INFORMATION PROCEDURE

Information Security - National Rules of Behavior	
EPA Classification No.: CIO 2150-P-21.0	CIO Approval Date: 9/14/15
CIO Transmittal No.: 15-014	Review Date: 9/14/18

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

INFORMATION SECURITY – NATIONAL RULES OF BEHAVIOR

1. PURPOSE

To establish the EPA National Rules of Behavior (NRoB) to comply with OMB Circular A-130, Appendix III, paragraph 3(a(2)(a) regarding rules of behavior for users of information systems applicable to all users of EPA information and information systems for Agency users and to safeguard EPA information and information systems from misuse, abuse, loss, or unauthorized access.

2. SCOPE AND APPLICABILITY

The procedure covers use of all EPA information and information systems to include information and information systems used, managed, or operated by EPA employees, contractors, another agency or other organization on behalf of the agency. The EPA NRoB apply to all EPA employees, contractors, and all other users of EPA information and information systems.

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 EPA.

4. BACKGROUND

The Office of Management and Budget (OMB) Circular A-130, Appendix III, paragraph 3(a(2)(a) requires that all Federal agencies promulgate rules of behavior that "clearly delineate responsibilities and expected behavior of all individuals with access" to the agencies' information and information systems, as well as state clearly the "consequences of behavior not consistent" with the rules of behavior.

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 (FISMA) of 2014, Public Law Public Law No: 113-283 (12/18/2014) (To amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security.)
- Appendix III "Security of Federal Automated Information Resources," to OMB Circular A-130,"Management of Federal Information Resources"
- Executive Order 13103, "Computer Software Piracy"

- OMB Memorandum 06-19 "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"
- OMB Memorandum 08-21 "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- CIO 2101.0 Limited Personal Use of Government Office Equipment Policy
- CIO 2151.0, Privacy Policy
- CIO 2151-P-03.1, Procedures for Preparing and Publishing Privacy Act Systems of Records Notices

6. PROCEDURES

The following are the NRoB for the protection of information and information systems. Appendix A includes a listing of abbreviations and acronyms.

RULES OF BEHAVIOR

Users must acknowledge their knowledge and understanding of responsibilities as well as the EPA NRoB when using EPA information and information systems before being granted access to any government system. The acknowledgement statement is at the end of the annual information security awareness course and on the EPA Information Security website.

Individual systems may require separate acknowledgement of additional rules depending on the nature of the system and of the information processed by that system. In such cases, users are required to acknowledge that they will abide by system-specific rules in addition to these NRoB as a condition of gaining and retaining access to the system.

Violation of these rules will be reported to the user's Program or Regional Office Information Security Officer (ISO) and the Computer Security Incident Response Center (CSIRC). Non-compliance with these rules may subject the user to disciplinary action, as well as penalties and sanctions, including verbal or written warning, removal of system access privileges, reassignment to other duties, removal from Federal service, and/or civil or criminal prosecution depending on the severity of the violation.

Unauthorized access, use, misuse, or modification of government computer systems constitutes a violation of Title 18, United States Code, Section 1030.

System Access and Use

Preventing unauthorized access to EPA information systems and information requires the full cooperation of all users. Users must be aware of their responsibilities for maintaining effective access controls, particularly regarding the use of identification and authentication information and strict adherence to the permissions granted to them.

The following NRoB are relevant to EPA system access and use. Users must:

- Understand they have no expectation of privacy regarding any communications or data transiting or stored on EPA information systems, that information is the property of the Government and may become an official record.
- Be aware that at any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on EPA information systems.
- Use Government furnished equipment (GFE) for work-related purposes only, except as allowed by EPA telework policy and as prescribed by CIO 2101.0 Policy on Limited Personal Use of Government Office Equipment.
- Adhere to all Federal laws, EPA information security policies, procedures, standards and other directives.
- Limit personal use of the Internet and email in accordance with CIO 2101.0 Policy on Limited Personal Use of Government Office Equipment.
- Be responsible for all actions performed and activities initiated using his or her user account.
- Use only authorized and authorized devices and solutions when traveling internationally.
- Access and use only information or information systems for which he or she has been granted access by official authorization and for which access is required for the user's job function.
- Report inappropriate access to the Program or Regional Office ISO or the EPA Call Center.
- Follow established procedures for accessing information, including the use of user identification (ID), authentication information (e.g., personal identification numbers, passwords, digital certificates), and other physical and logical safeguards.
- Follow established procedures for requesting and disseminating information.
- Ensure all sensitive information is protected in a manner that prevents unauthorized personnel from having visual access to the information being processed. This may be accomplished by utilizing devices such as monitor privacy screens, hoods, or positioning equipment (monitors or printers) so that it faces away from doorways, windows, or open areas.
- Terminate sessions or employ a session-locking mechanism before leaving equipment unattended.

- Terminate sessions and log off of all information systems at the conclusion of the work day unless a specific need requires remaining logged on, e.g., system maintenance or incident response.

Users must not:

- Allow anyone to use their system or application account.
- Use EPA information or information systems to conduct or support a personal business.
- Place unauthorized software onto an EPA computing resource.
- Install peer-to-peer (P2P) software on EPA computers without explicit written approval of the Authorizing Official (AO) – generally the CIO.
- Use any computing resources to process, store, or transmit EPA information unless such use has been authorized.
- Connect any computing device or resource to any EPA system, including infrastructure systems, without Senior Information Official (SIO) or CIO authorization.
- Divulge access information (e.g., login procedures, lists of user accounts) for an unauthorized computing resource to anyone who does not have a “need to know” the information as determined by EPA management.
- Capture copies of security or configuration information from a computing resource for the purpose of unauthorized personal use or with the intention of divulging the information to anyone without a specific need to know as determined by EPA management.
- Leave an open login session unattended. The user shall lock the user interface to the session in such fashion that the user must identify and authenticate to regain access to the session.
- Bypass or attempt to bypass system controls or access data for any reason other than official duties.
- Use Internet, email and social media for fraudulent or harassing messages or for sexual remarks or the downloading of illegal or inappropriate materials (e.g., pornography) in accordance with CIO 2101.0 Policy on Limited Personal Use of Government Office Equipment and CIO 2184.0 Social Media Policy.

Identification and Authentication

Identification is the process by which a person, device, or program is differentiated from all others. User identification is commonly provided in the form of User-IDs, but is also provided using other methods, such as digital certificates.

Authentication is the process by which user identification is verified. Authentication can be performed using passwords, cryptographic keys, digital certificates, biometrics, access cards, tokens, or other methods.

To protect access to computing resources users must:

- Protect authentication information from disclosure at a level comparable to the most sensitive level of information on the most sensitive system accessible to the user's access rights once authenticated.
- Change authentication information immediately in the event of suspected or known compromise.
- Select and use unique authentication information for each computing resource or group of computing resources using discrete authentication objects.
- Notify the EPA Call Center when experiencing difficulties with user account or authentication information.
- Report any suspected or known authentication information (e.g., password, digital certificate) compromise to the Program or Regional Office ISO, system Information System Security Officer (ISSO), and to the EPA Call Center at 1-866-411-4-EPA (4372) or epacallcenter@epa.gov.
- Construct and maintain passwords in accordance with CIO 2150-P-02.1 Identification and Authentication Procedures document.

Users must not:

- Allow anyone else to know or use their identification and authentication information to access an EPA information system.
- Attempt to bypass or circumvent access controls to a computing resource.
- Store authentication information in writing, on-line (including password saving features of operating systems and applications, such as auto-fill), or in password storage systems (e.g., "password wallets" or "password safes") unless approved/authorized and/or provided by the EPA.
- Use the same authentication information for EPA system access and non-EPA purposes.

Electronic Data Protection

The user is responsible for protecting the confidentiality, integrity and availability of EPA information. Storage, disposal, mailing and electronic transmission of sensitive information shall be in accordance with Federal and EPA policies and directives. Users shall not create or maintain a System of Records (SoR or SOR) which contains information subject to the Privacy Act (e.g., files containing information related to individuals retrievable by name and/or other unique personal identifier) on an EPA system without approval of the EPA System Owner AND proper preannouncement of the SOR via a System Of Records Notice (SORN) published in the Federal Register (please consult the Agency Privacy officer and CIO policy CIO 2151-P-03.1 for assistance). Users shall protect controlled unclassified information (CUI) in accordance with EPA directives. Within EPA, CUI categories include Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII).

Personally Identifiable Information (PII). Per OMB M-06-19 (July 12, 2006), "the term Personally Identifiable Information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."

Sensitive Personally Identifiable Information (SPII). SPII is a subset of PII, which, if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience or unfairness to an individual. At EPA, SPII is defined as social security numbers or comparable identification numbers, financial information associated with individuals and medical information associated with individuals. SPII requires additional levels of security controls (see EPA Information Security – Privacy Procedures).

The Privacy Act protects personal information collected for entry into a system of records and information that is contained in a Privacy Act System of Records.

To protect PII, users shall comply with the CIO 2151.0 Privacy Policy:

- Ensure that PII retrieved by an individual's name or other personal identifier is maintained in an authorized system of records for which a Privacy Act SORN has been published in the Federal Register.
    - If Sensitive PII is being collected ensure you have the legal authority to do so and ensure a SORN was published before the system became active describing the information.
- PII in electronic form should only be accessed via EPA-authorized computing resources such as EPA provided desktop and laptop computers If SPII must be emailed, ensure it is within an encrypted attachment using EPA authorized encryption standards and the password provided separately (e.g. by phone, another email, or in person).
    - PII data-at-rest on EPA-authorized removable storage media (USB flash drives, external disk drives, etc.), desktop/laptop computer hard drives (or solid state equivalents thereof) shall be encrypted using EPA authorized encryption standards1.
- Use authentication information protection and where possible, automatically lock out after 15 minutes (or less) of user inactivity all mobile computing resources on which PII is stored.
- Identify files, extracts or outputs that contain PII and delete those that no longer serve a business purpose.
- Disseminate PII only to those EPA employees who have a "need to know" to perform their official duties, not a "want to know."

[1] Department of Homeland Security (DHS) threshold for encryption is: All user data is encrypted with FIPS 140-2-validated cryptographic modules, or modules approved for classified data.

- Maintain PII in a manner that will ensure no inadvertent or unauthorized disclosures occur:
  - Do not leave in open view of others;
  - Use an opaque envelope when transmitting through the mail;
  - Secure paper records in a locked file drawer and electronic records in a password protected or restricted access file; and
  - Do not place or store PII on a shared network drive unless access controls are enforced.
- Ensure disposition complies with EPA records disposition schedules.
- Dispose of PII using sensitive waste disposal methods.

Users shall not:

- Remove electronic EPA data (including PII) from EPA controlled spaces unless it is appropriately protected, utilizing EPA authorized and provided cryptographic methods.
- Use personal computing resources for processing, transmitting, or storing PII pertaining to EPA official business.
- Email or otherwise transmit PII outside of the EPA's infrastructure, except when authorized and necessary to conduct official agency business. Emailing PII within the EPA local area network (LAN) or wide area network (WAN) is acceptable, including to and from all mobile devices that interact within the EPA's email system. Emailing PII to personal email accounts (e.g., Gmail, Hotmail, Yahoo, etc.) is prohibited.
- Leave SPII in hard copy unattended and unsecured.

Use of Software

Users shall abide by CIO 2104.1 Software Management and Piracy Policy, Executive Order 13103 and U.S. copyright laws when using EPA systems, and shall not acquire, install, reproduce, distribute, or transmit computer software in violation of these and other applicable directives and the applicable software license.

Teleworking

When authorized to telework from home or from other alternate workplaces users shall:

- Use GFE for work-related purposes only, except as allowed by EPA telework guidance and as prescribed by CIO 2101.0 Policy on Limited Personal Use of Government Office Equipment.
- Use only EPA-authorized technologies for remote access to the EPA network as prescribed by control AC-17 – Remote Access in the most current version of CIO 2150 P 01.2 Access Control Procedure.
- Follow security practices that are the same as or equivalent to those required at his or her primary workplace when teleworking from an alternate workplace.

- Secure or physically protect all computing resources when they are not in use.
- Protect sensitive data at his or her alternate workplace, including proper disposal of sensitive information (e.g., shredding using authorized shredders).
- Protect PII by using only EPA-authorized removable storage media (USB flash drives, external disk drives, SATA disk drives), desktop/laptop computer hard drives (or solid state equivalents thereof) encrypted using EPA authorized encryption standards.
- To access and use Sensitive PII (SPII) remotely, first obtain written permission from the Senior Information Official (SIO). If a request is approved, follow the procedures as prescribed by CIO 2101.0 Limited Personal Use of Government Office Equipment Policy.

Authorized and EPA Sponsored Social Media Representation

When an Authorized EPA user creates an official EPA-sponsored social media site or account; or posts in an official capacity on behalf of the EPA; the user shall:

- Receive approval from the Administrator's Office (Office of Web Communications) before posting.
- Initiate and maintain the profiles and access controls necessary to fulfill their designated representation responsibilities, such as registering for a forum in order to post information, according to their office's social media guidance.

When establishing accounts/profiles for EPA authorized and sponsored social media representation:

- Ensure the profile complies with EPA information security policy, procedures, standards, and guidance.
- Ensure the user's username is not an EPA LAN account username, does not reflect personal information about the user, and is authorized by an Office Director.
- Ensure the profile information, such as the user's biography, is authorized by the user's Office Director and that it reflects EPA-relevant information that is not sensitive.
- Ensure the profile is linked to the user's EPA email account (e.g., doe.john@epa.gov) and not to a personal account (e.g. Gmail, Hotmail, Yahoo, etc.).
- Ensure the authorized EPA accounts/profiles are restricted to EPA employee work and office-related information only, and no personal information, including PII, is included.
- Ensure the authorized EPA profile displays only images authorized by the user's Office Director.

Protection of Computing Resources

Users of EPA computing resources that process EPA information or connect to EPA systems shall:

- Use only EPA furnished computing resources (or authorized personally owned equipment) to access EPA systems and information.

- If using authorized but non-GFE, implement security controls as directed by EPA policy, procedures, standards and guidance.
- Maintain physical control of EPA computing resources at all times and take all necessary precautions for their protection against loss, theft, damage, abuse, or unauthorized use, which includes but is not limited to, employing lockable cases and keyboards, locking cables, and encrypted removable media drives.
- Keep operating system, antivirus, application, and firewall software on the computing resources up to date.
- Use only EPA-authorized Internet connections that conform to EPA security and communications standards (i.e., avoid using connections of unknown or questionable security, such as "public" wireless networks at restaurants, coffee shops, conference centers, parks, etc.).

Users shall not:

- Make any changes to an EPA computing resource system configuration unless directed to do so by an authorized EPA system administrator.
- Use wireless solutions and configurations that are not configured in accordance with the CIO's technical standards and specifically authorized by the SIO.
- Process, store, or transmit sensitive information on wireless devices unless encrypted using EPA authorized encryption methods.

Information Technology Incident Reporting

Users must be vigilant for questionable activities or behavior that may indicate that an information security incident is in progress. Users must address suspicious email activity, including spam, phishing or email originating from unknown sources and mass emails (i.e., emails with empty TO: addresses or very large numbers of TO: addressees) by opening a security incident with the EPA Call Center, (866) 411-4372 (866 411-4EPA) option 1, without opening the email or its attachments and without clicking on any links within the email.

Users must report actual and suspected incidents immediately to the EPA Call Center at 1-866-411-4-EPA (4372) (press 1 for Security). Examples of incidents include:

Email that warrants attention beyond deletion

- Obscene, racist, profane, libelous, or offensive email.
- Email that triggers unexpected computer activity.

Social engineering efforts

- Intelligence gathering email or phone calls (e.g., unknown persons soliciting personal or information system information).
- Requests for user identification and authentication information.

Unexpected computer activity

- Automatic installation of unknown software.
- Constant disk activity.

Intruders

- Computer use in EPA facilities by unknown or unidentified individuals.

Data loss

- Losses or compromises of PII.
- Losses or compromise of confidential business Information (CBI) or trade secrets.

Situations involving the improper handling or storage of PII must be reported immediately to the EPA Call Center**.**

User Accountability

Unauthorized use of a user account or a computing resource can result in criminal penalties under Section 1030, Title 18, of the United States Code. Users will be held accountable for their access and use of EPA computing resources. Users shall:

- Have no expectation of privacy while using any EPA computing resource including the EPA Internet, Intranet and email services.
- Complete EPA-required security awareness courses, briefings and updates and all mandated training commensurate with their information security responsibilities and roles at the required frequency and before accessing EPA systems.
- Read and understand warning banners and end-user licensing agreements.

Classified Information

Unauthorized disclosure of classified information (whether in print, on a blog, or on websites) does not remove the information's classified status or automatically result in declassification of the information. Classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by EPA employees and contractors, until an appropriate original classification authority declassifies it.

EPA employees and contractors shall never access classified information unless they have:

- Received the appropriate clearance from an appropriate authority.
- Signed an approved nondisclosure agreement.
- Demonstrated a need to know the information, and

- Received training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

This requirement does not restrict employee or contractor access to unclassified, publicly available news reports (and other unclassified material) that may in turn discuss classified material. This is distinguished from access to classified documents available on public websites or otherwise improperly published to the public.

7. RELATED DOCUMENTS

- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS)
- NIST Special Publications, 800 Series
- NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*
- EPA Privacy Act Manual

8. ROLES AND RESPONSIBILITIES

Assistant Administrators, Regional Administrators, and other key officials (e.g., Principal Deputy Assistant Administrators, Deputy Assistant Administrators, Deputy Regional Administrators, Assistant Regional Administrators, and Office Directors)

1) Assistant Administrators, Regional Administrators, and other key officials have the following responsibilities with respect to NRoB:
   a) Enforcing and ensuring the EPA NRoB and additional system specific rules of behavior (RoB), where applicable, are reviewed and signed or acknowledged electronically or manually prior to being granted access to EPA information and information systems and annually thereafter to maintain access.

Computer Security Incident Response Center (CSIRC)

1) The CSIRC has the following responsibilities with respect to NRoB:
   a) Protect the Agency's information assets and network.
   b) Ensure prompt response and documentation of all information technology related privacy and information security incidents.
   c) Ensure threat and incident information is reported, communicated, and used to inform the Agency's information technology security risk management awareness and training, privacy, and physical security management programs.
   d) Define the process by which the Agency responds to computer security-related incidents such as data spillage, computer viruses, unauthorized user activity, and serious software vulnerabilities.
   e) Provide a method to promote computer security awareness of related risks so the Agency is better prepared to handle those incidents and is protected against them.

f) Upon learning of a potential incident, take actions to verify whether an incident actually occurred.

g) Determine the scope and impact of each incident and prioritize actions.

h) Protect the Agency's information assets and network.

i) Work in conjunction with supporting entities to establish tools and resources in anticipation of security incidents and events.

j) Work with the IT maintenance and security communities to make recommendations for securing networks, systems, and applications.

k) Educate ISOs and end users on CSIRC goals and operations.

l) Provide coordination for the Agency computer security incident reporting.

m) Act as EPA's distributor for security advisories that are received from external Computer Emergency Readiness Team (CERT) organizations and that may have a potential impact on Agency computer systems.

n) Take actions to verify whether an incident actually occurred upon learning of a potential incident.

o) Determine the scope (potentially vulnerable target space) and impact of each incident and prioritize response activities.

p) Track all incidents that occur at the EPA.

q) Provide scripts to the EPA Call Center to ensure that potential security events are properly identified, sufficient initial information is obtained for follow-up, and Remedy tickets are properly routed.

r) Ensure that Remedy tickets for actual and potential incidents are:

   i) Updated throughout the incident management life cycle, and

   ii) Made available only to appropriate personnel.

s) Report and coordinate incidents with US-CERT, OIG, OPA, the EPA Physical Security Officer, and EPA Senior Management (e.g., CTO, SAISO), as appropriate.

t) Periodically provide information security reports and updates to US-CERT.

u) Set up an incident support resource that offers assistance and advice to users regarding potential incidents and vulnerabilities and the incident handling/reporting procedures.

v) Manage and coordinate all responses to malicious software incidents.

w) Assist the SAISO in establishing efficient and effective reporting system related to incidents involving EPA information resources.

x) Utilize post-incident analysis to determine if and when additional alerts should be issued to users specifying actions to reduce vulnerabilities exploited during an incident.

y) Assess impacts on EPA's security posture and controls as a result of handling and resolving incidents. Provide lessons learned for System Owners (SO), Information Security Officers (ISOs), Information System Security Officers (ISSOs), Senior Managers and others with recommendations to mitigate weaknesses identified during analysis.

z) Determine and implement specific response actions and escalation protocols for each incident type.

Information Management Officials (IMO)

1) IMOs have the following responsibilities with respect to NRoB:
   a) Enforce and ensure the EPA NRoB and any additional system specific RoB, where applicable, are reviewed and signed or acknowledged electronically or manually by each user prior to being granted access to EPA information and information systems and annually thereafter to maintain access.

Information Owners (IO)

1) IOs have the following responsibilities with respect to NRoB:
   a) Enforce and ensure the EPA NRoB and additional RoB of behavior for particular systems, if established, are signed or acknowledged electronically or manually annually by all information users for information for which the IO is responsible.

Information Security Officer (ISO)

1) ISOs have the following responsibilities with respect to NRoB:
   a) Enforce and ensure the EPA NRoB and additional system specific RoB, where applicable, are reviewed and signed or acknowledged electronically or manually by each user prior to being granted access to EPA information and information systems and annually thereafter to maintain access. Ensure access is removed for users who are not in compliance.

Information System Security Officer (ISSO)

1) ISSOs have the following responsibilities with respect to NRoB:
   a) Support the SIO, SO, SM, IO and ISO in managing and implementing the activities, processes, policies, procedures, control techniques, and other countermeasures identified under the EPA Information Security Program and ensure protection measures are compliant with FISMA and related information security directives for the information, information system, and service assigned.
   b) Serve as a principal advisor on all matters, technical and otherwise, involve the security of information, information systems, or services assigned.
   c) Implement policies, procedures, and control techniques identified in the Agency information security program.

Chief Information Officer (CIO)

1) The CIO has the following responsibilities with respect to NRoB:
   a) Establish the EPA NRoB for appropriate use and protection of the information and information systems that support EPA missions and functions.

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to NRoB:
   a) Develop, maintain, and distribute Agency-wide information security policies, procedures, and control techniques to provide direction for implementing the requirements of the information security program.
   b) Develop and maintain the EPA NRoB for appropriate use and protection of information and information systems that support the EPA missions and functions.
   c) Coordinate with the Director, Office of Technology Operations and Planning (OTOP) in delivering annual awareness training, the EPA NRoB content and tracking user completion of training.

Service Manager (SM)

1) SMs have the following responsibilities with respect to NRoB:
   a) Coordinate with information owners to decide who has access to services along with what types of privileges or access rights are assigned. Ensure service users and support personnel receive the requisite security training (e.g., instruction in RoB).
   b) Coordinate with information owners to determine if additional RoB are needed beyond those provided in the EPA NRoB and Service Providers' RoB for particular services. If additional RoB are needed, SMs will coordinate with information owners to establish and publish the additional RoB.

System Owners (SO)

1) SOs have the following responsibilities with respect to NRoB:
   a) Coordinate with information owners and service managers to determine if any additional RoB are needed beyond those provided in the EPA NRoB for particular systems. If additional RoB are needed, SOs will coordinate with information owners and service managers to establish and publish the additional RoB.

Users

1) Users have the following responsibilities with respect to NRoB:
   a) Comply with CSIRC security notifications immediately upon issue.
   b) Take immediate action to comply with directives from the CIO to mitigate the impact of any potential security risk, respond to a security incident.
   c) Report confirmed or suspected information security incidents and violations to the EPA Call Center and other designated entities.

      EPA CSIRC 1-866-411-4-EPA (4372) (press 1 for security).

   d) Successfully complete information security awareness training prior to initial access to EPA systems and information and at least annually thereafter.
   e) Sign or acknowledge electronically or manually the EPA NRoB, and additional RoB for particular systems if established, annually.

9. DEFINITIONS

- *Access* – means "Ability to make use of any information system (IS) resource.

  Further, *Access* means ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions."
- *Availability* – ensuring timely and reliable access to and use of information.
- *Confidentiality* – preserving restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- *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 System* – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- *Information Technology* (IT) – any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency. For purposes of the preceding sentence, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term Information Technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
- *Integrity* – guarding against improper modification or destruction of information, including ensuring information nonrepudiation and authenticity.
- *Organization* - a federal agency or, as appropriate, any of its operational elements.
- *Need-to-know* – means a determination within the executive branch in accordance with directives issued pursuant to this policy or procedure that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
- *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).
- *User* – individual or (system) process authorized to access an information system.
- *Written* (or in writing) – means to officially document the action or decision, either manually or electronically, and includes a signature.

10. WAIVERS

N/A

11. RELATED PROCEDURES, STANDARDS AND GUIDANCE

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

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

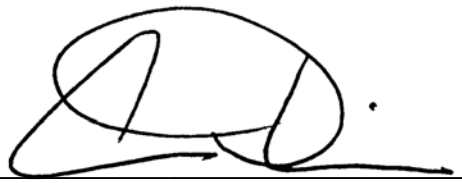
Related standards and guidelines are available on OEI's website.

12. MATERIAL SUPERSEDED

All previously published Rules of Behavior procedure, guidance, and example RoB documents.

13. ADDITIONAL INFORMATION

N/A



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

APPENDIX A: ABBREVIATION & ACRONYMS

AO	Authorizing Official
CAN	Campus Area Network
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Center
CUI	Controlled Unclassified Information
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FR	Federal Register
GFE	Government Furnished Equipment
ID	Identification
IMO	Information Management Official
IO	Information Owner / Steward
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
MAN	Metropolitan Area Network
NIST	National Institute of Standards and Technology
NRoB	National Rules of Behavior
NSI	National Security Information (classified or unclassified information categorized as NSI)
OMB	Office of Management and Budget
OTOP	Office of Technology Operations and Planning
P2P	Peer-to-Peer
PII	Personally Identifiable Information
RoB	Rules of Behavior
SAISO	Senior Agency Information Security Official
SIO	Senior Information Official
SM	Service Manager
SO	System Owner
SOR	System of Records
SORN	System of Records Notice
SP	Special Publication
SPII	Sensitive Personally Identifiable Information
USC	United States Code
WAN	Wide Area Network