BPA Policy 236-3

Privacy Program

Table of Contents

1. Purpose & Background

A. This policy establishes BPA's privacy program and provides guidance to staff to ensure compliance with federal privacy laws, regulations, and orders designed to protect Personally Identifiable Information (PII).

B. BPA uses administrative, physical, and technical safeguards to protect PII in BPA's information assets. BPA Policy 236-3 outlines the role of BPA users to ensure that the appropriate safeguards are in place to protect PII in all information assets, regardless of format.

C. Protecting the privacy of our employees, our customers, and the public is of paramount interest to BPA and required by law.

2. Policy Owner

The Executive Vice President of Compliance, Audit, and Risk has overall responsibility for this policy. The BPA Privacy Officer within Information Governance develops, implements, and manages this policy on behalf of the Executive Vice President of Compliance, Audit, and Risk.

3. Applicability

A. This policy applies to all activities that occur at BPA when accessing BPA's information assets that contain PII.

B. Records that contain PII in any form or format (physical or electronic), including but not limited to:

1. Official personnel files;
2. Payroll time and attendance files and other personnel related information;
3. Structured Electronic Information Systems used by BPA; and
4. Short-term and federal records created by BPA in the course of agency business.

4. Terms & Definitions

A. **Administrative safeguards**: Policies and procedures that protect PII; for example, training personnel on information handling best practices.

B. **Breach**: As defined in OMB Memo M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (1/3/2017), a breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information; or (2) an authorized user accesses or

potentially accesses PII for an other than authorized purpose. All breaches constitute an incident.

C. **Incident**: As defined in OMB Memo M-17-12, an incident is an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

D. **Personal files**: Also called personal papers, are documentary materials belonging to an individual which are not used to conduct agency business. Personal files are excluded from the definition of federal records and are not owned by the government. (*See* 36 CFR § 1220.18, *What Definitions Apply to the Regulations in Subchapter B* (8/28/2019).)

E. **Personally Identifiable Information (PII)**: As defined in DOE O 206.1, *Department of Energy Privacy Program* (2009), PII is 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.

F. **Physical safeguards**: Physical measures taken to protect PII; for example, restricted permissions to physical locations to ensure paper records are secured and access is properly controlled.

G. **Privacy Impact Assessment (PIA)**: An analysis of how PII is collected, used, shared, and maintained in an electronic information system. PIAs document risk, demonstrate to the public how BPA has incorporated privacy protections into the information lifecycle, and function as a resource document to facilitate decision making in case of an incident or breach. PIAs are required by the E-Government Act of 2002.

H. **Sensitive Personally Identifiable Information (PII)**: A subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements.

   1. Examples of stand-alone sensitive PII include: Social Security Numbers (SSN); driver's license or state identification numbers; Alien Registration Numbers; financial account numbers; and biometric identifiers such as fingerprint, voiceprint, or iris scan.

   2. Other PII is sensitive when combined with the name of an individual, such as account passwords, employee performance ratings, citizenship or immigration status, medical information, home addresses, and phone numbers. In contrast, a business card or public telephone directory of agency employees contains PII, but is not sensitive.

3. Sensitive PII is considered Controlled Unclassified Information. (*See also* BPA Policy 433-1, *Information Security* (Version 3, 2/23/16).)

I. **System of Records Notice (SORN)**: As defined in the Privacy Act (5 U.S.C. § 552), a notice in the Federal Register about a Privacy Act System of Records (SOR).

J. **System of Record (SOR)**: As defined in the Privacy Act (5 U.S.C. § 552), system of records is 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 identifier assigned to the individual.

K. **Technical safeguards**: The technology and related policies and procedures used to protect PII; for example, encrypting computers and emails, and requiring access cards for systems access.

5. Policy

A. Protecting the privacy of our employees, our customers, and the public is required by law. BPA uses administrative, physical, and technical safeguards to protect PII found in BPA information assets, regardless of format. See BPA Procedure 236-3-1, *Privacy Program Rules of Behavior Handbook* (2019), for rules to follow for handling and safeguarding all PII.

B. Sensitive or high risk PII requires greater protection than non-sensitive PII because of the increased risk to an individual if the data are compromised. The Appendix PII Fact Sheet provides examples of non-sensitive and sensitive PII. See BPA Procedure 236-3-1 (2019) for rules to follow for handling and safeguarding Sensitive PII.

C. BPA's Privacy Program works in collaboration with Information Security, Cyber Security, and the Office of General Counsel to address and respond to suspected and actual breaches of PII at BPA, following the unauthorized disclosure procedure in BPA Procedure 236-3-1 (2019). BPA reports all breaches to DOE's Privacy Office.

D. BPA only collects personal information that is necessary to conduct agency business in accordance with the Privacy Act of 1974, the Paperwork Reduction Act of 1995, and other privacy laws. (*See also* BPA Policy 236-2, *Information Collection* (Version 1.0, 2/3/2019).)

E. PII collected under the Privacy Act is stored in a Privacy System of Records (SOR) with a published SORN in the Federal Register. PII that is in a SOR cannot be disclosed without consent of the individual to whom the record pertains or by statutory exception.

F. All employees must complete annual agency-wide privacy awareness training.

G. All Structured Electronic Information Systems must have a PIA on file with the Privacy Office. (*See also* BPA Policy 236-300, *Enterprise Data Governance* (Version 1.0, 12/31/2018)).

H. BPA only collects Social Security numbers when required by statute or regulation.

6. Policy Exceptions

This policy does not apply to personal files, as defined in this policy.

7. Responsibilities

A. **Privacy Officer**

1. Ensure that BPA complies with applicable privacy requirements in law, regulation, and policy.
2. Manage privacy risks associated with any BPA activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems.
3. Collaborate with BPA's Information Security, Cybersecurity, and Office of General Counsel to respond to breaches.
4. Work with the DOE Chief Privacy Officer to update existing SORNs or develop new SORNs as appropriate.

B. **Chief Information Security Officer**

1. Develop and maintain the agency Cyber Security Program.
2. Facilitate external and internal information security reviews, and coordinate site visits that support federal and DOE oversight audits.
3. Conduct an immediate review of any BPA owned or operated IT System when notified of an actual or suspected breach of PII from that system.
4. Provide technical remediation and forensic analysis capabilities.
5. Conduct periodic risk assessments to identify areas of privacy-related vulnerabilities and risks that can be found among BPA IT systems.
6. Report actual or suspected breaches of electronic PII to DOE's Integrated Joint Cybersecurity Coordination Center (iJC3).
7. Support and assist the BPA Privacy Officer in safeguarding electronic PII.

C. **Privacy Act System Managers**

Manage PII found in published system of records notices (SORNs) in accordance with the provisions of the Privacy Act.

D. **Information System Owners and Information Owners**

1. Ensure completion of PIAs.
2. Implement, operate, and monitor all BPA IT systems in compliance with established protocols for control of PII access and in accordance with BPA Policy 236-300, *Enterprise Data Governance* (Version 1.0, 12/31/2018).

E. **Supervisors**

1. Ensure that all employees within their organization complete the annual agency-wide privacy awareness training.
2. Advise employees who work with PII of their responsibility to maintain proper administrative, physical, and technical safeguards around PII as described in BPA Procedure 236-3-1 (2019). Provide department- or job-specific training as needed.
3. Immediately report any suspected or confirmed unauthorized disclosure of PII to BPA's Privacy Office, Information Security, or the BPA Hotline.

F. **BPA Users**

1. Minimize the collection of PII to only that required to conduct BPA business.
2. Ensure PII is protected by appropriate safeguards to ensure security, confidentiality, and privacy as described in BPA Procedure 236-3-1 (2019).
3. Complete annual agency-wide privacy awareness training and, as appropriate, job specific, role-based training.
4. Acknowledge, on an annual basis, specific responsibilities related to the protection of PII and consequences of the failure to properly protect PII.
5. Immediately report any suspected or confirmed unauthorized disclosure of PII to the BPA Privacy Office, Information Security, or the BPA Hotline.

8. Standards & Procedures

See BPA Procedure 236-3-1*, Privacy Program Rules of Behavior Handbook* (2019) for procedures.

9. Performance & Monitoring

The Privacy Office measures the effectiveness of this policy by analyzing privacy breaches and assessing risk of breaches.

10. Authorities & References

A. Freedom of Information Act, as amended (5 U.S.C. § 552) gives individuals the right to access information from the federal government.

B. Privacy Act of 1974, as amended (5 U.S.C § 552a) regulates the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies.

C. E-Government Act of 2002 (44 U.S.C. § 3501 note) requires federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form to complete PIAs on those systems.

D. Federal Information Security Modernization Act of 2014 (44 U.S.C. § 3551) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

E. Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. §§ 3501 through 3520) requires that federal agencies obtain OMB approval before requesting most types of information from the public. The PRA and Privacy Act of 1974, as amended, are two separate laws for different issues with separate requirements, but they are meant to work together. The PRA deals with approval to collect the information and the Privacy Act deals with maintaining and protecting the information.

F. 44 U.S.C. § 3554(b)(7)(C)(iii)(III) requires agency heads to report major information security incidents to Congress within seven days.

G. Privacy guidance provided by the Office of Management and Budget establishes Executive Branch policy and procedures for managing PII. OMB guidance includes:

- Circular A-130 “Managing Information as a Strategic Resource” (July 28, 2016),
- OMB Memo M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (September 15, 2016), and
- M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information” (1/3/2017).

H. DOE O 206.1, *Department of Energy Privacy Program* (2009), establishes implementation of agency statutory and regulatory requirements for privacy for DOE departmental elements, including BPA.

11. Review

This policy is reviewed by the Privacy Office every three years.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
1.0	11/6/2019	Initial publication of policy

Appendix: Personally Identifiable Information

What is PII?

The definition of PII is broad. PII includes any information collected or maintained by the Bonneville Power Administration about any individual. This includes:

- Information that can be used to distinguish or trace an individual, such as name, Social Security number, and biometric data, *and*
- Information about a person's past or present status or activities, such as education, medical history, criminal history, or employment history.

What is Sensitive/High Risk PII?

Sensitive/High Risk PII is PII that must be protected against loss because improper disclosure could result in substantial harm, embarrassment, inconvenience or unfairness to an individual. Improper disclosure includes loss, theft, and unauthorized release or sharing.

Examples of SENSITIVE/High Risk PII	
Social Security number or last four digits	Education
Medical history and conditions	Height and weight
Credit card and financial account numbers (personal and government)	Workplace performance and disciplinary history
Driver's license, state ID and passport number	Employment history and information

What is Non-Sensitive/Low Risk PII?

Non-Sensitive/Low Risk PII is information that is often publicly available, and its dissemination is unlikely to lead to harm. Keep in mind that you should exercise care when handling *any* kind of PII.

Examples of NON-SENSITIVE/Low Risk PII	
Name	Phone number
Email address	HRMIS ID
Home address	BUD login

Can PII be sensitive in some cases and not in others?

Yes. Context matters. Some kinds of PII are always considered sensitive, including Social Security numbers, birth dates, and biometric identifiers like fingerprints. Other categories of PII are sensitive in certain contexts. For example:

- A list of employee names attending a meeting would be non-sensitive. A list of employee names facing disciplinary action would be sensitive because it is potentially harmful or embarrassing.
- Identifiable photographs are PII, but the sensitivity cannot be predicted because it depends on both content and context.

What other kinds of things are PII?

Many other things may be PII; the charts above are not exhaustive and only contain examples. *Remember,* PII includes any information that meets the definition above, and sensitivity depends on context.

Privacy questions? Contact BPA's Privacy Office at Privacy@BPA.gov.
For more resources, including tips on how to protect PII, visit the Privacy Office webpage at http://portal.bpa.gov/sites/bpaprivacyprogram.