INFORMATION POLICY

Privacy Policy	
EPA Classification No.: CIO 2151.1	CIO Approval Date: 9/14/2015
CIO Transmittal No.: 15-013	Review Date: 9/14/2018

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

PRIVACY POLICY

1. PURPOSE

The Privacy Policy establishes the Environmental Protection Agency's (EPA) requirements for safeguarding personally identifiable information (PII) and Privacy Act information in accordance with the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Management Act (FISMA), and policy and guidance issued by the President and Office of Management and Budget (OMB). PII and Privacy Act information must be protected from unauthorized access during collection, access, use, dissemination and storage. This Policy provides authorization for the National Privacy Program that establishes the processes the Agency will use to govern the Program, informs Agency employees and managers about their roles and responsibilities, and details the consequences for non-compliance with requirements of the Privacy Policy.

2. SCOPE AND APPLICABILITY

This Policy applies to all EPA employees, managers, contractors, and grantees working on behalf of EPA who handle, control, or access documents, records, or information technology (IT) systems that contain PII or Privacy Act information.

3. AUDIENCE

The audience for this Policy includes all EPA employees, managers, contractors, and grantees working on behalf of EPA.

4. BACKGROUND

Various laws and OMB directives as enumerated in Sections 5 and 10 of this document require the protection of PII and Privacy Act information that federal agencies collect. Privacy Act information, a subset of PII, is information about an individual that is retrieved by name or other personal identifier assigned to the individual which has special requirements under the Privacy Act. PII is any information about an individual maintained by an agency that can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual. The Privacy Act of 1974 (5 U.S.C. § 552a) sets forth requirements for federal agencies when they collect, maintain or disseminate Privacy Act information.

Privacy laws also require agencies to establish a Data Integrity Board (DIB) when they need to participate in a computer matching program (i.e., computer comparison of two or more federal (payroll or personnel) systems of records or a system of records to a non-federal system of records). The DIB includes senior officials who oversee the computer matching activity and report on the matching program to OMB. New information technologies have created additional responsibilities for managing personal information. Promoting openness and adopting new technologies have the potential to make devices and data vulnerable to malicious or accidental breaches of security and privacy and create challenges in providing adequate protection and notice. Many other laws, regulations and requirements relate to the managing of

PII by EPA. EPA practices will guard against unauthorized disclosure or misuse of PII in all forms. EPA is committed to ensuring the protection of Privacy Act information and PII as new and amended laws are enacted, OMB guidance is issued, technology changes are made, and agency business needs evolve.

The Agency's initial Privacy Policy, issued by the Chief Information Official (CIO) on September 27, 2007, established agency requirements for safeguarding the collection, access, use, dissemination, and storage of Privacy Act information and PII in accordance with the Privacy Act of 1974, E-Government Act of 2002, FISMA and policy and guidance issued by the President and OMB. It also created the National Privacy Program to ensure agency compliance with privacy requirements. Revisions to this policy address the use of social media sites and mobile devices and incorporate consequences for non-compliance with requirements in this Policy. EPA will use the privacy controls issued by National Institute of Standards and Technology (NIST) Special Publication 800-53 to protect PII and promote a closer relationship with security professionals in implementing and enforcing privacy protection requirements.

5. AUTHORITY

- 5 U.S.C. § 552a - Privacy Act
- E-Government Act of 2002 (Pub.L. 107-347 116 Stat. 2899, 44 U.S.C. § 101)
- 40 C.F.R. Part 16 – Implementation of Privacy Act of 1974, as revised - January 4, 2006
- 48 C.F.R. § 24.1 Federal Acquisition Regulation (FAR), Protection of Individual Privacy
- 48 C.F.R. § 1524.1, EPA Acquisition Regulation (EPAAR), Protection of Individual Privacy
  40 F.R. 28948 – OMB's Privacy Act Implementing Guidelines
- 54 F.R. 25818 – OMB's Computer Matching and Privacy Protection Act Final Guidance
- Delegation of Authority 1-33 Privacy Act
- Federal Information Security Management Act (FISMA) (Pub.L. 107-347, 116 Stat. 2899, 2946-61, 44 U.S.C. § 3541)
- OMB Circular A-130, Appendix I
- OMB 25 Point Implementation Plan to Reform Federal Information Technology
- Presidential Memorandum, Building a 21st Century Digital Government, May 2012
- Fed RAMP Concept of Operations, June 4, 2012
- NIST Publication, 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations"

6. POLICY

It is the policy of the EPA to safeguard an individual's privacy in a manner consistent with the Privacy Act, E-Government Act, OMB directives and other federal directives concerning privacy.

- EPA will safeguard all PII in its possession.
- EPA will limit the collection of PII to only that which is necessary to accomplish an official EPA mission, administrative function, regulatory or statutory requirement, or to comply with OMB or Homeland Security directives concerning privacy.
- EPA will provide a Privacy Act Statement to the individual whose PII is being collected when required by applicable law.
- EPA will not collect or use a social security number as a personal identifier in connection with any information system or database, unless the collection and/or use is authorized by law.
- EPA's Privacy Officer will review all internal EPA forms that collect PII and approve all forms before they are submitted to the EPA Internal Forms Officer for issuance of an EPA form number.

- EPA will not disseminate or publish PII without the prior consent of the individual or unless provided for by law.
- EPA will complete a Privacy Threshold Analysis (PTA) form to determine the need for a Privacy Impact Assessment (PIA). The PIA is a life-cycle document. It must be updated throughout the life cycle of the investment.
- EPA will report as soon as practicable all incidents involving the security, loss, misuse or unauthorized disclosure of PII regardless of form or format in accordance with established EPA, OMB and U.S. Computer Emergency Readiness Team (US-CERT) security incident reporting procedures and requirements.
- EPA will ensure prompt notification to individuals affected by a breach of sensitive PII (i.e., social security numbers, medical or financial information associated with an individual) commensurate with risk of harm to the individuals and consistent with the Agency's breach notification procedures.
- EPA will approve in writing all requests to access sensitive PII from an offsite location or to transport or transmit sensitive PII offsite.
- EPA will employ a risk-based approach to protect PII from unauthorized disclosure and misuse.
- EPA's use of technology will support and not diminish the protections provided in statutes related to the use, collection and disclosure of PII.
- EPA employees, managers, contractors and grantees working on behalf of EPA will safeguard PII and follow Agency procedures when teleworking and using mobile devices and cloud technologies.
- EPA will ensure that no system of records is used in a computer matching agreement (CMA) unless the matching activity is reflected in the system's routine uses and approved by the DIB.
- EPA will comply with applicable federal laws relating to privacy in its social media use.
- EPA's Privacy Officer will review all memoranda of understanding (MOUs), interconnection security agreements and other agreements that cover sharing PII prior to finalizing the agreement.
- EPA employees, managers, contractors and grantees working on behalf of EPA will:
    - Adhere to privacy rules of conduct and may be subject to all applicable penalties under the Privacy Act. Each case will be handled on an individual basis with a full review of all pertinent facts;
    - Comply with the provisions of the Privacy Act and agency regulations and policies pertaining to collecting, accessing, using, disseminating and storing PII and Privacy Act information;
    - Ensure that PII contained in a system of records, to which they have access in the performance of their duties, is protected so that the security and confidentiality of the information are preserved;
    - Not disclose any personal information contained in any system of records or PII collection, except as authorized;
    - Access and use only information for which they have official authorization;
    - Be accountable for their actions and responsibilities related to the information and resources entrusted to them;
    - Protect PII from disclosure to unauthorized individuals;
    - Protect the integrity of PII in their possession;
    - Protect the availability of information and ensure appropriate access levels;
    - Be knowledgeable of PII and Privacy Act policies, requirements and issues;
    - Promptly report breaches of PII, unauthorized disclosures and system vulnerabilities in accordance with Agency policies and procedures; and
    - Be subject to the following consequences for non-compliance:
        - Employees may be subject to disciplinary action for failure to take appropriate action upon discovering a breach or for failure to take required steps to prevent a breach from occurring or re-occurring.

  - Consequences will be commensurate with the level of responsibility, type of PII involved and the severity of the violation. The circumstances, including whether the behavior or action was intentional, will be considered in taking appropriate action. Any action taken must be consistent with law, regulation, applicable case law and any relevant collective bargaining agreement. Consequences can include suspension of access privileges, reprimand, suspension, demotion, removal and criminal and civil penalties, including prison terms and fines.
- EPA will train all managers, supervisors, employees and contractors on their responsibilities, privacy rules of conduct and the consequences for non-compliance.

7. ROLES AND RESPONSIBILITIES

- The **Administrator** has the authority to approve the establishment or amendment of an EPA Privacy Act system of records notice. The Administrator has delegated this authority to the Chief Information Officer (CIO), in the Office of Environmental Information (OEI),

- **Agency Privacy Officer:**
  - Is a senior level staff member designated by the CIO;
  - Develops Agency level privacy policies, procedures, standards, and guidelines, as needed;
  - Provides overall privacy management and policy guidance;
  - Develops, coordinates and implements privacy-related activities and response procedures to be followed in the event of a breach of PII;
  - Publishes Federal Register notices for systems of records as required by the Privacy Act;
  - Reviews and approves PIAs as required by the E-Government Act;
  - Provides leadership and oversight to the network of Liaison Privacy Officials (LPOs);
  - Posts policies and procedures on the Privacy intranet; and notifies agency IMOs and LPOs of new developments in the Privacy Program;
  - Develops mandatory annual training for LPOs;
  - Develops and implements privacy awareness training program for key personnel with privacy responsibilities;
  - Monitors EPA privacy activities, including quality and timeliness of responses to Privacy Act requests;
  - Reviews Systems of Records Notices (SORNs) for publication in the Federal Register;
  - Submits a biennial report to OMB on the Agency's implementation of the computer matching provisions of the Privacy Act, pursuant to Section (u)(6) of the Act;
  - Provides Privacy reporting to the OMB on FISMA, results of on-site reviews, Inspector General audits and other reviews;
  - Reviews and approves forms that collect PII prior to number issuance;
  - Leads Agency efforts to protect PII used for agency operations;
  - Identifies new OMB requirements which require new and or revised policies and procedures;
  - Incorporates new requirements into Agency policies and procedures and implements changes in a timely manner;
  - Provides overall Privacy management and policy guidance;
  - Approves PTAs and PIAs;
  - Monitors the content of the Privacy website and EPA printed publications to ensure that non-public information about EPA employees is protected from public view;
  - Ensures the Agency conducts periodic reviews of the Agency's PII inventory to promptly identify deficiencies, weaknesses or risks;

  - Participates in assessing the impact of technology on the privacy of personal information;
  - Ensures that the Agency takes appropriate steps to remedy identified privacy compliance issues; and
  - Coordinates with the Senior Agency Information Security Officer (SAISO) to ensure that Privacy and Security Policy, Procedures and Guidance are consistent with respect to securing PII.

- **Chief Information Officer (CIO):**
  - Is the designated Senior Agency Official for Privacy (SAOP) in accordance with the E-Government Act and has overall responsibility and accountability for ensuring the Agency's implementation of information privacy protections, including the Agency's full compliance with federal laws, regulations and policies relating to information privacy, such as the Privacy Act;
  - Communicates changes and/or new policies and procedures to Agency Senior Information Officials (SIO) and other senior managers, as appropriate;
  - Approves Agency level privacy policies, procedures, standards and guidelines;
  - Approves the establishment or amendment of EPA Privacy Act systems of records and notices for publication in the Federal Register;
  - Ensures that appropriate changes are made in a timely manner to privacy policies, procedures, standards and guidelines;
  - Ensures the availability of sample cascading goals and objectives for inclusion in performance agreements of employees with privacy responsibilities; and
  - Convenes the DIB to carry out computer matching responsibilities pursuant to the Privacy Act.

- **Chief Privacy Officer**:
  - Is a senior level manager designated by the CIO;
  - Implements the Privacy Program at EPA;
  - Establishes key goals and objectives for the Agency's Privacy Program;
  - Establishes and tracks performance measures associated with the key goals and activities and measures the progress of the Privacy Program;
  - Provides performance measurement reports showing the annual progress of the Agency's Privacy Program to the Senior Agency Official for Privacy and via the website makes the reports available to the EPA offices and regions responsible for implementing the Privacy Program;
  - Performs oversight of the implementation of Agency level privacy policies, procedures, standards and guidelines within the Program and Regional Offices to ensure they are properly executed, consistently applied and effective; and
  - Reports oversight results to the Senior Agency Official for Privacy.

- **EPA employees, managers, contractors and grantees** working on behalf of EPA must:
  - Comply with the provisions of the Privacy Act and EPA Privacy Act regulations and procedures; and
  - Report incidents involving the security, loss, misuse or unauthorized disclosure of Privacy Act information and PII, regardless of form or format, in accordance with Agency incident reporting procedures.

- **Information Management Officials (IMOs):**
  The agency official and organization with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
  - Ensure that privacy policy and procedures are communicated from the SIO to employees in their organizations; and
  - Ensure that privacy requirements are implemented in their organizations.

- **Information Security Officers (ISOs):**
  - Review systems containing PII on a periodic basis to determine if data elements are still required;
  - Terminate systems containing PII when no longer needed (in accordance with proper destruction procedures);
  - Conduct privacy on-site compliance reviews;
  - Ensure systems meet privacy requirements prior to deployment; and
  - Coordinate PII breach response activities, as required.

- **Information System Security Officer (ISSO):**
  - Supports the SIO and ISO in managing and implementing the activities, processes, policies, procedures, control techniques, and other countermeasures identified under the EPA Information Security Program and ensures protection measures are compliant with FISMA and related information security directives for the information, information system, and service assigned.
  - Serves as a principal advisor on all matters, technical and otherwise, involving the security of information, information systems, or services assigned.
  - Implements policies, procedures, and control techniques identified in the Agency information security program.

- **Liaison Privacy Officials (LPOs):**
  - Ensure completion of required training by users and compliance with Agency privacy requirements in their organizations;
  - Administer the day-to-day activities and responsibilities of privacy in their specific program and regional areas;
  - Ensure proper training for individuals in their area of responsibility, including monitoring on-line training for the employees;
  - Complete mandatory annual training for LPOs;
  - Communicate requests for matching program activities;
  - Maintain accurate inventories of organizational systems containing PII and report changes to the inventories to the Agency Privacy Officer;
  - Respond to data calls from the Agency Privacy Officer;
  - Conduct privacy on-site compliance reviews;
  - Support Agency breach responses;
  - Implement privacy procedures when issued by the National Privacy Program Manager; and
  - Assist in preparing privacy documentation (i.e., PTAs, PIAs, SORNs) for new and/or revised systems.

- **Office of Administration & Resources Management (OARM):**
  - Ensures appropriate privacy related language is included in contracts, grants and interagency agreements using the proper Federal Acquisition Regulations and Environmental Protection Agency Acquisition Regulations clauses related to privacy regulations and responsibilities;
  - Reviews and approves sample privacy cascading goals and objectives developed by OEI for inclusion in Performance Agreements of employees with privacy responsibilities to establish accountability;
  - Notifies individuals of Electronic Official Personnel Folder (eOPF) mis-filings in their personnel folder and submits notification reports on mis-filings to the Agency Privacy Officer annually;
    - Participates in computer matching programs, as required;
    - Serves as a member of the DIB; and
    - Supports the Agency's breach response activities.

- **Office of the General Counsel (OGC)**:
  - Interprets the Privacy Act and other privacy-related regulations, statutes and requirements;
  - Provides legal counsel on privacy matters and performs legal reviews on privacy notices, forms, SORNs, Privacy Act statements, regulations, policies and procedures;
  - Issues decisions on written appeals from individuals who request access to Privacy Act information;
  - Serves as a member of the Breach Evaluation Team Executive Committee (BET-EX);
  - Supports the Agency's breach response activities; and
  - Serves on the DIB.

- **Office of the Inspector General (OIG)**:
  - Carries out the appeal responsibilities related to decisions made on OIG Privacy Act records;
  - Participates in computer matching programs as required;
  - Conducts criminal investigations related to a breach or disclosure of sensitive PII when warranted;
  - Supports Agency's breach response activities; and
  - Serves on the DIB.

- **Office of Information Analysis and Access (OIAA):**
  - Ensures social media policies and procedures include PII protections.

- **Office of Public Affairs (OPA)**:
  - Protects Privacy Act information and PII by monitoring the content of EPA's website, printed publications and other EPA information media; and
  - Participates in the response to breaches of PII as appropriate.

- **Quality and Information Council (QIC)**:
  - Addresses enterprise-wide issues and reviews Agency policies to guide EPA decision makers in the area of information technology/information management and related issues within the framework of the OEI.
  - Privacy policy and procedures are reviewed through the QIC process.

- **Quality and Information Council (QIC) Steering Committee (SC):**
  - Supports the QIC in providing input, consultation and recommendations for information technology and information management related privacy policies and procedures.

- **Senior Agency Information Security Officer (SAISO):**
  - Supports privacy through security policies, procedures and controls;
  - Assists in recommending and developing appropriate technical solutions to protect the privacy information collected or maintained within IT systems;
  - Supports activities in response to technical breaches of PII; and
  - Compiles and submits the FISMA report for the Agency to OMB.

- **Senior Information Officials (SIOs)**:

  The agency official and organization responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.
  - Monitor and perform oversight of the implementation of the program or regional privacy policies and procedures to ensure they are properly executed, consistently applied, and effective;
  - Make appropriate changes in a timely manner to program or regional privacy procedures based on monitoring and oversight results, and recommend changes to agency level policies and procedures, as appropriate;
  - Ensure that guidance which identifies positions/job types with key Privacy Program responsibilities, along with appropriate cascading goals and objectives, are applied within their respective offices;
  - Designate the organization's LPO;
  - Ensure that a PIA has been completed prior to establishing a new or significantly modified collection of privacy-related information;
  - Review and approve determinations concerning requests to access sensitive PII from a remote location or to take sensitive PII offsite;
  - Ensure compliance with federal regulations and agency policies and procedures for protecting data in mobile devices used to transport or access PII;
  - Maintain a documented record of all approved remote access, transport of sensitive PII, downloads and/or local storage on a computer not located within EPA space;
  - Ensure that privacy policies and procedures are implemented in their organizations;
  - Ensure all sensitive PII approved to be stored offsite is returned within 90 days; and
  - Ensure coordination with Agency managers in response to a breach of sensitive PII.

- **System Owners:**
  - Apply privacy requirements in program offices and regions;
  - Establish safeguards to ensure confidentiality, integrity and availability controls;
  - Authorize privacy documentation for new and/or revised systems;
  - Terminate systems when no longer needed in accordance with proper destruction/transfer procedures;
  - Approve initial determinations on access to information;
  - Account for access, amendments and disclosures to Privacy Act systems of records and notify LPOs of system changes; and
  - Ensure that PTAs and/or PIAs are conducted for newly developed systems and/or systems that undergo substantial revisions.

8. DEFINITIONS

Access. Access also includes the act of communicating with EPA systems that collect PII.

Agency Inventory. A list of federal information systems that contain PII.

Availability. Ensuring timely and reliable access to and use of information.

Breach. The loss of control, compromise, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether in paper or electronic formats.

Cloud Computing. Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Computer Matching. Computer Matching is any computerized comparison of two or more payroll or personnel automated systems of records, or a system of records with non-federal records, for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs.

Computer Matching Agreement (CMA). CMAs are required for a computerized comparison of two or more automated systems of records, or a system of records with non-federal records for purposes of verifying that recipients are eligible to receive benefits or to recoup payments.

Data Integrity Board (DIB). The DIB is comprised of EPA's CIO, Principal Deputy General Counsel and Inspector General. The DIB is supported by the National Privacy Program Manager and other key personnel. Pursuant to Appendix I to OMB Circular A-130 4(a) (b) the board reports annually to Congress and OMB on ongoing computer matching programs and provides guidance to EPA concerning computer matching agreements.

Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Interconnection Security Agreement. This is a document that identifies how PII will be protected as it is shared between two or more systems.

National Privacy Program. The organizational entity that oversees EPA's Privacy Program. It is housed in OEI and is comprised of the Agency Privacy Officer, Chief Privacy Officer, and Senior Agency Official for Privacy. The National Program also works closely with Liaison Privacy Officials in program and regional offices and key privacy personnel identified in section 7 of this Policy, including IMOs, ISOs, SAISO, and system managers/owners to carry out its responsibilities.

Official Use. Authorized use of any record or the information contained therein to perform the official duties of an EPA employee, grantee or contractor.

Personally Identifiable Information (PII). Any information about an individual maintained by an agency, which can be used to distinguish, trace or identify an individual's identity, including personal information which is linked or linkable to an individual (e.g., name, date of birth, address).

Privacy Act Information. Information about an individual that is retrieved by name or other personal identifier assigned to the individual.

Privacy Impact Assessment (PIA). An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Threshold Analysis (PTA). An analysis that includes responses to privacy information questions for all new systems and any other investment that undergoes substantial modifications. The PTA determines if the investment will be collecting any PII data elements and if a full PIA is required.

Risk-based Approach. An activity, mechanism, or methodology that is designed to provide "adequate security" (as defined in OMB Cir. A-130, Appendix III) for the affected information technology and/or information resources. In the context of this policy, this applies principally to the security objective of confidentiality.

Sensitive Personally Identifiable Information (SPII). 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, biometrics, financial information associated with individuals and medical information associated with individuals. SPII requires additional levels of security controls (which can be found in the Information Security Privacy Procedures).

Social Media. Websites, applications and Web-based tools that allow the creation and exchange of user-generated content. Through social media, people or groups can engage in dialogue, interact, and create, organize, edit, comment on, combine and share content.

System of Records. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Notices for all Privacy Act systems of records must be published in the Federal Register.

System of Records Notice (SORN). The Federal Register notice in which an agency announces the establishment, amendment or deletion of a system of records.

System Manager/Owner. A Division Director or equivalent responsible for the implementation of the Privacy Act within their respective areas.

U.S. Computer Emergency Readiness Team (US-CERT). The Department of Homeland Security's US-CERT leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans.

9. WAIVERS

None

10. RELATED PROCEDURES, STANDARDS AND GUIDANCE

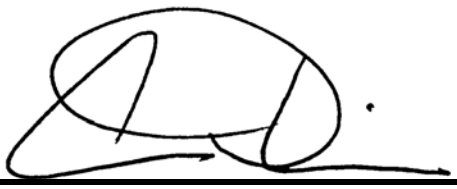
- U.S. EPA Directive 2190 - Privacy Act Manual (Revised December 2005) Privacy Act Manual
- Guidance for Preparing Privacy Impact Assessments Privacy Impact Assessments
- Privacy Threshold Analysis http://intranet.epa.gov/privacy/guidance_document.htm
- Conducting Privacy On-site Reviews CIO 2151-P-07.0
- Procedure for Responding to Breaches of Personally Identifiable Information CIO 2151-P-02.2
- Guidance for Establishing Rules of Behavior (RoB) for Information Security Plans, November 6, 2003
- CIO Policy Transmittal 06-11: Interim Policy and Procedures for Protecting Personally Identifiable Information (PDF)
- Agency Guidance on Incident Response Handling and Information Security Officer Handbook (PDF)
- Social Media Policy CIO 2184.0
- Mobile Computing Policy CIO 2150.4
- EPA Order 3180, EPA Flexiplace Policy http://intranet.epa.gov/ohr/rmpolicy/hr/3180.pdf

11. MATERIAL SUPERSEDED

This revised policy replaces CIO 2151.0.

12. ADDITIONAL INFORMATION

For further information, please contact the Agency Privacy Officer.



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