Information Security – EPA National Rules of Behavior

1. PURPOSE

Office of Management and Budget (OMB) Circular A-130 requires that all Federal agencies promulgate rules of behavior, "including consequences for violating rules of behavior, for employees and contractors that have access to Federal information or information systems." This includes individuals who create, collect, use, process, store, maintain, disseminate, disclose or dispose of all federal information.

The Environmental Protection Agency (EPA) must ensure that "employees and contractors have read, agreed to, and abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access." The System Owner (SO) shall also ensure all users with access to the information system(s) under the SO's purview read, acknowledge and adhere to the National Rules of Behavior (RoB) and system specific RoB (if deemed applicable) at least annually thereafter.

The purpose of this directive is to establish the EPA National RoB and standards of behavior to comply with OMB Circular A-130 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls regarding rules of behavior applicable for all users of EPA information and information systems and to safeguard EPA information and information systems from misuse, abuse, loss or unauthorized access.

2. SCOPE

This directive applies to the use of all EPA information and EPA information systems used, managed or operated by EPA employees, contractors, other agencies or other organizations on behalf of the Agency. The EPA EPA National RoB applies to all EPA employees, contractors and all other users of EPA information and information systems.

3. AUDIENCE

The EPA National RoB apply to all EPA employees, contractors, temporary personnel, other agencies or other organizations on behalf of the Agency who use EPA information and information systems that support the operations and assets of the EPA (hereinafter "users").

4. AUTHORITY

- Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," July 2016
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020

5. STANDARD

The following are the EPA National RoB for the protection of information and information systems. The Appendix includes a listing of abbreviations and acronyms.

Prior to being granted access to any EPA information systems, users must attest to their knowledge and understanding of their responsibilities and the EPA National RoB. All users with access to the information system(s) under their purview must read, acknowledge and adhere to the EPA National RoB and system-specific RoB (if deemed applicable) at least annually thereafter. The acknowledgement statement is at the end of the annual information security awareness course and on the EPA Information Security website.

Individual information 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 EPA National RoB as a condition of gaining and retaining access to the system. Users can contact their SO or Information Security Officer (ISO) for their system-specific RoB.

Unauthorized access, use, misuse or modification of government computer systems constitutes a violation of Title 18, United States Code, Section 1030. Non-compliance with these rules may subject the user to criminal and/or civil penalties and sanctions; disciplinary action up to removal, an administrative action to deny or revoke the user's eligibility for a national security sensitive position, public trust position, or credential; or other administrative actions as appropriate.

RULES OF BEHAVIOR
As an EPA employee, contractor, temporary personnel, other agencies or other organizations on behalf of the Agency who use EPA information and information systems that support the operations and assets of the EPA, licensee, certificate holder or grantee, I understand that I must adhere to the following Rules of Behavior:

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.

I will:

- Use Government furnished equipment (GFE) and network resources for work-related purposes only, except as allowed by EPA telework policy and as prescribed by CIO 2101.2 Policy on Limited Personal Use of Government Office Equipment.
- Adhere to all Federal laws, EPA information security policies, procedures, standards and other directives.
- Use only authorized devices, software and services to accomplish duties.
- Ensure equipment being transported to or through countries other than the United States is specifically approved in each instance by OISP.
- Access and use only information or information systems for which I have been granted access by official authorization and for which access is required for my job function.

- Report inappropriate access to the Program or Regional Office ISO and the Enterprise IT Service Desk (EISD).
- Follow established procedures for accessing information, including the use of user identification (ID), authentication information (e.g., personal identification numbers, passwords, digital certificates and Multi-Factor Authentication (MFA) devices) and other physical and logical safeguards.
- Follow established procedures for requesting and disseminating information. I will ensure all information gathered and distributed is done so through approved channels.
- Ensure all 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.
- Log out of computers and applications, use the computer screen lock mechanism and remove my Personal Identify Verification (PIV) card to ensure equipment left unattended for any period of time cannot be used unless an employee logs in to it. I will ensure physical equipment such as safes, cabinets, and offices are also secured any time they are left unattended, for any period of time, to prevent unauthorized access. I will terminate sessions and log off of all information systems at the conclusion of the workday unless a specific need requires remaining logged on, e.g., system maintenance or incident response.

I will not:

- Allow anyone to use my system or application account.
- Install and/or download unauthorized software on an EPA computing resource without written approval by the Information Management Office (IMO) and IRM Branch Chief (IRMBC).
- Use any computing resources to process, store or transmit EPA information unless such use has been authorized.
- Connect any non-EPA computing device or resource to any EPA information system, including infrastructure systems, without SIO or Chief Information Officer (CIO) authorization.
- Divulge access information (e.g., login procedures, lists of user accounts) for any authorized computing resource to anyone who does not have a “need to know,” 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. I will 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 EPA policy and procedures.

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, I will:
- 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 resource.
- Notify the EISD 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 EISD at 1-866-411-4-EPA (4372) or eisd@epa.gov.
- Construct and maintain strong passwords in accordance with EPA policy and procedures.

I will not:
- Allow anyone else to know or use my 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, web browsers 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, e.g., password, for EPA information system access that is used for non-EPA information system access.

Electronic Data Protection
The user is responsible for protecting the confidentiality, integrity and availability of EPA information. Storage, disposal, mailing and electronic transmission of information shall be in accordance with Federal directives and EPA policies and procedures. Users shall not create or maintain a data set 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 information system without approval of the EPA Information System Owner and proper preannouncement of the System of Records (SOR) via a System of Records Notice (SORN) published in the Federal Register (please consult the Office of Customer Advocacy, Policy and Portfolio Management (OCAPPM), the Agency Privacy Officer and EPA privacy policy and procedures for assistance). Users shall protect

controlled unclassified information (CUI) in accordance with EPA directives. Within EPA, CUI categories include but are not limited to General Privacy Basic.

Per OMB M-17-12 (January 03, 2017), "the term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the Agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available -in any medium or from any source -that would make it possible to identify an individual."

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, I will comply with the EPA Privacy Policy:

- I will 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, I will ensure I have the legal authority to do so in consultation with the Liaison Privacy Official (LPO) and ensure a SORN was published before the system became active describing the information.
  - I understand that all requests to access SPII from a remote location or taking SPII off site requires SIO approval. I will contact an LPO for additional information.
- I understand that 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 to external to EPA recipients, I will ensure it is within an encrypted attachment using EPA authorized encryption standards[1] and the password provided separately (e.g., by phone, in person, etc.).
  - SPII data-at-rest on only EPA-authorized removable storage media (RSM) (e.g., USB thumb/flash drives, external removable hard drives, solid-state drives) shall be encrypted using EPA authorized encryption standards[2].
- I will destroy physical and electronic copies of PII in accordance with federal requirements/standards when no longer required, and not subject to any legal hold, in

[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.*
[2] *Department of Homeland Security (DHS) threshold for encryption is: All user data is encrypted with FIPS 140-3- validated cryptographic modules, or modules approved for classified data.*

consultation with Records Liaison Officer (RLO) for record retention requirements and LPOs for destruction standards.

- I will disseminate PII or SPII only to those EPA employees who have a "need to know" to perform their official duties, not a "want to know."
- I will maintain PII or SPII in accordance with Federal standards to ensure no inadvertent or unauthorized disclosures occur:
  - I will not leave in open view of others.
  - I will use an opaque envelope when transmitting through the mail.
  - I will secure paper records in a locked file drawer and electronic records in a password protected or restricted access file.
  - I will not place or store PII on a shared network drive unless access controls are enforced.
  - I will ensure that emails containing SPII are encrypted before sending.
  - I will ensure disposition complies with EPA records disposition schedules.
  - I will dispose of PII using sensitive information waste disposal methods.

I will not:

- Remove electronic EPA data (including PII) from EPA controlled spaces unless it is appropriately protected, utilizing EPA authorized and provided cryptographic methods unless approved by the IMO or SIO.
- Use personal computing resources for processing, transmitting, or storing data 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.) or cloud storage spaces (Google Drive, Dropbox, etc.) is prohibited.
- Leave SPII in hard copy unattended and unsecured.

Use of Software

Users shall abide by EPA Software Management and Piracy Policy, Executive Order 13103 and U.S. copyright laws when using EPA information 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 I will:

- Use GFE for work-related purposes only, except as allowed by EPA telework guidance and as prescribed by CIO 2101.2 Policy on Limited Personal Use of Government Office Equipment policy and procedures.

Government Furnished Equipment

I will:

- Use only EPA-authorized technologies for remote access to the EPA network as prescribed by EPA policy and procedures.
- Follow security practices that are the same as or equivalent to those required at my 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 my alternate workplace, including proper disposal of sensitive information (e.g., shredding using authorized shredders).
- Protect EPA information by using only EPA-authorized and registered removable storage media (e.g., 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 SPII remotely, first obtain written permission from the SIO.

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, I will:

- 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, I will:

- Ensure that the profile complies with EPA information security policy, procedures, standards and guidance.
- Ensure that 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 that 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 that 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 that 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 that the authorized EPA profile displays only images authorized by the user's Office Director.

Protection of Computing Resources
As a user of EPA computing resources that process EPA information or connect to EPA information systems, I will:

- Use only EPA-furnished computing resources to access EPA information systems and information.
- If using authorized but non-GFE, implement security controls as directed by EPA policy, procedures, standards, guidance and follow Federal Records Act requirements.
- 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 by applying supplied patches within the allotted timeframe.
- Use only EPA-authorized Internet connections that conform to EPA security and communications standards (e.g., avoid using connections of unknown or questionable

security, such as “public” wireless networks at restaurants, coffee shops, conference centers, parks, etc.).
- Use EPA-authorized Remote Access to connect to the EPA’s network from a remote location using a laptop or desktop computer connected to the internet. The Agency uses a Virtual Private Network (VPN) to securely authenticate the connection.

I will not:
- Make any changes to an EPA computing resource configuration unless directed to do so by an authorized EPA information system administrator.
- Use wireless solutions and configurations that are not configured in accordance with the CIO’s IT/IM Architecture standards.
- 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 communications originating from trusted or unknown sources and mass emails (e.g., emails with empty TO: addresses or very large numbers of TO: addressees) by opening a security incident with the EISD, (866) 411-4372 (866 411-4EPA) option 1, without opening the email or its attachments and without clicking on any links within the email.

I will report actual and suspected incidents immediately to the EISD. 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 or mobile phone (if applicable) activity.
- Automatic installation of unknown software.
- Constant hard drive activity.

Intruders
- Computer use in EPA facilities by unknown or unidentified individuals.
- Data loss.
- Data breach.
- Losses or compromises of PII.
- Losses or compromises of CUI, such as PII, proprietary business information or patent information.

Situations involving the improper handling or storage of CUI, as appropriate, must be reported immediately to the EISD.

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. I will:

- 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 information 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 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. Classified information may never be accessed over the EPA network or an EPA computer.

I understand that 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 for the information.
- 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.

6. ROLES AND RESPONSIBILITIES

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

7. RELATED INFORMATION

- Executive Order 13103, “Computer Software Piracy,” September 1998
- OMB Memorandum M-17-12 “Preparing for and Responding to a Breach of Personally Identifiable Information,” January 2017
- EPA CIO 2101.2, Limited Personal Use of Government Office Equipment Policy
- EPA CIO 2151.1, Privacy Policy

- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures
- EPA CIO 2154.5 EPA Mobile Computing Policy
- EPA CUI Policy CIO 2158.1

8. DEFINITIONS

- **Access** – the "ability to make use of any information system 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.
- **Controlled Unclassified Information (CUI)** – Is information that requires protection according to a law, regulation, or government wide policy that is not otherwise protected by Classified National Security Information (CNSI or Atomic Energy Act of 1954 Requirements.
- **Government Furnished Equipment** – property in the possession of, or directly acquired by, the Government and subsequently furnished to the Contractor for performance of a contract.
- **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.
- **Network resources** – any kind of device, information, or service available across a network.
- **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.

- **Resource** – Passive system-related entity, including devices, files, records, tables, processes, programs, and domains that contain or receive information. Access to an object (by a subject) implies access to the information it contains.
- **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.

9. WAIVERS

N/A

10. DIRECTIVE(S) SUPERSEDED

This procedure supersedes all previously published EPA National RoB procedures, guidance and example RoB documents.

11. CONTACTS

For information about this directive, please contact the Office of Mission Support (OMS), Office of Information Security and Privacy (OISP) at Infosec@epa.gov.

VAUGHN NOGA Digitally signed by VAUGHN NOGA
Date: 2024.04.10 10:31:06 -04'00'

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

APPENDIX A: ACRONYMS & ABBREVIATIONS

CIO	Chief Information Officer
CUI	Controlled Unclassified Information
EISD	Enterprise IT Service Desk
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
GFE	Government Furnished Equipment
ID	Identification
IMO	Information Management Official
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
LPO	Liaison Privacy Official
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OCAPPM	Office of Customer Advocacy, Policy and Portfolio Management
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
OMS	Office of Mission Support
OMS-EI	Office of Mission Support – Environmental Information
PII	Personally Identifiable Information
PIV	Personal Identify Verification
RLO	Records Liaison Officer
RoB	Rules of Behavior
RSM	Removable Storage Media
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
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network