EPA **INFORMATION**
PROCEDURE

Information Security – Awareness and Training Procedures	
EPA Classification No.: CIO 2150-P-02.2	CIO Approval Date: 02/16/2016
CIO Transmittal No.: 16-006	Review Date: 02/16/2019

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

INFORMATION SECURITY –
AWARENESS AND TRAINING PROCEDURES

1. PURPOSE

To implement the security control requirements for the Awareness and Training (AT) control 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 information and information systems 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 operation 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 must 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 family of Awareness and Training controls.

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 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal Information Resources,” November 2000
- 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
- EPA Contracts Management Manual
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO Policy Framework and Numbering System

6. PROCEDURES

The "AT" designator identified in each procedure represents the NIST-specified identifier for the Awareness and Training control family, 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.

AT-2 – Security Awareness Training

For All Information Systems:

1) The Senior Agency Information Security Officer (SAISO), in coordination with Information Security Officers (ISO) for EPA-operated systems, shall; and Service Managers (SM), in coordination with the SAISO and ISOs, for systems operated on behalf of the EPA, shall ensure service providers:

   a) Develop, maintain and manage the EPA’s security awareness program to ensure users receive adequate training and user awareness content.

i) The content of the basic information system security awareness training materials and security awareness techniques shall be determined based on specific requirements of the organization, federal regulations and the information systems to which personnel have authorized access.

(1) The content of EPA's security awareness program must include:

(a) A basic understanding of the need for information security.

(b) User actions to maintain security.

(c) User actions to respond to suspected security incidents[1].

(d) Awareness of the need for operations security as it relates to the EPA's information security program.

2) System Owners (SO), in coordination with ISOs, Information Management Officers (IMO), Information Owners (IO), Managers and Supervisors and the SAISO for EPA-operated systems, shall; and SMs, in coordination with IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Provide all EPA information system users (including managers, senior executive staff and contractors[2]) information system security awareness training for their respective systems as determined necessary to supplement the mandated awareness training provided by the SAISO:

i) As part of initial training for new users and before authorizing access to the system.

ii) When required by system changes.

iii) At least annually thereafter.

b) Ensure training is completed before information system users are permitted access to an information system or able to perform assigned duties. If the user fails to comply, user access shall be suspended.

c) Ensure each Program Office, Region and Lab augments security awareness training by mechanisms (e.g., "message of the day," posters, special events, email notices) it deems necessary to address local or programmatic information security issues, incidents, policies and procedures.

Note: Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages and conducting information security awareness events.

AT-2(1) – Security Awareness Training | Practical Exercises

Not selected as part of the control baseline.

[1] *Refer to the latest version of the EPA Information Security – Incident Response Procedures for requirements on responding to security incidents.*

[2] *Training or instruction for contractors should be identified or described in the Statement of Work (SOW) or Performance Work Statement (PWS). Refer to the latest version of the EPA Information Security – System and Services Acquisition (SA) Procedures for requirements on contractor training.*

AT-2(2) – Security Awareness Training | Insider Threat

For Moderate and High Information Systems:

1) The SAISO, in coordination with the EPA Office of Homeland Security (OHS), ISOs, IMOs, IOs and Managers and Supervisors, for EPA-operated systems, shall; and SMs, in coordination with the SAISO, OHS, IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Include security awareness training on recognizing and reporting potential indicators of insider threat.
        i) Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence and other serious violations of organizational policies, procedures, directives, rules, or practices.

AT-3 – Role-Based Security Training

For All Information Systems:

1) The SAISO, in coordination with SOs, ISOs, IMOs, IOs, Managers and Supervisors, for EPA-operated systems, shall; and SMs, in coordination with the SAISO, IOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Develop and maintain role based training, education and credentialing requirements to ensure EPA employees and contractors[3] designated as having significant information security responsibilities receive adequate training with respect to such responsibilities. Responsibilities include:
        i) Making final determination for acceptability of training to meet role based training, education and credentialing requirements.
        ii) Making final determination for acceptability of credentials (e.g., (ISC)^2, ISACA, SANS, NSA IEM, etc.) to meet role based credentialing requirements.
    b) Provide role-based security-related training to all personnel with assigned security roles and responsibilities:
        i) Before authorizing access to the system or before users perform assigned duties.
        ii) When required by system changes.
        iii) At least annually thereafter.
    c) Ensure role-based training is completed before information system users are permitted access to an information system or able to perform assigned duties. If the user fails to comply, user access shall be suspended.

[3] *Training or instruction for contractors should be identified or described in the SOW or PWS. Refer to the latest version of the EPA Information Security – System and Services Acquisition (SA) Procedures for requirements on contractor training.*

d) Ensure ISOs identify all individuals requiring role-based security-related training within their respective program offices or regions.

e) Ensure managers and supervisors make certain that all users shall, on an annual basis, complete the training hours as specified by the SAISO in the Role Based Training Program.

f) Ensure all users who have already completed information system security training and who are appointed to a new position that requires additional role-based security training complete the relevant training within 60 calendar days of appointment.

g) Structure content of role-based security training on assigned roles and responsibilities and the specific requirements of the EPA and the information systems to which personnel have authorized access.

   i) Training shall address management, operational and technical roles and responsibilities covering physical, personnel and technical safeguards and countermeasures.

   ii) Supervisors and Managers shall provide the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program.

   iii) Security training shall be consistent with requirements contained in 5 C.F.R. Part 930.301, guidance from NIST SP 800-16, *Information Technology Security Training Requirements: A Role-and Performance-Based Model* and NIST SP 800-50, *Building an Information Technology Security Awareness Training program*.

   iv) SOs shall develop Agency-specific certification courses for the administrative functions for each technology platform (e.g., Oracle, UNIX, Windows) as necessary to administer the technology in accordance with unique Agency requirements. These certification courses shall not duplicate or replace commercial training certifications or courses designed to provide certification or instruction on vendor or industry operational or administrative practices for technology.

   v) Individuals assigned administrative functions shall satisfactorily complete applicable certification courses prior to assuming unsupervised administrator duties.

   vi) Security training content shall be obtained from the most economical and relevant sources. Relevant sources include, but are not limited to, the following:

      (1) A security-training provider in accordance with the Information Systems Security Line of Business.

      (2) Content that is developed or provided in-house.

      (3) Another governmental agency.

      (4) Commercial vendors.

AT-3(1) – Role-Based Security Training | Environmental Controls

Not selected as part of the control baseline.

AT-3(2) – Role-Based Security Training | Physical Security Controls

Not selected as part of the control baseline.

AT-3(3) – Role-Based Security Training | Practical Exercises

Not selected as part of the control baseline.

AT-3(4) – Role-Based Security Training | Suspicious Communications and Anomalous System Behavior

Not selected as part of the control baseline.

AT-4 – Security Training Records

For All Information Systems:

1) Supervisors and Managers, in coordination with the SAISO, SOs, ISOs, IMOs and IOs, for EPA-operated systems, shall; and SMs, in coordination with the SAISO, IOs, SOs, ISOs and IMOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Document and monitor individual information system security awareness and training activities and records as required in accordance with federal regulations and EPA's policies and procedures.
        i) Records shall consist of certificates of completion signed by the training provider, the trainee's Manager or Supervisor, the ISO, or IMO or other similar electronic or manual mechanism. Record of completion can be accomplished electronically via a learning management system.
        ii) Supervisors, Managers and ISOs shall track the status of awareness and training progress and completion at least every 30 calendar days, then no less than weekly within 60 calendar days of the deadline for the annual FISMA report.
        iii) Reports of the status of all users' training must be made available to supervisors, SOs and Senior Information Officials (SIO), as needed, at a minimum weekly prior to the deadline for the annual FISMA report.
        iv) Each Program Office and Region shall report on the status of employees' training activities at the end of the fiscal year to the SAISO of the EPA, as required by the annual FISMA reporting requirement.
        v) EPA employees shall include security awareness training, including any role-based security-related training, in their Individual Development Plans (IDP) annually.
    b) Retain individual training records for a minimum of seven (7) years.
        i) Utilize Skillport as the System of Record for individual employee training records.

AT-5 – Contacts with Security Groups and Associations

Incorporated into PM-15.

7. RELATED DOCUMENTS

- NIST Special Publications, 800 series

- 5 C.F.R. Part 930.301

8. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

1) The CIO has the following responsibilities with respect to awareness and training:
   a) Establish overall strategy for the IT security awareness and training program.
   b) Ensure that the Agency head, senior managers, system and data owners and others understand the concepts and strategy of the security awareness and training program and are informed of the progress of the program's implementation.
   c) Ensure that an Agency-wide IT security program is implemented, is well supported by resources and budget and is effective.
   d) Ensure that the Agency has enough personnel with significant security responsibilities and that they are sufficiently trained to protect its IT resources.
   e) Ensure the role-based security training of Agency personnel.
   f) Ensure that all users are sufficiently trained in their security responsibilities.
   g) Ensure that effective tracking and reporting mechanisms are in place.

Director, Office of Technology Operations and Planning (OTOP)

1) The Director, OTOP has the following responsibilities with respect to awareness and training:
   a) Provide security awareness and role-based training delivery mechanisms and related support.

EPA Administrator

1) EPA Administrator has the following responsibilities with respect to awareness and training:
   a) Ensure that an Agency-wide IT security program is implemented, well supported by resources and budget and is effective.
   b) Ensure that the Agency has enough sufficiently trained personnel to protect its IT resources.

Information Management Officers (IMO)

1) IMOs have the following responsibilities with respect to awareness and training:
   a) Ensure all EPA information and information system users within their organizations successfully complete information security awareness training prior to initial access to EPA systems and information and at least annually thereafter to maintain access.
   b) Ensure all EPA employees designated as having significant information security responsibilities complete role based information security training as defined under the EPA Information Security Program.

Information Owners (IO)

1) IOs have the following responsibilities with respect to awareness and training:

a) Approve and provide information to SOs, common control providers, service managers and service providers on who has access (and with what types of privileges or access rights) and ensure system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior) for assigned systems.

Information Security Officers (ISO)

1) ISOs have the following responsibilities with respect to awareness and training:
   a) Ensure all EPA information and information system users within their organizations successfully complete information security awareness training prior to initial access to EPA systems and information and at least annually thereafter to maintain access. Ensure access is removed for users who do not successfully complete awareness training.
   b) Ensure all EPA employees designated as having significant information security responsibilities complete role-based information security training and credentialing, as defined under the EPA Information Security Program.
   c) Determine the acceptability of training to meet role-based training, education and credentialing requirements in accordance with information security training and education program requirements. Refer to the SAISO for final determination as necessary.

Managers and Supervisors

1) Managers and Supervisors have the following responsibilities with respect to awareness and training:
   a) Work with the CIO and IT security program manager to meet shared responsibilities.
   b) Serve in the role of SO and IO, where applicable.
   c) Augment awareness and training as necessary for the specific security issues of the information or information system.
   d) Ensure users and operational personnel receive role-based security training and awareness.
   e) Ensure IDPs include required training and awareness, especially for users in roles with significant security responsibilities.
   f) Promote the professional development and certification of the IT security program staff, full-time or part-time security officers and others with significant security responsibilities.
   g) Ensure that all users (including contractors, grantees, etc.) of their systems are role-based security trained in how to fulfill their security responsibilities before allowing them access to information systems.
   h) Ensure that users (including contractors, grantees, etc.) understand specific rules of each system and application they use.
   i) Work to reduce errors and omissions by users due to lack of awareness and/or training.

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to awareness and training:
   a) Complete basic information system security awareness materials as part of initial training for new users.
   b) Develop and maintain role based training, education and credentialing requirements to ensure personnel with significant information security responsibilities receive adequate training with respect to such responsibilities.
      i) Make final determination for acceptability of training to meet role based training, education and credentialing requirements.
      ii) Make final determination for acceptability of credentials to meet role based credentialing requirements.
   c) Develop and manage the user awareness program and develop and maintain user awareness content.
   d) Coordinate with the Director, Office of Technology Operations and Planning (OTOP) in delivering awareness, training, education and National Rules of Behavior (NROB) content and tracking completion.

Service Managers (SM)

1) The SMs have the following responsibilities with respect to awareness and training:
   a) Coordinate with information owners for deciding who has access to the service (and with what types of privileges or access rights) and ensuring service users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

System Owner (SO)

1) The SOs have the following responsibilities with respect to awareness and training:
   a) Decide who has access to the system (and with what types of privileges or access rights).
   b) Ensure that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

EPA Employees Designated As Having Significant Information Security Responsibilities

1) EPA employees designated as having significant information security responsibilities have the following responsibilities with respect to awareness and training:
   a) Complete role-based information security training and credentialing as defined under the EPA Information Security Program.

EPA Information and Information System Users

1) EPA Information and Information system users have the following responsibilities with respect to awareness and training:
   a) Complete basic information system security awareness materials as part of initial training for new users, when required by system changes, and annually thereafter.
   b) Complete role-based security training within 60 calendar days of appointment to a new position that requires additional role-specific training.

c) Include security awareness training, including any role-specific training, in their IDPs annually.

9. DEFINITIONS

- *Assessment* – See Security Control Assessment.
- *Authorization* – The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations and the Nation based on the implementation of an agreed upon set of security controls.
- *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 the EPA's intranet boundary.
- *Incident* – an occurrence that actually or potentially jeopardizes the confidentiality, integrity; or availability of an information system or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- *Information* – an instance of an information type.
- *Information Security* – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.
- *Information Security Policy* – an aggregate of directives, regulations, rules and practices that prescribe how an organization manages, protects and distributes information.
- *Information System* – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- *Organization* – a federal agency or, as appropriate, any of its operational elements.
- *Records* – the recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (e.g., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
- *Security Control Assessment* – The testing and/or evaluation of the management, operational and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.
- *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 and performed by service provider personnel. The system may be operated within or externally to EPA's intranet boundary.
- *Threat* – Any circumstance or event with the potential to adversely impact Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.
- *User* – individual or (system) process authorized to access an information system.
- *Vulnerability* – weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.
- *Written* (or in writing) – means to officially document the action or decision, either manually or electronically and includes a signature.

10. WAIVERS

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

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

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

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

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

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.

12. MATERIAL SUPERSEDED

EPA Information Procedure: CIO 2150-P-02.1, *Interim Information Security – Awareness and Training Procedures*, July 18, 2012.

13. ADDITIONAL INFORMATION

N/A

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

APPENDIX A: ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
IDP	Individual Development Plan
IMO	Information Management Officer
IO	Information Owner/Steward
ISO	Information Security Officer
IT	Information Technology
IV&V	Independent Verification and Validation
NIST	National Institute of Standards and Technology
NROB	National Rules of Behavior
OEI	Office of Environmental Information
OHS	Office of Homeland Security (OHS)
OMB	Office of Management and Budget
OTOP	Office of Technology and Operations Planning
PARS	Performance Appraisal and Recognition System
PWS	Performance Work Statement
SAISO	Senior Agency Information Security Officer
SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SOW	Statement of Work
SP	Special Publication
USC	United States Code