



INFORMATION PROCEDURE

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

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

INFORMATION SECURITY – ACCESS CONTROL PROCEDURE

1. PURPOSE

To implement the security control requirements for the Access Control (AC) family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

The 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 EPA.

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

3. AUDIENCE

The audience is all EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the 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 shall meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. This document addresses the procedures and standards set forth by the EPA, and complies with the controls in the Access Control family.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) as amended
- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)
- 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
- 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-08-16, "Guidance for Trusted Internet Connections Statement of Capability (SOC) Form," April 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
- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- Federal Information Processing Standards (FIPS) 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
- EPA Enterprise Architecture Policy
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Information Security – Roles and Responsibilities Procedures
- CIO Policy Framework and Numbering System

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

6. PROCEDURES

For the following section titles, the "AC" designator identified in each procedure represents the NIST-specified identifier for the Access Controls control family and the number represents the control identifier, as identified in NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

Abbreviations including acronyms are summarized in Appendix A.

AC-2 – Account Management

For All Information Systems:

- 1) System Owners (SO), in coordination with Information Owners (IO), for EPA-operated systems shall; and Service Managers (SM) in coordination with IOs, for systems operated on behalf of the EPA,¹ shall ensure service providers:
 - a) Manage through a life cycle consisting of establishing, activating and modifying accounts; periodically reviewing accounts; and disabling, removing or terminating information system accounts, defined as individual, group, system and role-based accounts defined as administrator, application, guest and temporary.
 - b) Assign Account Managers to accomplish life cycle activities.
 - c) Identify and select the following types of system accounts to support EPA missions/business functions: individual, group, system, application, guest and temporary.
 - i) Group and role accounts shall be treated the same as user accounts for processing and applying controls (e.g., only providing minimum access needed), and
 - ii) Processes shall be established for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
 - d) Document within applicable system security plans a description of authorized system users (e.g., public, EPA employees), criteria group and role accounts' membership with access privileges, and other applicable account attributes.
 - e) Have requests to create information system accounts approved by IOs.
 - f) Require System Administrators, Account Managers, managers and supervisors to adhere to the following requirements regarding creating, enabling, modifying, disabling or removing accounts:
 - i) Actions are based on:
 - (1) A valid access authorization,
 - (2) Intended system usage, and
 - (3) Other attributes as required by the organization or associated mission/business functions.

¹ Information Owners and Service Managers shall follow FedRAMP requirements for all cloud services obtained where EPA information is transmitted, stored, or processed on non-EPA operated systems. More information is available at the following URL: <http://cloud.cio.gov/fedramp/agency>.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- ii) Identify access requirements with required access levels for each system or application for authorized users, to include newly assigned personnel or transfers, prior to modifying or providing access,
- iii) Only assign users the minimum access privileges required,
- iv) Not grant access rights for administration or security functions of the system to normal system or application users,
- v) Process and approve requests or ensure requests for access to an information system, to establish information system accounts, or modify access are processed and approved according to the following:
 - (1) Only when initiated via written request from the user’s management,
 - (a) If the request is received via e-mail or other EPA enterprise collaboration tool (e.g., SharePoint), the request is verbally confirmed with the requester prior to granting access privileges and the e-mail or other electronic exchange is maintained for reference, annotated with the date and time of the verbal verification.
 - (2) User account request documentation is completed in full prior to account creation,
 - (a) At a minimum, the request provides the user’s name, clearance level, whether Information Security Awareness and Training (ISAT) requirements have been accomplished, all rules of behavior have been read and acknowledged in writing, and explicitly details the access privileges requested.
 - (3) Requests are approved by all applicable Information Account Managers,
 - (a) The Authorizing Official (AO) or designated representative reviews and approves requests for privileged accounts or access.
 - (4) Appropriate background checks are completed and adjudicated for unprivileged and privileged access and accounts according to EPA risk designation procedures and checklists,
 - (5) Group membership is approved in writing from SOs for EPA-operated systems and IOs for systems operated on behalf of the EPA, and
 - (6) Group membership preserves least privilege through the user’s need-to-know/need-to-share.
- vi) Maintain all access request forms while the account remains active and in accordance with EPA Records Schedule 129 on account terminations, and
- vii) Users successfully complete ISAT and role-based training requirements and all rules of behavior have been read and acknowledged in writing before receiving access to or modifying the system.²
 - (1) EPA Enterprise Wireless guest users shall read and acknowledge the rules of behavior before receiving access to the system.
- g) Automated controls prevent privileged accounts from accessing the Internet.

² Refer to Information Security – Awareness and Training Procedures for requirements on security training.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- h) Managers and supervisors and users adhere to the following requirements regarding establishing new accounts or access or modifying access:
 - i) Request in writing to establish new accounts or access from Account Managers,
 - ii) Notify Account Managers, in writing, when a user’s access requirements, e.g., information system usage, privileges or need-to-know/need-to-share change,
 - iii) Obtain written approval from Account Managers of requests to establish or modify information system accounts or access, and
 - iv) Individuals requesting to establish or modify an information system account or access shall, prior to assuming responsibility for the account or new access permissions:
 - (1) Provide proper identification,
 - (2) Successfully complete ISAT,
 - (3) Read and acknowledge in writing all applicable rules of behavior, and
 - (4) Complete and sign access request forms.
 - 2) Managers and supervisors shall oversee and review users’ activities to enforce use of information system access controls.
 - 3) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Require that Cloud Service Providers (CSPs) configure systems such that access is consistent with defined, documented, and approved user access requirements, roles and responsibilities and account privileges and adhere to the following:
 - i) System accounts and access are reviewed at least monthly to ensure that:
 - (1) Only the appropriate levels of access are allowed,
 - (2) Access is granted only to authorized personnel, and
 - (3) Users’ access rights are limited to least privilege.
 - ii) Activities of users with significant information system roles and responsibilities are reviewed more frequently than normal system users.
 - iii) Managers and supervisors and Information Security Officers (ISO) notify Account Managers: when accounts are no longer required, users are terminated – friendly or unfriendly, users are transferred, user access requirements change, or if for any reason users will not be accessing accounts for greater than 30 days.
- Note: Refer to definitions of friendly and unfriendly terminations in Section 9 of this document.
- iv) Deactivate user accounts with more than 30 days of non-use.
 - v) Delete or archive user accounts with more than 365 days of non-use.³
 - vi) Users can be allowed to self-activate accounts with greater than 30 days and less than 180 days of non-use. After 180 days of non-use or inactivity, administrator activation is required.

³ Refer to Information Security – Identification and Authentication Procedures for requirements on deleting inactive identifiers.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- vii) When a user’s official association with the EPA or authorization to access EPA information systems is terminated, all accounts associated with that user are disabled immediately. Such accounts include network access, e-mail access, etc.
 - (1) After processing the disabled account for records management, litigation hold and other similar information disposition purposes, the account shall be deleted or archived.
- viii) When users will not be accessing accounts for more than 30 days, all accounts associated with that user are disabled immediately.
- ix) All accounts are processed for records management, litigation hold and other similar information disposition purposes prior to deleting, disabling or transferring.
- x) Managers and supervisors and the ISO ensure the following activities are performed whenever an individual (EPA employee, grantees, etc.) terminates employment or transfers jobs to another Federal Agency:
 - (1) Change or cancel all passwords, codes and locks;
 - (a) Disable all accounts and user IDs;
 - (b) Update access control lists, mailing lists, etc.;
 - (c) Collect all keys, badges and similar items;
 - (d) Reconcile any financial accounts over which the individual had control;
 - (e) Properly secure or dispose of electronic records;
 - (f) In the event an individual is removed, laid off or let go under unfriendly termination, the above actions shall 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.
 - (g) Accomplish these procedures in accordance with applicable personnel, contractual and grant mechanisms; and
 - (h) Refer to Information Security – Personnel Security Procedures for requirements on personnel termination and transfer.
- xi) Managers and supervisors and the ISO ensure the following activities are performed whenever an individual (EPA employee, grantees, etc.) transfers jobs within the EPA:
 - (1) Assess all accounts, user IDs and accesses for changes in the user’s role, responsibility and location;
 - (i) Access shall be based on the user’s need-to-know/need-to-share and least privilege.
 - (2) Update access control lists, mailing lists, etc.;
 - (3) Collect all keys, badges and similar items as appropriate for the changing role and responsibility;
 - (4) Reconcile any financial accounts over which the individual had control;
 - (5) Properly secure or dispose of electronic records;

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- (6) Accomplish these procedures in accordance with applicable personnel, contractual and grant mechanisms; and
- (7) Refer to Information Security – Personnel Security Procedures for requirements on personnel termination and transfer.
- xii) Managers and supervisors and the ISO ensure the following activities are performed whenever an individual (EPA employee, grantees, etc.) takes an extended leave of absence (i.e., more than 30 days):
 - (1) Assess all accounts, user IDs and accesses to determine impact;
 - (a) Access shall be based on the user’s need-to-know/need-to-share and least privilege.
 - (2) Update access control lists, mailing lists, etc.;
 - (3) Collect all keys, badges and similar items as appropriate for the extended absence;
 - (4) Reconcile any financial accounts over which the individual had control;
 - (5) Properly secure or dispose of electronic records; and
 - (6) Accomplish these procedures in accordance with applicable personnel, contractual and grant mechanisms.
- xiii) ISOs shall ensure user accounts are disabled when a user does not complete required annual awareness training, or does not read and acknowledge in writing all rules of behavior.
 - (1) Access may be revoked if the Rules of Behavior (RoB), EPA information security directives, or applicable laws are violated. Other action, up to and including termination of EPA employment, may also be taken, depending on the particular violation.
- xiv) ISOs shall ensure Managers and supervisors remove responsibilities and SOs, IOs and SMs disable access privileges associated with their security responsibilities for users with significant security responsibilities when such a user does not complete required initial or annual role based training.

AC-2(1) – Account Management | Automated System Account Management

For Moderate and High Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Employ automated mechanisms to support the management of information system accounts.
 - i) Automated mechanisms can include, for example: e-mail or text messaging to automatically notify Account Managers when users are terminated or transferred; use of the system to monitor account usage; or telephonic notification to report atypical system account usage.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

AC-2(2) – Account Management | Removal of Temporary / Emergency Accounts

For Moderate and High Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Approve and authorize the use of special accounts, monitoring them while in use and removing, disabling or otherwise securing them when not in use.
 - i) Special accounts include guest, training, anonymous maintenance or temporary emergency accounts.
 - b) Render maintenance accounts inactive immediately after the maintenance task is completed.
 - c) Render training accounts inactive immediately after the training is completed.
 - i) Training accounts shall be rendered inactive (e.g., by resetting the password) at the end of the training event.
 - (1) If multiple classes are held during a given day, the account may remain active until the end of the day, rather than resetting the accounts between classes held on the same day.
 - d) Adhere to the following requirements for guest, temporary and emergency accounts:
 - i) Acknowledgement of the EPA rules of behavior is required before access is authorized.
 - ii) Automatically terminate within five (5) days after the need is fulfilled; or
 - iii) Automatically disable within five (5) days if additional actions are required, such as preserving records, or if additional access is authorized at a future date.
 - (1) Lock accounts that cannot be disabled.

AC-2(3) – Account Management | Disable Inactive Accounts

For Moderate and High Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to automatically disable inactive accounts after a maximum of 30 days of inactivity and alert the necessary personnel of such an event.
 - i) Users can be allowed to self-activate accounts with greater than 30 days and less than 180 days of non-use. After 180 days of non-use/inactivity, administrator activation is required.

AC-2(4) – Account Management | Automated Audit Actions

For Moderate and High Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- a) Configure the information system to automatically audit account creation, modification, disabling and termination actions and notify, as required, appropriate individuals.

AC-2(5) – Account Management | Inactivity Logout

For High Information Systems:

- 1) Users of EPA-operated systems shall:
 - a) Log out of the information system when:
 - i) The time-period of expected inactivity exceeds ninety (90) minutes.
 - ii) The user is leaving the vicinity of the system and will not be able to observe if the information system is being physically tampered with, or
 - iii) The user is unable to ensure unauthorized users cannot obtain information from the display device.

For FedRAMP⁴ Moderate Information Systems:

- 1) SMS, in coordination with IOs, shall ensure service providers:
 - a) Ensure users log out when:
 - i) The time-period of expected inactivity exceeds ninety (90) minutes.
 - ii) The user is leaving the vicinity of the system and will not be able to observe if the information system is being physically tampered with, or
 - iii) The user is unable to ensure unauthorized users cannot obtain information from the display device.

AC-2(7) – Account Management | Role-Based Schemes

For FedRAMP Moderate Information Systems:

- 1) SMS, in coordination with IOs, shall ensure service providers:
 - a) Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles. Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.
 - b) Monitor privileged role assignments.
 - c) Disable access when privileged role assignments are no longer appropriate.

AC-2(8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION

Not selected as part of the control baseline.

⁴ The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

AC-2(9) – Account Management | Restrictions on Use of Shared Groups / Accounts

For FedRAMP Moderate Information Systems:

- 1) SMs, in coordination with IOs, shall ensure service providers:
 - a) Only permit the use of shared/group accounts that meet conditions for establishing shared/group accounts.

Note: Required only if shared/group accounts are deployed.

AC-2(10) – Account Management | Group Account Credential Termination

For FedRAMP Moderate Information Systems:

- 2) SMs, in coordination with IOs, shall ensure service providers:
 - a) Configure information systems to terminate shared/group account credentials when members leave the group.

AC-2(11) – Account Management | Usage Conditions

For High Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Define circumstances and/or usage conditions for particular information system accounts as necessary to provide adequate information protection and configure the information system to enforce the circumstances and/or usage conditions.
 - i) SOs, IOs and SMs can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.

AC-2(12) – Account Management | Account Monitoring / Atypical Usage

For High Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA shall ensure service providers:
 - a) Monitor information system accounts for atypical usage, including access at unusual days and times and for unusual information transfer volumes that are not consistent with the normal usage patterns; and
 - b) Report atypical usage of information system accounts to CSIRC, the EPA Call Center, or other personnel or roles identified in the applicable security plan as an incident.

For FedRAMP Moderate Information Systems:

- 1) SMs, in coordination with IOs, shall ensure service providers::
 - a) Monitor information system accounts for atypical use; and

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

b) Report atypical usage of information system accounts to organization-defined personnel or roles.

AC-2(13) – Account Management | Disable Accounts for High-Risk Individuals

For High Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA shall ensure service providers:
 - a) Disable accounts of users posing a significant risk within one (1) hour of discovery of the risk.

AC-3 – Access Enforcement

For All Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA shall ensure service providers:
 - a) Configure the information system to enforce approved authorizations for logical access to the system in accordance with EPA policy, procedures, and standards;
 - b) Document approved explicit override of automated access controls in the associated system security plan(s) (SSP) and coordinate with applicable common control providers, for systems or applications that are normally used to support emergency operations such as emergency response for hurricanes and other natural or human initiated disasters.
 - i) The SSP shall include a description of the override process to include authorization and termination of the override and temporary auditing and monitoring compensating controls.

AC-3(1) – Access Enforcement | Restricted Access to Privileged Functions

Incorporated into AC-6.

AC-3(2) – Access Enforcement | Dual Authorization

Not selected as part of the control baseline.

AC-3(3) – Access Enforcement | Mandatory Access Control

Not selected as part of the control baseline.

AC-3(4) – Access Enforcement | Discretionary Access Control

Not selected as part of the control baseline.

AC-3(5) – Access Enforcement | Security-Relevant Information

Not selected as part of the control baseline.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

AC-3(6) – Access Enforcement | Protection of User and System Information

Not selected as part of the control baseline.

AC-3(7) – Access Enforcement | Role-Based Access Control

Not selected as part of the control baseline.

AC-3(8) – Access Enforcement | Revocation of Access Authorizations

Not selected as part of the control baseline.

AC-3(9) – Access Enforcement | Controlled Release

Not selected as part of the control baseline.

AC-3(10) – Access Enforcement | Audited Override of Access Control Mechanisms

Not selected as part of the control baseline.

AC-4 – Information Flow Enforcement

For Moderate and High Information Systems:

- 1) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs in coordination with IOs, for systems operated on behalf of the EPA shall ensure service providers:
 - a) Configure the information system to enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with EPA policy, procedures and standards.
 - b) Implement controls and requirements delineated in the EPA Information Security Architecture.
 - c) Coordinate with the Chief Enterprise Architect (CEA) and Senior Agency Information Security Officer (SAISO) to develop and maintain the EPA Information Security Architecture.

AC-4(1) – Information Flow Enforcement | Object Security Attributes

Not selected as part of the control baseline.

AC-4(2) – Information Flow Enforcement | Processing Domains

Not selected as part of the control baseline.

AC-4(3) – Information Flow Enforcement | Dynamic Information Flow Control

Not selected as part of the control baseline.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

AC-4(4) – Information Flow Enforcement | Content Check Encrypted Information

Not selected as part of the control baseline.

AC-4(5) – Information Flow Enforcement | Embedded Data Types

Not selected as part of the control baseline.

AC-4(6) – Information Flow Enforcement | Metadata

Not selected as part of the control baseline.

AC-4(7) – Information Flow Enforcement | One-Way Flow Mechanisms

Not selected as part of the control baseline.

AC-4(8) – Information Flow Enforcement | Security Policy Filters

Not selected as part of the control baseline.

AC-4(9) – Information Flow Enforcement | Human Reviews

Not selected as part of the control baseline.

AC-4(10) – Information Flow Enforcement | Enable / Disable Security Policy Filters

Not selected as part of the control baseline.

AC-4(11) – Information Flow Enforcement | Configuration of Security Policy Filters

Not selected as part of the control baseline.

AC-4(12) – Information Flow Enforcement | Data Type Identifiers

Not selected as part of the control baseline.

AC-4(13) – Information Flow Enforcement | Decomposition Into Policy-Relevant Subcomponents

Not selected as part of the control baseline.

AC-4(14) – Information Flow Enforcement | Security Policy Filter Constraints

Not selected as part of the control baseline.

AC-4(15) – Information Flow Enforcement | Detection of Unsanctioned Information

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

Not selected as part of the control baseline.

AC-4(16) – Information Flow Enforcement | Information Transfers on Interconnected Systems

Incorporated into AC-4.

AC-4(17) – Information Flow Enforcement | Domain Authentication

Not selected as part of the control baseline.

AC-4(18) – Information Flow Enforcement | Security Attribute Binding

Not selected as part of the control baseline.

AC-4(19) – Information Flow Enforcement | Validation of Metadata

Not selected as part of the control baseline.

AC-4(20) – Information Flow Enforcement | Approved Solutions

Not selected as part of the control baseline.

AC-4(21) – Information Flow Enforcement | Physical / Logical Separation of Information Flows

For FedRAMP Moderate Information Systems:

- 1) SMS, in coordination with IOs, shall ensure service providers:
 - a) Configure the information system to separate information flows logically or physically using organization-defined mechanisms and/or techniques to accomplish organization-defined required separations by types of information.

AC-4(22) – Information Flow Enforcement | Access Only

Not selected as part of the control baseline.

AC-5 – Separation of Duties

For Moderate and High Information Systems:

- 1) SOs, in coordination with managers and Supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors, for systems operated on behalf of the EPA shall ensure service providers:
 - a) Delineate duties so that the potential for abuse of authorized privileges and risk of malevolent activity without collusion is minimized,
 - b) Define system and application roles to enable implementation of separation of duty requirements, and

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- c) Implement and document separation of duties for all systems through assigned information system access authorizations.
- 2) Require managers and supervisors to review and assign duties to individuals such that assigned duties do not violate separation of duty requirements.
- 3) Instruct ISOs and Information System Security Officers (ISSOs) to ensure the following separation of duties minimum requirements are implemented:
 - a) A single individual cannot 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:
 - (1) Check issuance,
 - (2) Funds transfer,
 - (3) Input of vendor invoices,
 - (4) Other purchasing information, and
 - (5) Receiving information.
 - ii) Some additional examples of this principle include the following:
 - (1) The same individual shall not enter and authorize a purchase order.
 - (2) The same individual shall not request a user account and also create the account in the system.
 - (3) A system administrator shall not be the one to conduct the audits/reviews of the system he/she is administering.
 - (4) The ISO or ISSO shall not be a system administrator.
 - (5) 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.

- b) At a minimum, the following functions and sub-functions within the Agency shall be assigned to different individuals:
 - i) Data Creation and Control Functions
 - (1) Data collection and preparation
 - (2) 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
 - (3) Data verification, reconciliation of output and approval
 - (4) Database administration
 - ii) Software Development and Maintenance Functions
 - (1) Applications programming

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- (2) Design review
- (3) Application testing and evaluation
- (4) Application maintenance
- iii) Security Functions
 - (1) Security implementation
 - (2) Review of security controls, security audits and audit trail review

AC-6 – Least Privilege

For Moderate and High Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors’ managers, for systems operated on behalf of the EPA shall ensure service providers:
 - a) Configure systems to prevent non-privileged accounts from having access to security settings or logging/auditing settings or controls.
 - b) Employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

AC-6(1) – Least Privilege | Authorize Access to Security Functions

For Moderate and High Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors’ managers, for systems operated on behalf of the EPA shall ensure service providers:
 - a) Explicitly authorize all security functions in the SSP to particular roles.
 - i) Security functions include, but are not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.
 - ii) Roles include, but are not limited to, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers and other privileged users.

AC-6(2) – Least Privilege | Non-Privileged Access for Non-Security Functions

For Moderate and High Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Use privileged accounts or roles, i.e., with access to system administration and security functions, only when necessary to perform those system administration and security

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

duties. Users of those accounts or roles use non-privilege accounts when conducting non-system administration or security actions.

- i) Only users in privileged roles shall be authorized to use privileged accounts.
 - (1) Stipulations may be defined in the SSP for use of privileged accounts during emergency situations by users not in privileged roles.
- b) Privileged accounts or roles are audited at a minimum for:
 - i) Use of privileged or non-privileged functions, and
 - ii) When accounts are added to a privileged group.
- c) The rationale for use of network access for privileged commands is documented in the SSP.
- d) The system prevents non-privileged users from executing privileged functions including, but not limited to:
 - i) Creating information system accounts
 - ii) Performing system integrity checks
 - iii) Administering cryptographic key management activities
 - iv) Circumventing intrusion detection and prevention mechanisms
 - v) Circumventing or disabling malicious code protection mechanisms

AC-6(3) – Least Privilege | Network Access to Privileged Commands

For High Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Authorize network access to privileged commands, e.g., system administrator commands, as defined in the applicable security plan, only for system administration activities and compelling operational needs required to properly maintain the system including incident response procedures and documents the rationale for such access in the security plan for the information system.

AC-6(4) – Least Privilege | Separate Processing Domains

Not selected as part of the control baseline.

AC-6(5) – Least Privilege | Privileged Accounts

For Moderate and High Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors, for systems operated on behalf of the EPA, shall ensure service providers:

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- a) Restrict privileged accounts on the information system to system administrators, security administrators, systems assurance and security groups or other personnel or roles with an approved justification.

AC-6(6) – Least Privilege | Privileged Access By Non-Organizational Users

Not selected as part of the control baseline.

AC-6(7) – Least Privilege | Review of User Privileges

Not selected as part of the control baseline.

AC-6(8) – Least Privilege | Privileged Levels for Code Execution

Not selected as part of the control baseline.

AC-6(9) – Least Privilege | Auditing Use of Privileged Functions

For Moderate and High Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to audit the execution of privileged functions.

AC-6(10) – Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

For Moderate and High Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards/countermeasures.

AC-7 – Unsuccessful Logon Attempts

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

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.

For All Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to enforce a maximum of five consecutive invalid login attempts by a user during a 15-minute time period, and
 - b) Configure the information system to automatically lock privileged and non-privileged accounts and delay the next login prompt for 30-minutes when the maximum number of unsuccessful login attempts is exceeded.
 - i) Users are permitted access to the help desk to release their account prior to the 30 minutes lock out period if it hinders productivity.

For FedRAMP Low and Moderate Information Systems:

- 1) SMS, in coordination with IOs, shall ensure service providers:
 - a) Enforce a limit of no more than three (3) consecutive invalid logon attempts by a user during a 15 minute period.
 - b) Lock the account/node automatically for a 30-minute period when the maximum number of unsuccessful attempts is exceeded.

AC-7(1) – Unsuccessful Logon Attempts | Automatic Account Lock

Incorporated into AC-7.

AC-7(2) – Unsuccessful Logon Attempts | Purge / Wipe Mobile Device

Not selected as part of the control baseline.

AC-8 – System Use Notifications

For All Information Systems:

- 1) SOs, in coordination with managers and supervisors and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with managers and supervisors, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to display the following approved system use notification message before granting system access:
 - i) The user is accessing a U.S. Government information system and information systems that are provided for official US. Government purposes only;
 - ii) Unauthorized access to or unauthorized use of U.S. Government information or information systems is subject to criminal, civil, administrative or other lawful action;

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- iii) The term “U.S. Government information system” includes systems operated on behalf of the U.S. Government;
 - iv) You have no reasonable expectation of privacy regarding any communications or information used, transmitted or stored on U.S. Government information systems;
 - v) At any time, the U.S. Government may for any lawful government purpose and without notice, monitor, intercept, search and seize any authorized or unauthorized communication to or from U.S. Government information systems or information used or stored on U.S. Government information systems;
 - vi) At any time, the U.S. Government may for any lawful government purpose, search and seize any authorized or unauthorized device, to include non-U.S. Government owned devices, that stores U.S. Government information;
 - vii) Any communications or information used, transmitted or stored on U.S. Government information systems may be used or disclosed for any lawful government purpose, including but not limited to, administrative purposes, penetration testing, communication security monitoring, personnel misconduct measures, law enforcement and counterintelligence inquiries; and
 - viii) You may not process or store classified national security information on this computer system.
- b) Configure network security, routing, and monitoring devices to display an approved system use notification before granting access for all administrative and maintenance access.
 - c) Configure all non-publicly accessible systems to display the system use notification message that provides approved security notices and remains on the screen until the user takes explicit actions to log on to, or further access the information system.
 - d) Configure publicly accessible systems (i.e., web sites) as follows:
 - i) System use information is displayed to and acknowledged by the user before granting access.
 - (1) Use information shall include any references to monitoring, recording or auditing in keeping with privacy accommodations for such systems that generally prohibit those activities, and
 - (2) Use information shall include a description of the authorized uses of the system.
 - e) Provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) in the system use notification message or banner.
 - i) Privacy and security policies shall be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidelines,
 - (1) EPA’s Privacy and Security Notice are located at <http://www.epa.gov/epahome/usenotice2.htm>.
 - ii) A link to EPA’s Privacy and Security Notice shall be published at the top of all Region and Program Office pages, and

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

iii) In compliance with the Children’s Online Privacy Protection Act (COPPA), the standard Children’s Privacy Policy shall appear on, or be linked from, all EPA web sites aimed at children age 13 and under.

AC-9 – Previous Logon (Access) Notification

Not selected as part of the control baseline.

AC-9(1) – Previous Logon (Access) Notification | Unsuccessful Logons

Not selected as part of the control baseline.

AC-9(2) – Previous Logon (Access) Notification | Successful / Unsuccessful Logons

Not selected as part of the control baseline.

AC-9(3) – Previous Logon (Access) Notification | Notifications of Account Changes

Not selected as part of the control baseline.

AC-9(4) – Previous Logon (Access) Notification | Additional Logon Information

Not selected as part of the control baseline.

AC-10 – Concurrent Session Control

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.

For High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to limit the number of concurrent sessions to zero (0) for any user. That is, a user may have one (1) session and no others at the same time.

For FedRAMP Moderate Information Systems:

- 1) SMs, in coordination with IOs, shall ensure service providers:
 - a) Limit the number of concurrent sessions to three (3) sessions for privileged access and two (2) sessions for non-privileged access.

AC-11 – Session Lock

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- a) Configure the information system to initiate a session lock to prevent further access to the system:
 - i) After a maximum of 15 minutes of inactivity, or
 - ii) Upon receiving a request from a user.
- b) Configure the session lock:
 - i) To remain in effect until the user re-establishes access using established identification and authentication procedures, or
 - ii) To ensure it's implemented at the point where session activity can be determined.
- 2) Users shall not use the session lock control as a substitute for logging out of a system.

AC-11(1) – Session Lock, Pattern-Hiding Displays

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to conceal information previously visible on the display with a publicly viewable image.

AC-12 – Session Termination

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to automatically terminate a user session after defined conditions or trigger events (defined in the applicable security plan) requiring session disconnect.

Note: This requirement addresses the termination of user-initiated logical sessions. A logical session (for local, network and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an EPA information system.

- i) Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

AC-12(1) – Session Termination | User-Initiated Logouts / Message Displays

Not selected as part of the control baseline.

AC-13 – Supervision and Review – Access Control

Incorporated into AC-2 and Audit and Accountability Control (AU) AU-6.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

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 a 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.

For All Information Systems:

- 1) Users may access public websites or publicly available information on accessible Federal information systems without identification and authentication.
- 2) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Identify and document in the SSP specific user actions that can be performed on the information system without identification and authentication.
 - i) Supporting rationale for not requiring identification and authentication shall be documented in the SSP;
 - ii) Stipulations may be defined in the SSP for bypassing identification and authentication mechanisms to facilitate operations in emergency situations; and
 - iii) 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.
 - (1) The access shall be authorized and monitored by a Senior Information Official (SIO).
 - b) Implement additional security measures at the directory and file level for application-specific user IDs and generic user IDs not requiring passwords.
 - i) Those user IDs shall be given rights to only those directories and files necessary for proper execution of the application.

AC-14(1) – Permitted Actions Without Identification or Authentication | Necessary users

Incorporated into AC-14.

AC-15 – Automated Marking

Incorporated into Media Protection (MP) Control MP-3.

AC-16 – Security Attributes

Not selected as part of the control baseline.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

AC-16(1) – Security Attributes | Dynamic Attribute Association

Not selected as part of the control baseline.

AC-16(2) – Security Attributes | Attribute Value Changes by Authorized Individuals

Not selected as part of the control baseline.

AC-16(3) – Security Attributes | Maintenance of Attribute Associations By Information System

Not selected as part of the control baseline.

AC-16(4) – Security Attributes | Association of Attributes by Authorized Individuals

Not selected as part of the control baseline.

AC-16(5) – Security Attributes | Attribute Displays for Output Devices

Not selected as part of the control baseline.

AC-16(6) – Security Attributes | Maintenance of Attribute Association by Organization

Not selected as part of the control baseline.

AC-16(7) – Security Attributes | Consistent Attribute Interpretation

Not selected as part of the control baseline.

AC-16(8) – Security Attributes | Association Techniques / Technologies

Not selected as part of the control baseline.

AC-16(9) – Security Attributes | Attribute Reassignment

Not selected as part of the control baseline.

AC-16(10) – Security Attributes | Attribute Configuration By Authorized Individuals

Not selected as part of the control baseline.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

AC-17 – Remote Access

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

For All Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:

- a) Document within the SSP all allowed methods of remote access (e.g., dial-up, broadband, wireless) to an information system.

Note: Remote access is access to organizational information by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet).

Note: A VPN when adequately provisioned with appropriate security controls (e.g., employing appropriate FIPS 140-2 compliant encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks.

- b) Establish and document usage restrictions and implementation guidance for each allowed remote access method in the SSP.

- c) Continuously monitor,⁵ in coordination with the Director, Office of Technology Operations and Planning (OTOP) for EPA systems, unauthorized remote access to the system for:

- i) Routing all connections traversing the Internet through EPA Trusted Internet Connection (TIC) capabilities (Appendix B).⁶
- ii) Unauthorized connections, including dual-homed devices and bypassing EPA Trusted Internet Connection (TIC) capabilities.

- iii) When detected on EPA systems:

- (1) An alert is sent to appropriate system personnel and the Computer Security Incident Response Capability (CSIRC), and
- (2) An alert is sent every hour thereafter until the device is removed from the network or authorized by the configuration management process.
 - (a) Alerts are escalated after 24 hours without appropriate action

- iv) When detected on systems operated on behalf of the EPA:

- (1) Notifications are provided to EPA personnel in accordance with interconnection agreement, memorandum of agreement/understanding, contract or similar requirements and coordination documents.

⁵ Continuous Monitoring requirements are developed by the SAISO and provided in the EPA Continuous Monitoring Strategic Plan. Detailed implementation procedures, guidance and standards are provided by the Director of OTOP.

⁶ Trusted Internet Connection-Mandate as a result of M-08-05 issued November 2007 which is meant to optimize individual external connections, including Internet points of presence currently in use by the US Federal Government.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- d) Authorize remote access to the information system prior to the connection.
- e) Enforce requirements for the remote connection to the information system.
- f) Ensure remote access controls are applicable to information systems other than the publicly accessible capabilities of public web servers or systems specifically designed for public access.
- g) Implement adequate security measures (e.g., virus and spam protection, firewall, intrusion detection) on client computers prior to allowing remote or adequately protected VPN access,
 - i) Access to the EPA network is a privilege and shall be denied, at the EPA Risk Executive’s discretion, to clients attached to networks deemed unacceptably vulnerable.
- h) Restrict remote access over untrusted networks such as the Internet or via modem for security appliance or security software administration. Remote access over untrusted networks, such as the Internet or via modem, is not used for administration of routers.
 - i) Only devices that have been approved and specified by the Director, OTOP and registered on the Intranet may be used for remote router administration.
- i) Ensure, in coordination with the Director, OTOP for EPA systems, that endpoint protection systems are configured to disallow “dual-homed” connections, e.g. a laptop shall not be permitted to be connected to an EPA system via wired/VPN connection while using a separate wired or wireless connection to a non-EPA external system.

AC-17(1) – Remote Access | Automated Monitoring / Control

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to employ automated mechanisms to facilitate the monitoring and control of remote access methods.
 - i) User activity shall be audited on a variety of information system components to ensure compliance with remote access policy.

AC-17(2) – Remote Access | Protection of Confidentiality / Integrity using Encryption

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Configure the information system to use cryptography⁷ to protect the confidentiality and integrity of remote access sessions.

⁷ All cryptography shall be implemented using FIPS 140-2 validated modules in FIPS mode.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- i) The encryption strength of mechanism shall be selected based on the security categorization of the information and in compliance with FIPS 140-2.

AC-17(3) – Remote Access | Managed Access Control Points

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Route all connections traversing the Internet through EPA Trusted Internet Connection (TIC) capabilities (Appendix B).⁸

AC-17(4) – Remote Access | Privileged Commands/Access

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Allow the execution of privileged commands and access to security relevant information via remote access only for compelling operational needs and when rationale for such access is documented in the SSP.
 - i) Such access shall be audited and logged.

AC-17(5) – Remote Access | Monitoring for Unauthorized Connections

Incorporated into System and Information Integrity (SI) control SI-4.

AC-17(6) – Remote Access | Protection of Information

Not selected as part of the control baseline.

AC-17(7) – Remote Access | Additional Protection for Security Function Access

Incorporated into AC-3(10).

AC-17(8) – Remote Access | Disable Non-Secure Network Protocols

Incorporated into Configuration Management (CM) control CM-7.

AC-17(9) – Remote Access | Disconnect / Disable Access

For FedRAMP Moderate Information Systems:

⁸ *Trusted Internet Connection-Mandate as a result of M-08-05 issued November 2007 which is meant to optimize individual external connections, including Internet points of presence currently in use by the US Federal Government.*

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- 1) SMS, in coordination with IOs, shall ensure service providers:
 - a) Provide the capability to expeditiously disconnect or disable remote access to the information system within a time period no greater than 15 minutes.

AC-18 – Wireless Access

For All Information Systems:

- 1) The Director, OTOP shall:
 - a) Develop implementation guidance and minimum usage restrictions for wireless access in the EPA.
 - b) Establish configuration and connection requirements.
- 2) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Obtain authorization from the Authorizing Official for wireless use prior to implementation.
 - b) Implement and enforce requirements for using wireless connections to EPA systems.
 - c) Continuously monitor, in coordination with the Director, OTOP for EPA systems, for unauthorized wireless connections.
 - i) When detected on EPA systems:
 - (1) An alert is sent to appropriate system personnel and the CSIRC.
 - (2) The device is automatically isolated and an alert is sent upon isolation.
 - (3) An alert is sent every 24 hours thereafter until device is removed from the network or authorized via the configuration management process.
 - (a) Alerts are escalated after 24 hours without appropriate action.
 - (4) When detected on systems operated on behalf of the EPA, notifications are provided to EPA personnel in accordance with interconnection agreement, memorandum of agreement/understanding, contract or similar requirements, and coordination documents.
 - d) Ensure that endpoint protection systems are configured to disallow “dual-homed” wireless/wired connections, e.g. a laptop shall not be permitted to be connected to an EPA system via wired/VPN connection while using a wireless connection to a non-EPA external system.

AC-18(1) – Wireless Access | Authentication and Encryption

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Authenticate users and devices on the wireless system.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- b) Implement FIPS 140-2 compliant cryptographic protections for the integrity and confidentiality of information transmitted on the wireless system.

AC-18(2) – Wireless Access | Monitoring Unauthorized Connections

Incorporated into SI-4.

AC-18(3) – Wireless Access | Disable Wireless Networking

Not selected as part of the control baseline.

AC-18(4) – Wireless Access | Restrict Configurations by Users

For High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Authorize roles allowed to independently configure wireless networking capabilities, e.g., network administrators through documentation in the SSP.
 - b) Confine wireless communications to organization-controlled boundaries according to standards, procedures and guidance developed by the Director, OTOP.

AC-18(5) – Wireless Access | Antennas / Transmission Power Levels

For High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Select radio antennas and calibrate transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

AC-19 – Access Control for Mobile Devices

For All Information Systems:

- 1) The Chief Information Officer (CIO) shall:
 - a) Identify types of mobile devices authorized for use with EPA information.
- 2) The Director, OTOP shall:
 - a) Develop technical implementation procedures and guidance for mobile device access control with access to EPA information; this includes configurations for devices used on travel to high-risk locations.
 - b) Continuously monitor all network traffic within the EPA data and voice communications networks to detect and respond to intrusion and network misuse.

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

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

capability (e.g., notebook/laptop computers, personal digital assistants, smartphones, tablets, digital cameras and audio recording devices).

Note: Technical implementation procedures and guidance related to mobile devices includes but is not limited to 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).

- 3) SOs, in coordination with IOs, for EPA-operated systems shall; and SMs and IOs, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Implement and enforce mobile device access requirements according to EPA standards.
 - b) Continuously monitor for unauthorized connection of mobile devices in coordination with the Director, OTOP for EPA systems.
 - c) Follow the procedures below when unauthorized connections are detected on EPA systems:
 - i) An alert is sent to appropriate system personnel and the CSIRC,
 - ii) Information system functionality that provides the capability for automatic execution of code (e.g., AutoRun, AutoPlay) on mobile devices without user direction is disabled,
 - iii) The device is automatically isolated and an alert is sent upon isolation, and
 - iv) An alert is sent every 24 hours thereafter until device is removed from network or authorized by configuration management process.
- 4) Ensure Users shall:
 - a) Adhere to the guiding principles and framework established in the EPA Mobile Computing Policy.
 - b) Connect non-EPA owned mobile devices only to authorized EPA information management and technology solutions to access EPA's network outside of EPA's secured physical location (e.g. telework status, official travel).
 - c) Synchronize with or store EPA information using only authorized EPA information management and technology solutions.
 - d) Securely store mobile devices containing EPA information when they are not in use.

AC-19(1) – Access Control for Mobile Devices | Use of Writeable / Portable Storage Devices

Incorporated into MP-7.

AC-19(2) – Access Control for Mobile Devices | Use of Personally Owned Portable Storage Devices

Incorporated into MP-7.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

AC-19(3) – Access Control for Mobile Devices | Use of Portable Storage Devices with No Identifiable Owner

Incorporated into MP-7.

AC-19(4) – Access Control for Mobile Devices | Restrictions for Classified Information

Not selected as part of the control baseline.

AC-19(5) – Access Control for Mobile Devices | Full Device / Container-Based Encryption

For Moderate and High Information Systems:

- 1) SIOs shall ensure:
 - a) Enterprise solutions for full-disk encryption are deployed to protect the confidentiality and integrity of information on all EPA mobile computing devices such as laptops, netbooks, and similar devices;
 - b) Mobile storage devices such as USB hard drives, USB thumb drives, tapes, MP3 players, and similar devices use approved encryption to protect information storage areas; and
 - c) Mobile computing devices such as smartphones, tablets, and other similar handheld devices employ enterprise defined mobile device management and encryption solutions.
 - d) Encryption mechanisms utilized are FIPS 140-2-compliant.

AC-20 – Use of External Information Systems

For All Information Systems:

- 1) Information of which EPA IOs have relinquished control⁹ may be accessed from external systems through defined interfaces or exchange mechanisms.¹⁰
 - a) The Director, OTOP, Director, Office of Information Analysis and Access (OIAA), and Director, Office of Information Collection (OIC) shall coordinate to develop procedures, standards, and guidance on implementation requirements and configurations for interfaces and exchange mechanisms.
- 2) Authorized users of EPA information, e.g., EPA employees, personnel under contract with EPA and interns, may access, store or process EPA information through mechanisms, such as virtual desktop interfaces, controlled processing environments or encrypted containers,

⁹ Information for which EPA Information Owners have relinquished control no longer requires protection under the Federal Information security Act (FISMA), Office of Management and Budget (OMB) directive A-130 and other related regulations and directives. Information for which EPA has relinquished control is not equivalent to information defined as releasable to the public. EPA has a responsibility under FISMA and OMB A-130 to protect the integrity and availability of public information provided by EPA on EPA systems or on systems operated on behalf of EPA.

¹⁰ The defined interfaces and exchange mechanisms shall clearly state and notify users that EPA has relinquished control of the information and no longer has responsibility to protect the integrity, confidentiality, or availability of the information, the information is provided on an “as is” basis and the user assumes responsibility for its use.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

that ensure the information and systems are adequately protected and meeting information security requirements.

- a) The EPA CIO shall determine and authorize mechanisms.
- b) The Director, OTOP shall develop procedures, standards, and guidance on implementation requirements and configurations for authorized mechanisms.

AC-20(1) – Use of External Information Systems | Limits on Authorized Use

For Moderate and High Information Systems:

- 1) SOs, in coordination with the Director, OTOP, and IOs, for EPA-operated systems shall; and SMs and IOs, in coordination with the Director, OTOP, for systems operated on behalf of the EPA, shall ensure service providers:
 - a) Have implemented protections for external information systems in accordance with EPA directives before EPA information is stored, processed, or transmitted on those systems.

AC-20(2) – Use of External Information Systems | Portable Storage Devices

For All Information Systems:

- 1) Portable storage devices may be used on external systems when not transferring information for storage to the external system, for example, to present a brief at a conference on the host's projection system where the brief during the presentation is accessed through the projection system from the portable storage device.
 - a) Users shall contact their help desk support to scan rewriteable devices for malware prior to accessing EPA systems after such use.

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

AC-20(3) – Use of External Information Systems | Non-Organizationally Owned Systems / Components / Devices

Not selected as part of the control baseline.

AC-20(4) – Use of External Information Systems | Network Accessible Storage Devices

Not selected as part of the control baseline.

AC-21 – Information Sharing

For Moderate and High Information Systems:

- 1) SIOs shall ensure service providers:
 - a) Determine whether access authorizations assigned to information users, i.e., external partners, EPA employees and contractors, match the access restrictions on all sensitive

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

but unclassified information, e.g., privileged medical information, contract-sensitive information and proprietary information; and

- b) Assist users in making appropriate information sharing decisions with such information by:
 - i) Developing mechanisms or processes to assist users in making appropriate sharing decisions; and
 - ii) Training personnel on the mechanisms or processes.

AC-21(1) – Information Sharing | Automated Decision Support

Not selected as part of the control baseline.

AC-21(2) – Information Sharing | Information Search and Retrieval

Not selected as part of the control baseline.

AC-22 – Publicly Accessible Content

For All Information Systems:

- 1) SIOs shall ensure service providers:
 - a) Designate individuals as authorized to post information onto publicly accessible information systems;
 - b) Train designated individuals to ensure that publicly accessible information does not contain non-public information;
 - c) Review the proposed content of publicly accessible information to ensure non-public information is not included prior to posting onto the information system; and
 - d) Review content on the publicly accessible information system for non-public information and remove such information if discovered.
 - i) Content shall be reviewed at a frequency commensurate with the frequency information is posted. For example, blog sites that are used daily should be reviewed daily.
 - ii) Personnel conducting these reviews should be different than those posting or conducting the reviews prior to posting.

For FedRAMP Low and Moderate Information Systems:

- 1) SMS, in coordination with IOs, shall ensure service providers:
 - a) Review the content on the publicly accessible information system for nonpublic information at least quarterly and remove such information, if discovered.

AC-23 – Data Mining Protection

Not selected as part of the control baseline.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

AC-24 – Access Control Decisions

Not selected as part of the control baseline.

AC-25 – Reference Monitor

Not selected as part of the control baseline.

7. RELATED DOCUMENTS

- Mobile Computing Management Procedures, EPA Classification No. CIO-2150.4-P-01.1
- Mobile Computing Policy, EPA Classification No. CIO-2150.4
- NIST Special Publications, 800 series
- NIST Federal Information Processing Standards

8. ROLES AND RESPONSIBILITIES

Chief Enterprise Architect (CEA)

- 1) The CEA is responsible for:
 - a) Coordinating with the SAISO to develop and implement the agency’s information security architecture.
 - b) Facilitating the integration of information security into all layers of enterprise architecture to ensure agency implementation of security solutions.

Director, Office of Technology Operations and Planning (OTOP)

- 1) The Director, OTOP has the following responsibilities with respect to access control:
 - a) Establish, document, authorize and monitor all methods of remote access to an information system.
 - b) Develop implementation guidance and minimum usage restrictions for wireless access in the EPA.
 - c) Develop procedures, standards and guidance on implementation requirements and configurations for interfaces and exchange mechanisms.

System Owner (SO)

- 2) The information SO has the following responsibilities with respect to access control:
 - a) Ensure that system user and group accounts are managed according to EPA standards.
 - b) Establish terms and conditions for use of external information systems for authorized individuals.
 - c) Identify and document specific user actions that can be performed on the information system without identification and authentication.
 - d) Ensure the principles of least privilege and separation of duties are followed.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

- e) Ensure that the information system displays an approved system use notification message or banner.
- f) Ensure that all information system access is consistent with defined, documented and approved user access requirements, roles and responsibilities, and account privileges.
- g) Monitor all methods of remote access to an information system.
- h) Ensure security controls for the systems where the information is processed, stored or transmitted.
- i) Enforce separation of duties through assigned information system access authorizations.
- j) Separate duties of individuals as necessary to prevent malevolent activity without collusion.

Information Security Officers (ISO)

- 3) ISOs have the following responsibilities with respect to access control:
 - a) Designate the individuals responsible for maintaining application/system access control lists.
 - b) Receive a signed request from a designated manager prior to creating an account or assigning privileges.
 - c) Review changes to access authorizations periodically.
 - d) Review the activities of users with significant information system roles and responsibilities more frequently than regular system users.
 - e) Enforce separation of duties through assigned information system access authorizations.
 - f) Enforce principle of least privilege for account creation and management.
 - g) Coordinate with Account Managers for routine account maintenance.
 - h) Review access logs to identify and delete dormant accounts (those inactive for 30 days) as appropriate.

Information Owners (IO)

- 4) The IO has the following responsibilities with respect to access control:
 - a) Ensure that all information system access is consistent with defined, documented and approved user access requirements, roles and responsibilities, and account privileges.
 - b) Ensure the information system enforces approved authorizations for logical access to the system in accordance with EPA policy, procedures and standards.
 - c) Implement and enforce requirements for wireless connections to EPA systems.
 - d) Authorize and approve all special accounts; ensure they are monitored while in use; and that they are removed, disabled or otherwise secured when not in use and maintained. Special accounts include guest, training, anonymous maintenance or temporary emergency accounts.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

Information System Security Officer (ISSO)

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

Managers and Supervisors

- 6) Managers and supervisors have the following responsibilities with respect to access control:
 - a) Provide immediate notification to designated support systems and applications administrative personnel when an agency employee or contractor no longer requires access.
 - b) Coordinate with system administrators when requesting account creation or modification.
 - c) Enforce separation of duties through assigned information system access authorizations.
 - d) Separate duties of individuals as necessary, to prevent malevolent activity without collusion.
 - e) Ensure that users are registered on production systems for conducting legitimate Agency business only.
 - f) 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.

Service Managers (SM)

- 7) Service Managers have the following responsibilities with respect to access control:
 - a) Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles.
 - b) Enforce Role Based Access Controls (RBAC) over all users and resources, where the policy rule set for each policy specifies the information system session lock mechanism where applicable.
 - c) Support and maintain the binding of attributes to information in storage, in process and in transmission.
 - d) Monitor for unauthorized wireless connections to the information system.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

Senior Information Officials (SIO)

- 8) Senior Information Officials have the following responsibilities with respect to access control:
 - a) Monitor user actions that can be performed on the information system without identification and authentication.
 - b) Ensure enterprise solutions for full-disk encryption are deployed to protect the confidentiality and integrity of information on all EPA mobile computing devices such as laptops, netbooks and similar devices.
 - c) Determine whether access authorizations assigned to information users, i.e., external partners, EPA employees and contractors, match the access restrictions on all sensitive but unclassified information, e.g., privileged medical information, contract-sensitive information and proprietary information.
 - d) Assist users in making appropriate information sharing decisions.
 - e) Designate individuals authorized to post information onto publicly accessible information systems.
 - f) Train designated individuals to ensure that publicly accessible information does not contain non-public information.
 - g) Review content on the publicly accessible information system for non-public information, and remove such information if discovered.

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 relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local or tribal government.
- *EPA Operated System* – A system where EPA personnel have sole, direct system management responsibilities. System administration is directed by EPA personnel and may be accomplished by EPA Federal employees or contractors. The system may be operated internally or externally to EPA's intranet boundary.
- *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 the EPA and for which the EPA has no direct supervision or 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

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

(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.
- *Non-public 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).
- *Sensitive information* – Information, where the loss, misuse, or unauthorized access to or modification of said information could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
- *Separation of Duties* – Assignment of an individual's duties so that users are prevented 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 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 or network security); and (iii) security personnel who administer access

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

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).
- *System Operated on Behalf of the EPA* – A system where EPA personnel do not have sole or direct system management responsibilities. System administration is directed by and performed by service provider personnel. The system may be operated at or externally to the EPA’s intranet boundary.
- *Termination* – Removal of an employee from the organization, association with, or employment in the organization (e.g., government, contracted organization, grantee organization, etc.).
- *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.
- *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)* – to officially document the action or decision, either manually or electronically, and includes a signature.

11. WAIVERS

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

- Substantive business case needs
- 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.

Information Security – Access Control Procedure	
PA Classification No.: CIO 2150-P-01.2	CIO Approval Date: 09/21/2015
CIO Transmittal No.: 15-015	Review Date: 09/21/2018

12. 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>

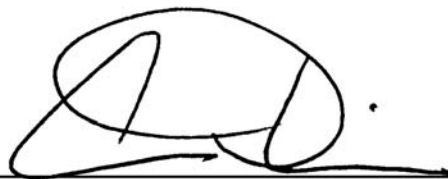
Related standards and guidelines are available on OEI's website.

13. MATERIAL SUPERSEDED

- Information Directive: CIO 2150-P-01.1 Information Security – Interim Access Control Procedure

14. ADDITIONAL INFORMATION

N/A



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

APPENDIX A: ABBREVIATIONS AND ACRONYMS

AO	Authorizing Official
CIO	Chief Information Officer
COPPA	Children's Online Privacy Protection Act
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
IaaS	Infrastructure as a Service
ID	Identifier
IPsec	Internet Protocol Security
IR	Infrared
ISAT	Information Security Awareness and Training
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
PaaS	Platform as a Service
PC	Personal Computer
PDA	Personal Digital Assistants
PIV	Personal Identity Verification
RBAC	Role Based Access Control
RoB	Rules of Behavior
RIF	Reduction in Force
SP	Special Publication
SSH	Secure Shell
SSP	System Security Plan(s)
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

Figure 1: Conceptual Model for TIC Trust Relationships

