and Budget (OMB) Memorandum M-05-24, Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004
 - OMB Memorandum M-06-16, “*Protection of Sensitive Agency Information*,” June 2006
 - OMB Memorandum M-07-11, “*Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*,” March 2007
 - OMB Memorandum M-08-05, “*Implementation of Trusted Internet Connections (TIC)*,” November 2007
 - OMB Memorandum M-08-22, “*Guidance on the Federal Desktop Core Configuration (FDCC)*,” August 2008
 - OMB Memorandum M-08-27, “*Guidance for Trusted Internet Connection (TIC) Compliance*,” September 2008
 - OMB Memorandum M-09-32, “*Update on the Trusted Internet Connections Initiative*,” September 2009
 - Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001
 - FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
 - FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
 - FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006
 - EPA Information Security Program Plan
 - EPA Information Security Policy
-

6. PROCEDURES

AC-2 – Account Management

- a. Information system accounts must be managed through a life cycle consisting of
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

establishing, activating, and modifying accounts; periodically reviewing accounts; and disabling, removing or terminating accounts.

- i. NIST SP 800-66, Revision 1 must be utilized as guidance on account management when protected health information is involved.
- ii. NIST SP 800-43 and NIST SP 800-68, Revision 1 must be utilized as guidance on account management for Windows-based operating systems.

Note: Refer to the definition of account management in Section 9 of this document.

- b. The following must be adhered to regarding establishing and activating accounts:
 - i. Granting access to the information system must be based on:
 - A valid access authorization.
 - Intended system usage.
 - Other attributes as required by the organization or associated missions/business functions.
 - ii. Access requirements must be identified for newly assigned personnel or transfers, as well as defining required levels of access for each system and/or application, prior to providing access.
 - iii. Each user must be assigned only the minimum access privileges he or she requires.
 - iv. Normal system or application users must not be granted access rights to administration or security functions of the system.
 - v. Authorized users of the information system must be identified and their access rights/privileges must be specified.
 - vi. An individual who requests an information system account must adhere to the following requirements prior to assuming responsibility for the account or new access permissions:
 - Proper identification must be supplied.
 - Rules of Behavior must be read and acknowledged in writing.
 - Completed access request forms must include a signature (handwritten or digital) of the account recipient's acceptance of responsibility for the account.
 - vii. Requests to establish information system accounts must be approved.
 - Approval of requests to establish information system accounts must be in writing.
 - Access requests must be approved by all applicable information system managers.
 - Email administrators shall request and authorize access to the email system for users in their areas of responsibility.
 - viii. Processing of requests to access an information system and create accounts must adhere to the following:
-

EPA Classification No.:	CIO-2150.3-P-01.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

- Access requests must be processed only when initiated via written request from the user's management since they have adequate knowledge regarding the users' legitimate need to access/modify data.
 - The written or email request must provide the user's name and explicitly detail the access privileges requested.
 - User account request documentation must be completed in full prior to account creation.
 - If the request is received via email, the request must be verbally confirmed with the requester prior to granting access privileges, and the email must be printed and annotated with the date and time of the verbal verification.
 - Creation of user accounts or assignment of access privileges without the approved written or verified email request is forbidden.
- ix. Processing of requests for privileged access to an information system must include additional scrutiny such as:
- Higher level of background checks.
 - Higher level of management approval.
- x. Before receiving access to the system, the individual requesting access must complete the required security training.
- Refer to *Information Security – Awareness and Training Procedures* for requirements on security training.
- xi. User accounts should remain active until the individual is transferred or their employment is terminated.
- xii. All access request forms must be maintained while the account remains active and in accordance with EPA Records Schedule 129 on account terminations.
- xiii. Individual users may become members of a group provided that:
- Group membership is approved in writing from management.
 - Group membership preserves the user's need-to-know/need-to-share least privilege.
- c. The following must be adhered to regarding modifying accounts:
- i. Account management must be notified when a user's information system usage or need-to-know/need-to-share changes.
 - ii. Information system management must be notified of all access changes for their users (e.g., information system usage, privileges, or need-to-know/need-to-share changes, etc.).
 - iii. Requests to modify information system accounts must be documented in writing.
 - iv. Requests to modify information system accounts must be approved.
 - Approval of requests to modify information system accounts must be in writing.
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- Requests must be approved by all applicable information system managers.
- d. The activities of users must be supervised and reviewed with respect to the enforcement and usage of information system access controls.
 - i. The information system owner shall ensure that all information system access is consistent with defined, documented, and approved user access requirements, roles and responsibilities, and account privileges.
 - ii. System access must be reviewed at least every 30 days to ensure that:
 - Only the appropriate levels of access are allowed.
 - Access is granted to only authorized personnel.
 - Users' access rights are limited to least privilege.
 - iii. The activities of users with significant information system roles and responsibilities must be reviewed more frequently than regular system users.
 - iv. Access controls must be reviewed every 30 days for the following:
 - Access lists must be up-to-date (e.g., access rights are removed for terminated and transferred employees and contractors).
 - Access control mechanisms must be tested to ensure that they cannot be bypassed.
 - The level of access provided to each individual must be limited to the level required to complete his/her job responsibilities.
 - v. Information managers shall review system accounts every 30 days to identify and delete accounts that have been inactive for 180 days or more.
 - Refer to *Information Security – Identification and Authentication Procedures* for requirements on deleting inactive identifiers.
- e. The following must be adhered to regarding deactivating accounts (i.e., disabling, terminating, removing, or transferring accounts):
 - i. Account management must be notified when information system users are terminated or transferred.
 - Terminations may be friendly or unfriendly.
 - The AO or designated representative shall review and approve any individual requiring administrator privileges.

Note: Refer to definitions of friendly and unfriendly terminations in Section 9 of this document.

- ii. When a user's official association with EPA or authorization to access EPA information systems is terminated, all accounts associated with that user must be disabled immediately. These include network access, email access, etc.
 - iii. In other cases, accounts must be disabled after a maximum of 180 days of user inactivity.
 - iv. When an account is disabled, all official records must be appropriately
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

accounted for before the account is removed.

- v. When accounts are transferred, unneeded authorizations must be removed and any official records must be appropriately accounted for.
 - vi. The following activities must be performed whenever an individual (EPA employees, contractors, grantees, etc.) terminates employment, transfers jobs, or takes an extended leave of absence (i.e., 180 days):
 - Change or cancel all passwords, codes, and locks.
 - Disable all accounts and user IDs.
 - Update access control lists, mailing lists, etc.
 - Collect all keys, badges, and similar items.
 - Reconcile any financial accounts over which the individual had control.
 - Ensure electronic records are accessible and properly secured, or appropriately disposed of.
 - In the event an individual must be removed or laid off or under unfriendly termination, the above actions must be completed immediately. In addition, the user should be rotated to a non-sensitive position, if possible, before the employee is notified that he or she will be terminated. While this may seem extreme, angry and demoralized employees have been known to sabotage programs, erase databases, and plant malicious software or “back-doors” to information systems.
 - Ensure that these procedures have been accomplished in accordance with applicable personnel, contractual, and grant mechanisms.
 - Refer to *Information Security – Personnel Security Procedures* for requirements on personnel termination and transfer.
 - vii. User accounts must be disabled when a user has not completed required initial awareness training or specialized training.
 - viii. Access may be revoked if the Rules of Behavior, EPA information security policies, or applicable laws are violated. Other action, up to and including termination of EPA employment, may also be taken, depending on the particular violation.
 - f. All special accounts must be authorized and approved by the information system manager; monitored while in use; and removed, disabled, or otherwise secured when not in use. Special accounts include guest, training anonymous maintenance or temporary emergency accounts.
 - i. Maintenance accounts must be rendered inactive immediately after the maintenance task is completed.
 - ii. Training accounts must be rendered inactive immediately after the training is completed.
 - Training accounts must be rendered inactive (e.g., by resetting the password) at the end of the training event.
 - If multiple classes are held during a given day, the account may
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

remain active at the end of the day, rather than resetting the accounts between classes held on the same day.

iii. Temporary and emergency accounts must automatically:

- Terminate within five (5) days after the need is fulfilled; or
- Disable within five (5) days if additional actions are required, such as preserving records, or if additional access is authorized at a future date.

- g. If disabling accounts (i.e., temporary, emergency, anonymous, guest) is not possible, then such accounts must be locked.
- h. The information system must automatically disable inactive accounts after a maximum of 180 days of inactivity, and alert the necessary personnel of such an event.
- i. The information system must be configured to automatically audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

AC-3 – Access Enforcement

- a. The information system must enforce assigned authorizations for logical access to the system in accordance with applicable policy.
 - i. FIPS 201-1 and NIST SP 800-12, 800-19, 800-66, Revision 1, 800-68, Revision 1, 800-73-3, 800-76-1, 800-78-2, 800-87, Revision 1, 800-95, 800-96, and 800-98 must be utilized as guidance for access enforcement.
- b. Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) must be employed to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.
- c. Access enforcement mechanisms must be employed at system and application levels, when applicable, to provide increased information security.
- d. In the event of emergencies or other serious events, consideration must be given to implementing an audited, explicit override of automated mechanisms.
- e. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used must be in accordance with federal standards and NIST validation requirements.
- f. For MOD and HGH systems and require keeping privileged and service account credentials stored offline in a protected container/location with backup media.
- g. Controls shall be implemented to ensure that only authorized individuals are able to participate in throughout any video teleconference.

Note: For classified information, the cryptography used is largely dependent on the classification level of the information and the clearance of the individuals having access to the information.

- h. EPA must ensure that all information system access is consistent with defined,
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

documented, and approved user access requirements, roles and responsibilities, and account privileges by:

- i. Limiting the level of access provided to each individual to the level required to complete his/her job responsibilities.
 - Physical, procedural, and/or technical measures must be provided that allow the identification and authentication of individual users and prevent access by unauthorized persons.
- ii. Restricting the functional capabilities of individual users by implementing physical, procedural, and technical measures.
 - Individual users should still have the capability to manage access (e.g., create, read, modify, or delete) by other users to their information and applications.
- iii. Ensuring that the information system prevents anyone but authorized security administrators from accessing the information system's security related functions.
 - A method of enforcement includes, but is not limited to, configuring workstations with basic input/output system (BIOS) passwords or similar restriction capabilities to prevent unauthorized access. Desktop hardware must have BIOS passwords or similar capabilities to prevent unauthorized access.

AC-4 – Information Flow Enforcement

For moderate and high information systems

- a. EPA shall document all interconnections between external networks with an Interconnection Security Agreement (ISA).
 - i. NIST SP 800-47 must be used as guidance for developing interconnection agreements.
 - ii. Internal EPA interconnections of information systems do not require ISAs.
- b. The information system must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with the *Information Security – Access Control Policy*.
 - i. NIST SP 800-41, Revision 1, and 800-82 must be used as guidance on information flow enforcement.

Note: Refer to the definition of information flow control in Section 9 of this document.

- c. Information flow control policies and enforcement mechanisms must be employed to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems.
 - d. EPA shall utilize either protected processing domains (e.g., domain type-enforcement) or dynamic security policy mechanisms as a basis for flow control decisions.
 - i. The selection of domain-type enforcement versus dynamic security policy
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

mechanisms must follow the requirements in the Agency's architecture.

- ii. The selection must be approved.
 - Because different EPA organizations require unique levels of access to external resources (and vice versa), the Agency enterprise networks must, at a minimum, be divided into several distinct security zones (e.g., public access, extranet, and intranet).
 - Each of these zones has a different level of exposure to external threats.
 - Consequently, access into each zone must employ appropriate network security controls to maintain an overall level of information security.
- e. Information flow enforcement must be based on documented characteristics of the information and/or the information path.
- f. Information flow must be enforced through authorized mechanisms (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ documented and managed rule sets or through established configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics).
 - i. Refer to *Information Security – System and Communications Protection Procedures* for requirements on boundary protection, public access protection, denial of service protection, etc.

AC-5 – Separation of Duties

For moderate and high information systems

- a. Separation of duties must be:
 - i. Implemented on all systems through assigned information system access authorizations.
 - ii. Documented.
 - b. Duties of individuals must be separated as necessary, to prevent malevolent activity without collusion.
 - c. Duties performed by employees must be reviewed to ensure separation of duties and verify that users only have the system privileges that are needed to perform their assigned duties (least privilege).
 - d. A single individual shall not perform combinations of functions that could result in a conflict of interest, fraud or abuse.
 - i. Separation of duties is mandatory for all financial applications where misuse could cause a direct financial loss. Examples include but are not limited to:
 - Check issuance
 - Funds transfer
 - Input of vendor invoices
 - Other purchasing information
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- Receiving information
 - e. At a minimum, the following functions and sub-functions within the Agency must be assigned to different individuals:
 - i. Data Creation and Control Functions
 - Data collection and preparation.
 - Data entry – However, input of transactions that may result in a conflict of interest, fraud, or abuse (e.g., input of vendor invoices and purchasing and receiving information) shall be separated.
 - Data verification, reconciliation of output, and approval.
 - Data base administration.
 - ii. Software Development and Maintenance Functions
 - Applications programming
 - Design review
 - Application testing and evaluation
 - Application maintenance
 - iii. Security Functions
 - Security implementation
 - Review of security controls, security audits and audit trail review
 - iv. Some additional examples of this principle include the following:
 - The same individual shall not enter and authorize a purchase order.
 - The same individual shall not request a user account and also create the account in the system.
 - A system administrator shall not be the one to conduct the audits/reviews of the system he/she is administering.
 - The Information Security Officer (ISO) or Information System Security Officer (ISSO) shall not be a system administrator.
 - A Database Administrator (DBA) shall have the minimum level of operating system rights necessary to create, edit, and delete rights over the database-specific files in the SYSTEM directory, but no directory level rights in the SYSTEM directory. (Note: The DBA shall have all rights over the Database Management System [DBMS] directory and its subdirectories.)
 - f. Security personnel shall help ensure that separation of duties issues are identified and appropriate actions taken to correct any conflicts.
 - i. This type of control shall ensure that a single individual cannot subvert a critical process.
 - g. NIST SP 800-66, Revision 1 and 800-98 must be utilized as guidance on separation of duties.
 - h. Refer to AC-3 for requirements on the implementation of access authorizations defined in this control.
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

AC-6 – Least Privilege

For moderate and high information systems

- a. The concept of least privilege must be employed, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- b. Information systems of any impact level, it is recommended that users do not have access to security settings and logging/auditing facilities to ensure the integrity of an audit trail for actions taken within the information system
- c. The concept of least privilege must be employed for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to Agency operations and assets, individuals, other organizations, and the Nation.
 - i. Users are granted only the access rights to the directories and file structures needed to perform their job function and associated authorized duties.
- d. Access to EPA's defined list of security functions (hardware, software, and firmware) and security-relevant information must be explicitly authorized.
- e. Administrator accounts shall be used only for performing required administrator duties. All other functions not directly tied to administrator duties shall be performed through individual regular user accounts.

Note: Examples of security functions are establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters)

Note: Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

- f. Users of information system accounts, or roles, with access to EPA's defined list of security functions or security-relevant information must use non-privileged accounts, or roles, when accessing other system functions.

Note: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy such as Role Based Access Control (RBAC) is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

- g. If feasible, any use of privileged accounts, or roles, for non-privileged functions should be audited.
 - i. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- h. NIST SP 800-12, 800-19, 800-28 Version 2, 800-66, Revision 1, 800-68, Revision 1, 800-69, 800-81, and 800-83 must be utilized as guidance on least privilege.
- i. Refer to AC-3 for requirements on the implementation of access authorizations defined in this control.
- j. Access should be limited to certain information system accounts typically found in general support systems running Windows and Active Directory, such as Enterprise Administrator and accounts that have the ability to change security policy across an entire directory structure.

AC-7 – Unsuccessful Logon Attempts

Note: This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14 and regardless of whether the login occurs via a local or network connection.

- a. The information system must enforce a limit of five (5) consecutive invalid login attempts by a user during a 15-minute time period.
- b. For privileged and non-privileged accounts, the information system must automatically lock the account and delay the next login prompt for 30-minutes hours when the maximum number of unsuccessful login attempts is exceeded.
 - i. Users should be permitted access to the help desk to release their account prior to the 30 minutes lock out period if it hinders productivity.
- c. If a delay algorithm is selected, different algorithms may be employed for different information system components based on the capabilities of those components.
- d. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels.
- e. NIST SP 800-68, Revision 1 must be utilized as guidance on unsuccessful login attempts.

AC-8 – System Use Notifications

- a. The information system must display an approved, system use notification message or banner before granting system access and states that:
 - i. That the user is accessing a U.S. Government information system.
 - ii. That system usage may be monitored, recorded, and subject to audit.
 - iii. That unauthorized use of the system is prohibited and subject to criminal and civil penalties.
 - iv. That the use of the system indicates consent to monitoring and recording.
 - b. For network security, routing, and monitoring devices, an approved system use notification must be displayed before granting access for all administrative and maintenance access.
 - c. For all non-publicly accessible systems, the system use notification message must provide approved security notices and must remain on the screen until the user takes explicit actions to log on to or further access the information system.
 - d. For publicly accessible systems (i.e., web sites):
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- i. The system use information must be available and when appropriate, displayed before granting access.
 - ii. Any references to monitoring, recording, or auditing must be in keeping with privacy accommodations for such systems that generally prohibit those activities.
 - iii. The notice given to public users of the information system must include a description of the authorized uses of the system.
- e. The system use notification message or banner must provide appropriate privacy and security notices (based on associated privacy and security policies or summaries).
 - i. Privacy and security policies must be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.
 - EPA's Privacy and Security Notice can be located at <http://www.epa.gov/epahome/usenotice2.htm>.
 - ii. A link to EPA's *Privacy and Security Notice* must be published at the top of all Region and Program Office pages.
 - iii. The standard *Children's Privacy Policy* must appear on, or be linked from, all EPA web sites aimed at children age 13 and under.

AC-10 – Concurrent Session Control

For high information systems

Note: This control addresses concurrent sessions for a given information system and does not address concurrent sessions by a single user via multiple system accounts.

- a. The information system must limit the number of concurrent sessions to zero (0) for any user to one session.
 - i. The maximum number of concurrent sessions may be defined for an information system account globally, by account type, by account, or a combination.

AC-11 – Session Lock

For moderate and high information systems

- a. The information system must initiate a session lock:
 - i. After a maximum of 15 minutes of inactivity to prevent further access to the system.
 - ii. Upon receiving a request from a user to prevent further access to the system.
 - b. The session lock must:
 - i. Remain in effect until the user reestablishes access using established identification and authentication procedures.
 - ii. Be implemented at the point where session activity can be determined.
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

iii. Not be used as a substitute for logging out of the information system.

AC-14 – Permitted Actions Without Identification or Authentication

Note: This control is intended for those specific instances where an organization determines that no identification and authentication is required. It is not, however, mandating that such instances exist in given information system. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred.

- a. Specific user actions that can be performed on the information system without identification and authentication must be identified and documented.
 - i. Supporting rationale for the information system user actions not requiring identification and authentication must be provided and documented in the System Security Plan (SSP).
- b. User activity without identification and authentication on public websites or other publicly accessible federal information systems must be limited to accessing only publicly available information.
- c. Access permitted to or on the information system without identification and authentication must be limited to public access.
- d. Special actions to accomplish mission objectives may be permitted without identification and authentication, provided these actions are authorized by management.
 - i. Examples of such special actions are:
 - Intrusion and penetration testing activities.
 - Information system management approved emergency situations.
 - ii. The access must be monitored by an EPA authorized official.
 - iii. The access must be documented in writing with the accessing individuals' name(s), affiliation(s), time(s) of access, resource(s) accessed, and work being performed.
- e. Application-specific user IDs and generic user IDs not requiring passwords, such as those implemented on Value-Added Backbone Services (VABS) servers, must have additional security measures implemented at the directory and file level.
 - i. These User IDs must be given rights to only those directories and files necessary for proper execution of the application.

For moderate and high information systems

- f. Actions that can be performed on the information system without identification and authentication may be permitted only to the extent necessary to accomplish mission/business objectives.

AC-17 – Remote Access

Note: This control requires explicit authorization prior to allowing remote access to an

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control.

- a. All allowed methods of remote access (e.g., dial-up, broadband, wireless, virtual private network (VPN) to an information system must be documented.

Note: A VPN when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network).

- b. Usage restrictions and implementation guidance for each allowed remote access method must be established.
 - c. Remote access must be monitored for unauthorized access.
 - d. Remote access to the information system must be authorized prior to the connection.
 - e. Requirements for the remote connection to the information system must be enforced.
 - f. Remote access controls must be applicable to information systems other than the publicly accessible capabilities of public web servers or systems specifically designed for public access.
 - g. When remote access is required to the information system, the following steps must be considered and documented:
 - i. Identify the type(s) of information to be processed and its availability, integrity, and confidentiality concerns.
 - If information, when shared, can't be provided with the same level of security that it was provided while in its native environment, then the information must not be downloaded to or shared with another computer.
 - ii. Determine which information system(s) will be accessed and the level and type of access required (e.g., access to which applications, files, and utilities).
 - Define the level of access to be allowed based on the job responsibilities of the remote worker.
 - iii. Complete a risk assessment.
 - Identify the threats, vulnerabilities, and necessary safeguards to adequately protect a remote connection to the system and any applications and information.
 - Identify the vulnerabilities of the method in which data will be accessed (i.e., whether or not information will be transferred across the Internet).
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- Include in the assessment the threats and vulnerabilities in the remote environment.
 - iv. Ensure that the rules of behavior specific to remote access requirements have been developed for the remote support system and application.
 - v. Ensure that training and a security awareness program are developed for system and application users in a medium and/or format that is appropriate for the remote environment
 - vi. Ensure that training is provided prior to allowing remote access.
 - Training must cover the risks of the remote connection.
 - vii. Update the general support system and major application (if it will be accessed remotely) SSPs.
 - Ensure the risk assessment results are incorporated into the SSP.
 - h. The following procedures must apply to access to the EPA network via remote connection:
 - i. All access via the Internet must be subject to inspection using centrally managed and operated access control (firewall) and intrusion detection facilities.
 - ii. Traffic to internal EPA resources via the Internet must be implemented using EPA-approved user authentication and encryption methods.
 - iii. Client computers must have implemented adequate security measures (e.g., virus and spam protection, firewall, intrusion detection).
 - iv. Any government agency or corporate network from which a client computer is used to access the EPA network remotely must be subject to review and audit of security and vulnerabilities by EPA or an officially delegated entity after appropriate coordination with all appropriate entities.
 - v. Access to the EPA network is a privilege and must be denied, at EPA's discretion, to clients attached to networks deemed unacceptably vulnerable.
 - vi. Prior to authorizing an agency facility to be established as a point of entry for remote access, either via dial-up or the Internet, adequate reviews or audits must be performed and there must be certification of the security of that facility's network and network-attached resources that is consistent with FISMA requirements.
 - i. Remote access for firewall administration over untrusted networks such as the Internet or via modem is prohibited.
 - i. Firewall administration, whenever possible, must be accomplished directly from the firewall management console.
 - ii. Operational requirements may dictate that some form of remote access for firewall administration is granted.
 - Where remote access must be allowed for firewall administration, it must be accomplished via registered hosts that have been allowed access to a secure virtual local area network (VLAN) which resides on the agency's internal network.
 - This procedure allows the registered host to connect to the firewall
-

EPA Classification No.:	CIO-2150.3-P-01.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

complex using agency-approved authentication and encryption (e.g., secure shell) methods.

- The firewall complex must employ Transmission Control Protocol (TCP) wrappers at the host level which deny all access except for the hosts specified in the "hosts.allow" files.
- j. Administration of routers via remote access over untrusted networks is also prohibited.
 - i. Only devices that have been approved and specified by the Office of Technology Operations and Planning and registered on the Intranet may be used for remote router administration.
 - The means of remote access shall employ host-level TCP wrappers, router access control lists and user privilege levels, and Terminal Access Controller Access-Control System (TACACS) authentication.
- k. If the federal PIV credential is used as an identification token where cryptographic token-based access control is employed, the access control system must conform to the requirements of FIPS 201-1 and NIST SP 800-73-3 and 800-78-2.
- l. NIST SP 800-77 must be utilized as guidance on Internet Protocol Security (IPsec)-based virtual private networks.
- m. FIPS 201-1 and NIST SP 800-24, 800-44, Version 2, 800-45, Version 2, 800-46, Revision 1, 800-58, 800-68, Revision 1, 800-76-1, 800-87, Revision 1, and 800-96 must be utilized as guidance on remote access.

For moderate and high information systems

- n. The information system must employ automated mechanisms to facilitate the monitoring and control of remote access methods.
 - i. User activity must be audited on a variety of information system components to ensure compliance with remote access policy.
 - o. The information system must utilize cryptography to protect the confidentiality and integrity of remote access sessions.
 - i. The encryption strength of mechanism must be selected based on the security categorization of the information.
 - p. All remote accesses must be routed through a limited number of managed access control points.
 - i. Refer to OMB memoranda on the TIC.
 - q. Remote access information sessions must utilize two-factor authentication (e.g., via smart card or a time synchronization device) where one factor is provided by a device separate from or external to the computer gaining access.
 - r. The information system owner shall authorize the execution of privileged commands and access to security relevant information via remote access only for compelling operational needs and shall document the rationale for such access in the SSP for the information system.
 - s. Remote connections must be monitored for unauthorized remote access to the information system and appropriate action must be taken if an unauthorized connection is discovered.
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- t. Remote sessions for accessing EPA's list of security functions and security-relevant information must be employed and audited.
- u. For high systems users shall protect information about remote access mechanisms from unauthorized use and disclosure.
- v. Establishing a list of protocols that are not allowed except for explicitly identified components in support of specific operational requirements.

Note: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], VPN with blocking mode enabled).

- w. Networking protocols within the information system deemed to be non-secure must be disabled except for explicitly identified components in support of specific operational requirements.
- x. The organization monitors for unauthorized remote connections to the information system weekly and takes appropriate action if an unauthorized connection.

Note: The determination of the relative security of the networking protocol can be made by the organization or can be based on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

AC-18 – Wireless Access

- a. Establishing a wireless connection within the EPA network must be approved by the EPA Chief Technology Officer (CTO).
 - b. Usage restrictions and implementation guidance for wireless access must be established.
 - c. Wireless access to an information system must be authorized prior to connection.
 - d. The information system must be monitored for unauthorized wireless access.
 - e. Requirements for wireless connections to the information system must be enforced and controlled.
 - f. The following steps must be performed in order to establish wireless access to an information system:
 - i. A site survey must be performed to determine (i) the best physical location for access points and (ii) the appropriate radio channel in order to receive optimal reception throughout a given facility.
 - Considerations for implementing wireless access to an information system must include:
 - The presence of other wireless networks.
 - The type of construction material (e.g., thick cement, metal framing) used in walls, floors, and ceilings.
 - Location and surroundings of the facility.
 - ii. A site survey must be performed by a vendor or contractor that is knowledgeable and certified in the applicable area of technology.
 - g. Wireless access points must be installed with an EPA standard naming convention
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

that, at a minimum, identifies through abbreviations the following:

- Owning organization
 - Physical location of the device (i.e., room number, building abbreviation)
 - Type of device (i.e., access point)
 - The intended use as a restricted or open (shared) access point
- h. Wireless devices and connections must be configured in accordance with EPA wireless local area network (LAN) configuration documents.
 - i. NIST SP 800-48, Revision 1 and 800-97 must be utilized as guidance on wireless network security.
 - j. NIST SP 800-94 must be utilized as guidance on wireless intrusion detection and prevention.
 - k. NIST SP 800-46, Revision 1 and 800-58 must be utilized as guidance on wireless access restrictions.
 - l. Continuously using automated processes through the implementation of a wireless intrusion detection system. Weekly scanning should be performed on wireless network.

For moderate and high information systems

- m. Authentication of user, device, or both as necessary, and encryption methods compliant with NIST guidance must be used to protect wireless access to the information system.

For high information systems

- n. Unauthorized wireless connections to the information system, including thorough proactive scanning for unauthorized wireless access points must be monitored on a continuous basis and appropriate action must be taken if an unauthorized connection is discovered.
 - i. The scan must not be limited to only those areas within the facility containing the information systems, yet should be conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.
- o. Users are prohibited from independently configuring wireless networking capabilities.
- p. Wireless communications must be confined to organization-controlled boundaries by:
 - i. Reducing the power of the wireless transmission such that it cannot transit the physical perimeter of the organization.
 - ii. Employing measures such as TEMPEST to control wireless emanations.
 - iii. Configuring the wireless access such that it is point to point in nature.

AC-19 – Access Control for Mobile Devices

- a. Usage restrictions and implementation guidance must be established for EPA-
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

controlled mobile devices (i.e., devices for which EPA has the authority to specify and the ability to enforce specific security requirements).

Note: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

Note: Usage restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared).

- b. The connection of mobile devices meeting EPA's usage restrictions and implementation guidance to EPA's information systems must be authorized
- c. EPA's information systems must be monitored for unauthorized connection of mobile devices
- d. Requirements for the connection of mobile devices to EPA's information systems must be enforced.
- e. Information system functionality that provides the capability for automatic execution of code (e.g., AutoRun, AutoPlay) on mobile devices without user direction must be disabled.
- f. Specially configured mobile devices (e.g., *computers with sanitized hard drives, limited applications, more stringent configuration settings*) must be issued to individuals traveling to locations that EPA deems to be of significant risk in accordance with organizational policies and procedures.
- g. Mobile devices returning from locations that EPA deems to be of significant risk in accordance with organizational policies and procedures must be examined for signs of physical tampering and the hard disk drive must be purged and reimaged.

Note: Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed.

- h. All non-EPA mobile devices are prohibited from connecting to an EPA network unless the device has been approved, scanned, and inspected to ensure, at a minimum, the device has:
 - i. The most current software patches installed.
 - ii. The most current virus signatures.
 - iii. A personal firewall installed.
 - i. Full device encryption must be employed in order to protect information residing on
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

mobile devices.

- i. Tools, if available, for the wireless Personal Digital Assistant (PDA) being used, must be applied to encrypt data and files on the PDA.
- j. Users traveling with mobile devices shall keep the devices in their possession or sight at all times.
- k. Mobile devices must not be checked as luggage or left in hotel rooms unless secured with an EPA issued theft prevention device such as a cable lock.
- l. All EPA mobile devices must include a label identifying that it is EPA property and contact information should it be need to be returned to EPA.
- m. Refer to *Information Security – Media Protection Procedures* for guidance on protecting information residing on mobile devices.

For moderate and high information systems

- n. The use of writable, removable media must be restricted in organizational information systems.
- o. The use of personally owned, removable media is prohibited in organizational information systems.
- p. The use of removable media in organizational information systems is prohibited when the media has no identifiable owner and/or has not been granted proper authorization.

Note: An identifiable owner (e.g., individual, organization, or project) for removable media reduces the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

- q. Authorized personnel in possession of EPA-furnished mobile devices shall securely store the devices when they are not in use.
 - r. In relation to the implementation of all wireless PDA technology, the following must be adhered to:
 - i. Only devices, applications, network/personal computer (PC) connection methods, and wireless services designated as an EPA standard or approved by the Authorizing Official (AO) must be used for wireless PDA systems.
 - ii. Password protection, where a password must be entered in order to access data and applications, must be used on all wireless PDAs.
 - A password meeting EPA policies, procedures, and standards, as defined in *Information Security - Identification and Authentication Procedures*, must be used and enforced if this capability is available.
 - The password protection feature must prevent bypass without zeroing all data stored on the device; that is, if there is an attempt to bypass entering a password to access the device, the data on the device must be automatically deleted.
 - The password protection feature must be enabled at all times.
 - iii. Wireless devices must be installed with an EPA standard naming convention
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

that, at a minimum, identifies through abbreviations the following:

- Owning organization
 - Physical location of the device if it is stationary (i.e., room number, building abbreviation)
 - Principal office location of user if it is a mobile device
 - Type of device (e.g., PDAs, notebook computer)
- iv. Wireless PDAs used in areas where EPA information is processed must have wireless transmissions disabled as follows:
- Infrared (IR) ports must be disabled when IR transmissions are not being used. Data exchange via the IR port should be limited to only trusted EPA devices.
 - Bluetooth technologies on wireless PDAs must be disabled.
- s. The following must be adhered to regarding synchronizing any wireless PDA:
- i. Personally owned wireless devices are not permitted to synchronize with EPA equipment.
 - ii. Wireless PDAs that transfer, receive, store, process EPA information must not be synchronized to home or personally owned workstations and/or laptops.
 - iii. If synchronization management software does not require a password before use, it must only be launched when hot-syncing the wireless PDA and closed as soon as the hot-sync operation has been completed.
 - iv. When using synchronization management software and when booting up the computer that will be synced, the following rules must be complied with:
 - Do not launch the software during boot up if the software does not require a password before use.
 - Launch the software during boot up if the software does require a password before use.
 - v. Access control software, if available, must be installed on all workstations that have the capability to synchronize with other devices.
- t. If the wireless PDA is used for wireless Internet remote access to EPA networks, the following is required:
- i. Data encryption meeting the FIPS 140-1 or FIPS 140-2, Level 2 standard must be used on the wireless PDA.
 - Approved encryption algorithms are Triple Data Encryption Standard (3DES) or Advanced Encryption Standard (AES).
- u. Additional usage restrictions and implementation guidance for EPA-controlled mobile devices must be established, as needed.

AC-20 – Use of External Information Systems

- a. Terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems must be established that allows authorized individuals to:
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- i. Access the information system from an external information system.
- ii. Process, store, and/or transmit EPA-controlled information using an external information system.

Note: Refer to the definitions of external information system and authorized in Section 9 of this document.

- b. The terms and conditions for use of external information systems must be in accordance with Agency policies and procedures.
- c. The terms and conditions must address, at a minimum:
 - i. The types of applications that can be accessed on the EPA information system from the external information system.
 - ii. The maximum security categorization of information that can be processed, stored, and transmitted on the external information system.
- d. NIST SP 800-46, Revision 1 and 800-77 must be utilized as guidance on the use of external information systems.

Note: This procedure does not apply to the use of external information systems to access public interfaces to EPA information systems and information (e.g., individuals accessing federal information through www.epa.gov).

For moderate and high information systems

- e. Authorized individuals are permitted to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when EPA:
 - i. Can verify the implementation of required security controls on the external system as specified in EPA's information security policy and the SSP for the EPA information system being accessed.
 - ii. Has approved information system connection or processing agreements with the organizational entity hosting the external information system.
- f. The use of EPA-controlled portable storage media must be limited to authorized individuals on external information systems.

AC-22 – Publicly Accessible Content

- a. Authorized individuals must be designated by EPA before posting information onto publicly accessible information systems.
- b. Authorized individuals must be trained by EPA to ensure that publicly accessible information does not contain nonpublic information.

Note: Refer to the definition of nonpublic information in Section 9 of this document.

- c. The proposed content of publicly accessible information must be reviewed for nonpublic information prior to posting onto the information system.
 - d. Reviews of the content on the publicly accessible organizational information system for nonpublic information daily.
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- e. The content on the publicly accessible information system must be reviewed for nonpublic information on an annual basis.
 - i. If nonpublic information is discovered, it must be removed from the publicly accessible information system.
-

7. RELATED DOCUMENTS

- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995
 - NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996
 - NIST SP 800-19, *Mobile Agent Security*, October 1999
 - NIST SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000
 - NIST SP 800-28, Version 2, *Guidelines on Active Content and Mobile Code*, March 2008
 - NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003
 - NIST SP 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009
 - NIST SP 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002
 - NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007
 - NIST SP 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007
 - NIST SP 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009
 - NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*
 - NIST SP 800-48, Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008
 - NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
 - NIST SP 800-57, *Recommendation for Key Management*, March 2007
 - NIST SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005
 - NIST SP 800-63, Version 1.0.2, *Electronic Authentication Guideline*, April 2006
 - NIST SP 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, October 2008
 - NIST SP 800-68 Revision 1, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals*, October 2008
 - NIST SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition*, September 2006
 - NIST SP 800-73-3, *Interfaces for Personal Identity Verification*, February 2010
 - NIST SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007
 - NIST SP 800-77, *Guide to IPsec VPNs*, December 2005
 - NIST SP 800-78-2, *Cryptographic Algorithms and Key Sizes for Personal Identity*
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

Verification, February 2010

- NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006
 - NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005
 - NIST SP 800-87, Revision 1, *Codes for Identification of Federal and Federally-Assisted Organizations*, April 2008
 - NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007
 - NIST SP 800-95, *Guide to Secure Web Services*, August 2007
 - NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines*, September 2006
 - NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, February 2007
 - NIST SP 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, April 2007
 - NIST SP 800-104, *A Scheme for PIV Visual Card Topography*, June 2007
 - NIST SP 800-113, *Guide to SSL VPNs*, July 2008
 - NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007
 - NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008
 - NIST SP 800-121, *Guide to Bluetooth Security*, September 2008
 - NIST SP 800-123, *Guide to General Server Security*, July 2008
 - NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*, October 2008
-

8. ROLES AND RESPONSIBILITIES

Chief Technology Officer (CTO)

- a. The CTO has the following responsibilities with respect to access control:
 - i. Approve all methods of dial-up access.
 - ii. Approve all wireless connections.
 - iii. Establish, document, authorize, and monitor all methods of remote access to an information system.
 - iv. Delegating to Regions and other entities, as appropriate, co-management responsibilities for the Agency Security Architecture.

System Owner (SO)

- a. The information system owner has the following responsibilities with respect to access control:
 - i. Establish terms and conditions for use of external information systems for authorized individuals.
 - ii. Identify and document specific user actions that can be performed on the information system without identification and authentication.
 - iii. Ensure that the information system displays an approved system use notification message or banner.
 - iv. Ensure that all information system access is consistent with defined,
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

documented, and approved user access requirements, roles and responsibilities, and account privileges.

- v. Monitor all methods of remote access to an information system.
- vi. Ensuring security controls for the systems where the information is processed, stored, or transmitted

Information Security Officers

- a. ISOs have the following responsibilities with respect to access control:
 - i. Designate the individual(s) responsible for maintaining application/system access control lists.
 - ii. Receive a signed request from a designated manager prior to creating an account or assigning privileges.
 - iii. Periodically review changes to access authorizations.
 - iv. Review the activities of users with significant information system roles and responsibilities more frequently than regular system users.
 - v. Enforce separation of duties through assigned information system access authorizations.
 - vi. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.
 - vii. Review access logs to identify and delete dormant accounts (those inactive for 60 days) as appropriate.

Information System Security Officer (ISSO)

- a. The ISSO has the following responsibilities with respect to access control:
 - i. Ensure that issues regarding separation of duties are identified and appropriate actions taken to correct any conflicts.
 - ii. Monitor all methods of remote access to an information system.
 - iii. Ensuring the day-to-day security operations of an information system, including verifying security controls, technical and otherwise, are functioning as intended

Director of Office of Technology Operations and Planning (OTOP)

- a. The Director of OTOP has the following responsibilities with respect to access control:
 - i. Establish, document, authorize, and monitor all methods of remote access to an information system.

Program Managers

- a. Program managers have the following responsibilities with respect to access control:
 - i. Enforce separation of duties through assigned information system access authorizations.
 - ii. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

Account Manager

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- a. Account managers have the following responsibilities with respect to access control:
 - i. Ensure that users are registered on production systems for conducting legitimate Agency business only.
 - ii. Every EPA Automated Data Processing (ADP) coordinator and account manager shall be responsible for ensuring user identification termination for all EPA, contractor, or subcontractor employees upon the termination of a project or resignation or reassignment of personnel under his/her jurisdiction.
 - iii. Remove from the system a user terminating employment.

Automated Data Processing (ADP) Coordinator

- a. ADP Coordinators have the following responsibilities with respect to access control:
 - i. Ensure that users are registered on production systems for conducting legitimate agency business only.
 - ii. Ensure user identification termination for all EPA, contractor, or subcontractor employees upon the termination of a project or resignation or reassignment of personnel under his/her jurisdiction.
 - iii. Remove from the system a user terminating employment.

E-mail Administrators

- a. E-mail administrators have the following responsibilities with respect to access control:
 - i. Authorize, request, and terminate access to the e-mail system for users in their areas of responsibility.

Managers

- a. Managers the following responsibilities with respect to access control:
 - i. Provide immediate notification to designated support systems and applications administrative personnel when an agency employee or contractor no longer requires access.

Supervisor

- a. Supervisors have the following responsibilities with respect to access control:
 - i. Provide immediate notification to designated support systems and applications administrative personnel when an Agency employee or contractor no longer requires access.
-

9. DEFINITIONS

- Account Management – The identification of authorized users of the information system and the specification of access privileges consistent with the requirements in other security controls in the SSP.
 - Authorized Individuals – Organizational personnel, contractors, or any other individuals with authorized access to the agency information system and over which the organization has the authority to impose rules of behavior with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local, or tribal government.

- Explicitly Authorized Personnel – Security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.
 - External Information System – Any information system or components of information systems that are outside of the authorization boundary established by EPA and for which EPA has no direct supervision and authority over the application of required security controls or the assessment of the security controls' effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organization; and federal information systems that are not owned by, operated by, or under the direct supervision and authority of the Agency. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to those agencies, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies.
 - Information Flow Control – Regulation of where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization and not passing any web requests to the Internet that are not from the internal web proxy.
 - Nonpublic information – Any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Examples include information protected under the Privacy Act and vendor proprietary information.
 - Privileged Users - Individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, system and network administrators, maintainers, system programmers).
 - Remote Access – Any access to an organization information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., Internet).
 - Separation of Duties – assignment of an individual's duties such that it prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include but are not limited
-

EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- to: (i) mission functions and distinct information system support functions are divided among different individuals or roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and network security); and (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles.
- Session Lock – 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.
 - Signature (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation. Can be accomplished manually, sometimes referred to as a “wet signature,” or electronically.
 - Termination – Removal of an employee from the organization, association with, or employment in the organization (e.g., government, contracted organization, grantee organization, etc.).
 - i. *Friendly Termination* – termination under generally amicable circumstances and may include but is not limited to situations when an employee is voluntarily transferred, resigns to accept a better position, or retires.
 - ii. *Unfriendly Termination* – termination under adverse circumstances and may include but is not limited to situations when the person is being fired for cause, Reduction in Force (RIF), or involuntarily transferred or separated from service to the organization.
 - Written – or “in writing” means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.
-

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director, OTOP shall coordinate to maintain central repository of all waivers.

11. RELATED POLICY, STANDARDS AND GUIDANCE

Related policy and procedures are available on OEI's Policy Resources website.

<http://intranet.epa.gov/oei/imitpolicy/policies.htm>

Related standards and guidelines are available on OEI's website.

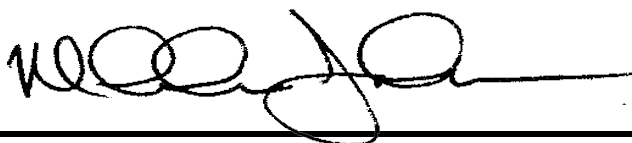
EPA Classification No.: CIO-2150.3-P-01.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

12. MATERIAL SUPERSEDED

EPA Information Security Manual, Directive 2195A1, 1999 Edition, Sections 9, 10.2, 10.3, 10.4, 11.2.1, 11.2.5 and 14 (in part).

13. ADDITIONAL INFORMATION

NA



Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

3DES	Triple Data Encryption Standard
ADP	Automated Data Processing
AES	Advanced Encryption Standard
AO	Authorizing Official
BIOS	Basic Input Output System
CTO	Chief Technology Officer
DBA	Database Administrator
DBMS	Database Management System
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ID	Identifier
IPsec	Internet Protocol Security
IR	Infrared
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OTOP	Office of Technology Operations and Planning
PC	Personal Computer
PDA	Personal Digital Assistants
PIV	Personal Identity Verification
RBAC	Role Based Access Control
RIF	Reduction in Force
SP	Special Publication
SSH	Secure Shell
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TIC	Trusted Internet Connection
USB	Universal Serial Bus
VABS	Value-Added Backbone Services
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.6	9/30/08	Initial draft	Heather Flager	Procedures-AC-Draft_TO62_020_1
2.0	6/1/09	Incorporated EPA comments	Heather Flager	Procedures-AC-Final_TO62_020_2
2.8	7/15/10	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_AC_Draft.T O-062_050_1.0
2.9	7/16/10	TISS comments and changes	Charleen Johnson	Procedures_AC_Draft.T O-062_050_1.0
3.0	1/14/11	TISS Final Draft Review	Charleen Johnson & Mark Hubbard	Procedures_AC_Draft.T O-062_050_1.0
3.1	4/20/12	SAISO Final Review	Abe Getchell & Jabran Malik	Procedures_AC_Draft.T O-062_050_1.0
3.2	7/13/12	SAISO Comments and Document Review	LaToya Gordon	Procedures_AC_Draft.T O-062_050_1.0