Policy No: CIO 2150-P-01.4

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Access Control (AC) Procedure

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Access (AC) Control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

2. SCOPE

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

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. AUTHORITY

EPA is responsible for ensuring 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 security requirements by implementing the security controls defined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

Additional legal foundations for the Access Controls Procedure include:

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113- 283, to amend chapter 35 of title 44, United States Code (U.S.C.)

- OMB Circular A-130, "Managing Information as a Strategic Resource," Appendix I, "Responsibilities for Protecting and Managing Federal Information Resources," July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

5. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "AC" designator (e.g., AC-2, AC-3) identified for each procedure below corresponds to the NIST- identifier for the Access Control family, as identified in NIST SP 800- 53, Revision 5,*Security and Privacy Controls for Federal Information Systems and Organizations.*

NIST defines the applicable AC security and privacy baseline controls in NIST 800-53B, Control Baselines for Information Systems and Organizations. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name.

AC-2 – ACCOUNT MANAGEMENT
FOR ALL SYSTEMS:

1) Define and document the types of accounts allowed and specifically prohibited for use within the system;
2) Assign account managers;
3) Require system-specific prerequisites and criteria if needed for group and role membership;

4) Specify:
   a) Authorized users of the system;
   b) Group and role membership; and
   c) Access authorizations (i.e., privileges) and system-specific attributes as required for each account;
5) Require approvals by Information Owner (IO) for requests to create accounts;
6) Create, enable, modify, disable, and remove accounts in accordance with the EPA Information Security – Access Control (AC) Procedure and associated supplemental guidance (EPA Cybersecurity Handbook);
7) Monitor the use of accounts;
8) Notify account managers and ISO and Information System Security Officers (ISSO) within:
   a) Three (3) days when accounts are no longer required;
   b) Four hours of departure for involuntary terminations and same day of departure for voluntary terminations when users are terminated or transferred; and
   c) Three (3) days when system usage or need-to-know changes for an individual;
9) Authorize access to the system based on:
   a) A valid access authorization;
   b) Intended system usage;
   c) Business need and system-specific criteria as required;
10) Review accounts for compliance with account management requirements every sixty (60) days;
11) Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
12) Align account management processes with personnel termination and transfer processes.

AC-2(1) – ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT FOR MODERATE AND HIGH SYSTEMS:

1) Support the management of system accounts using automated mechanisms.

AC-2(2) – ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT

For Moderate and High Systems:

1) Automatically remove temporary and emergency accounts immediately after the need for such an account has expired.

AC-2(3) – ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR MODERATE AND HIGH SYSTEMS:

1) Disable accounts within fifteen (15) days when the accounts:
   a) Have expired;
   b) Are no longer associated with a user or individual;
   c) Are in violation of organizational policy; or
   d) Have been inactive for fifteen (15) days for High Systems and forty-five (45) days for Moderate Systems.

AC-2(4) – ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS FOR MODERATE AND HIGH SYSTEMS:

1) Automatically audit account creation, modification, enabling, disabling, and removal actions.

AC-2(5) – ACCOUNT MANAGEMENT | INACTIVITY LOGOUT

FOR MODERATE AND HIGH SYSTEMS:

1) Require that users log out when time period of inactivity exceeds thirty (30) minutes and at the end of the user's normal work period.

AC-2(11) – ACCOUNT MANAGEMENT | USAGE CONDITIONS

FOR HIGH SYSTEMS:

1) Enforce restricting usage to certain days of the week, time of day or specific durations of time 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.

AC-2(12) – ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE

FOR HIGH SYSTEMS:

1) Monitor system accounts for atypical usage of system accounts such as accessing systems at times and locations not consistent with normal usage patterns; and
2) Report atypical usage of system accounts to Computer Security Incident Response Capability (CSIRC), the EPA Call Center and ISO.

AC-2(13) – ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

FOR MODERATE AND HIGH SYSTEMS:

1) Disable accounts of individuals immediately but no later than one (1) hour of discovery of users who pose a significant security and/or privacy risk including involuntary terminations and for whom reliable evidence indicating either intention to use authorized access to systems to cause harm or through whom adversaries will cause harm.

AC-3 – ACCESS ENFORCEMENT

FOR ALL SYSTEMS:

1) Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-3(14) – ACCESS ENFORCEMENT | INDIVIDUAL ACCESS

FOR PRIVACY CONTROL BASELINE:

1) Provide Privacy Act requests for systems containing personally identifiable information (PII) to enable individuals to have access to the following elements of their personally identifiable information: such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information as defined by the Privacy Act of 1974.

AC-4 – INFORMATION FLOW ENFORCEMENT

FOR MODERATE AND HIGH SYSTEMS:

1) Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on Memorandum of

Understanding (MOUs), Interconnection Security Agreements (ISAs), and other information sharing authorizations as specified by Federal regulations, requirements and directives.

AC-4(4) – INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION

FOR HIGH SYSTEMS:

1) Prevent encrypted information from bypassing decryption technologies, firewalls, and content filtering mechanisms by decrypting and blocking the flow of the encrypted information until authorized by the ISO.

AC-5 – SEPARATION OF DUTIES

For Moderate and High Systems:

1) Identify and document system and application roles to enable implementation of separation of duty requirements for both the general user and privileged users; and
2) Define system access authorizations to support separation of duties.

AC-6 – LEAST PRIVILEGE

For Moderate and High Systems:

1) Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

AC-6(1) – LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

FOR MODERATE AND HIGH SYSTEMS:

1) Authorize access for system administrators and those designated as their backup to:
   a) Establish system accounts, configure access authorizations (i.e., permissions, privileges), setting events to be audited and setting intrusion detection parameters (deployed in hardware, software, and firmware); and
   b) Security-related information including filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management

information, and access control lists.

AC-6(2) – LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS FOR MODERATE AND HIGH SYSTEMS:

1) Require that users of system accounts (or roles) with access to system administration and security functions use non-privileged accounts or roles, when accessing non- security functions.

AC-6(3) – LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS FOR HIGH SYSTEMS:

1) Authorize network access to system administrator commands, only for compelling operational needs required to properly maintain the system, and document the rationale for such access in the security plan for the system.

AC-6(5) – LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

FOR MODERATE AND HIGH SYSTEMS:

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

AC-6(7) – LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

FOR MODERATE AND HIGH SYSTEMS:

1) Review quarterly the privileges assigned to all privileged users to validate the need for such privileges; and
2) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-6(9) – LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS FOR MODERATE AND HIGH SYSTEMS:

1) Log the execution of privileged functions.

AC-6(10) – LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

For Moderate and High Systems:

1) Prevent non-privileged users from executing privileged functions

AC-7 – UNSUCCESSFUL LOGON ATTEMPTS FOR ALL SYSTEMS:

1) Enforce a limit of a maximum of five (5) consecutive invalid logon attempts by a user during a fifteen (15) minute time-period; and
2) Automatically lock the account or node for thirty (30) minutes or until authorization to release is received by the account manager and/or system administrator or successfully authenticated via a challenge response when the maximum number of unsuccessful attempts is exceeded.

AC-8 – SYSTEM USE NOTIFICATIONS FOR ALL SYSTEMS:

1) Display the following approved system use notification banner: "In proceeding and accessing U.S. Government information and information systems, you acknowledge that you fully understand and consent to all of the following: 1) You are accessing U.S. Government information and information systems that are provided for official U.S. Government purposes only; 2) Unauthorized access to or unauthorized use of U.S. Government information or information systems is subject to criminal, civil, administrative, or other lawful action; 3) The term U.S. Government information system includes systems operated on behalf of the U.S. Government; 4) You have no reasonable expectation of privacy regarding any communications or information used, transmitted, or stored on U.S. Government information systems; 5) At any time, the U.S. Government may for any lawful government purpose, 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; 6) 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; 7) 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 8) You may not process or store classified national security information on this computer system." To users before granting access to the system that provides privacy and security notices consistent with

applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

a) Users are accessing a U.S. Government system;

b) System usage may be monitored, recorded, and subject to audit;

c) Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

d) Use of the system indicates consent to monitoring and recording;

2) Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

3) For publicly accessible systems:

a) Display system use information requiring acknowledgement by the user, before granting further access to the publicly accessible system;

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

c) Include a description of the authorized uses of the system.

AC-10 – CONCURRENT SESSION CONTROL

FOR HIGH SYSTEMS:

1) Limit the number of concurrent sessions for each user to zero (0) or configure the system to not allow concurrent sessions.

AC-11 – DEVICE LOCK

For Moderate and High Systems:

1) Prevent further access to the system by initiating a device lock after a maximum of fifteen (15) minutes of inactivity; and

2) Retain the device lock until the user reestablishes access using established identification and authentication procedures.

AC-11(1) – DEVICE LOCK | PATTERN-HIDING DISPLAYS

FOR MODERATE AND HIGH SYSTEMS:

1) Conceal, via the device lock, information previously visible on the display

with a publicly viewable image.

AC-12 – SESSION TERMINATION

FOR MODERATE AND HIGH SYSTEMS:

1) Automatically terminate a user session after ninety (90) minutes of user inactivity or defined conditions or trigger events (defined in the applicable System Security Plan (SSP)) requiring session disconnect.

AC-14 – PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

FOR ALL SYSTEMS:

1) Identify explicit and limited user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
2) Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

AC-17 – REMOTE ACCESS

FOR ALL SYSTEMS:

1) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2) Authorize each type of remote access to the system prior to allowing such connections.

AC-17(1) – REMOTE ACCESS | MONITORING AND CONTROL

FOR MODERATE AND HIGH SYSTEMS:

1) Employ automated mechanisms to monitor and control remote access methods.

AC-17(2) – REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

For Moderate and High Systems:

1) Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

AC-17(3) – REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS FOR MODERATE AND HIGH SYSTEMS:

1) Route remote accesses through authorized and managed network access control points.

AC-17(4) – REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS FOR MODERATE AND HIGH SYSTEMS:

1) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: mission or system-specific operational or maintenance needs; and
2) Document the rationale for remote access in the security plan for the system.

AC-18 – WIRELESS ACCESS FOR ALL SYSTEMS:

1) Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
2) Authorize each type of wireless access to the system prior to allowing such connections.

AC-18(1) – WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION FOR MODERATE AND HIGH SYSTEMS:

1) Protect wireless access to the system using authentication of users, devices and encryption.

AC-18(3) – WIRELESS ACCESS | DISABLE WIRELESS NETWORKING FOR MODERATE AND HIGH SYSTEMS:

1) Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

AC-18(4) – WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS FOR HIGH SYSTEMS:

1) Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

AC-18(5) – WIRELESS ACCESS | ANTENNAS AND TRANSMISSION POWER LEVELS FOR HIGH SYSTEMS:

1) Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

AC-19 – ACCESS CONTROL FOR MOBILE DEVICES

FOR ALL SYSTEMS:

1) Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and
2) Authorize the connection of mobile devices to organizational systems.

AC-19(5) – ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION

For Moderate and High Systems:

1) Employ full-device encryption to protect the confidentiality and integrity of information on all EPA mobile devices.

AC-20 – USE OF EXTERNAL SYSTEMS

FOR ALL SYSTEMS:

1) Establish terms and conditions and identify controls asserted to be implemented on external systems via MOU/ISA or contract, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
   a) Access the system from external systems; and
   b) Process, store, or transmit organization-controlled information using external systems; or
2) Prohibit the use of non-government issued or controlled devices except as authorized by the CIO.

AC-20(1) – USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE

FOR MODERATE AND HIGH SYSTEMS:

1) Permit authorized individuals to use an external system to access the system or

to process, store, or transmit organization-controlled information only after:

a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or

b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

AC-20(2) – USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES – RESTRICTED USE

FOR MODERATE AND HIGH SYSTEMS:

1) Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using automated methods to prevent transfer of data, i.e., can access material on a portable device for presentations but not to transfer data from the device or execute any executable file on the device.

AC-21 – INFORMATION SHARING

For Moderate and High Systems:

1) Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for all controlled unclassified information (to include PII, Sensitive PII (SPII) and Confidential Business Information (CBI)) as outlined in MOUs and ISAs as applicable; and

2) Employ automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

AC-22 – PUBLICLY ACCESSIBLE CONTENT

FOR ALL SYSTEMS:

1) Designate individuals authorized to make information publicly accessible;

2) Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

3) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

4) Review the content on the publicly accessible system for nonpublic information at a minimum annually and remove such information, if discovered.

6. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

7. RELATED INFORMATION

- 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. DEFINITIONS

Definitions which pertain to the Information Security – Access Control Procedures are listed below.

- **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.

- **Controlled Unclassified Information** – Sensitive information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies, but is not classified under Executive Order 13526, Classified National Security Information, or the Atomic Energy Act, as amended. CUI is an umbrella term that encompasses many different document

markings to identify information that is not classified but which should be protected. Some past examples of sensitive information you may be familiar with would have been previously marked as:

- Personally Identifiable Information (PII)
- Sensitive Personally Identifiable Information (SPII)
- Confidential Business Information (CBI)
    - Unclassified Controlled Technical Information (UCTI)
    - Sensitive but Unclassified (SBU)
    - For Official Use Only (FOUO)
    - Law Enforcement Sensitive (LES), and others.

- **Device Lock** – Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences.

- **Disabled Accounts** - User accounts that have been placed in a dormant state. The accounts are still active yet require re-verification due to inactivity in order for the user to interact with the system or application.

- **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 (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 non-federal

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.

- **Involuntary Termination** – The employee's departure at the decision of the employer. There are two basic types of involuntary termination, often referred to as being "fired" and "laid off." To be fired, as opposed to being laid off, is generally thought to be the employee's fault and is, therefore, typically considered to be dishonorable and a sign of failure. Being laid off is a result of an organization's strategic, operational or financial decision and such a decision usually affects multiple employees through no fault of their own.
  - **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 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); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles.
- **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).
- **Significant Change** – A change that is likely to substantively affect the security or privacy posture of a system.
- **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.).
- **Voluntary Termination** – A decision made by the employee to leave the job. Such a decision is commonly known as "resignation," "quitting," "leaving" or "giving notice."
- **Written** (or in writing) – To officially document the action or decision, either manually or electronically, and includes a signature.

9. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls

that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

10. DIRECTIVE(S) SUPERSEDED

This Access Control Procedure supersedes Information Directive – Information Security – Access Control Procedure, CIO 2150-P-01.3, June 8, 2023.

11. CONTACTS

For further information, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP).

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2025.03.24 09:04:12 -04'00'

Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management