BPA Procedure 236-3-1

Privacy Program Rules of Behavior

Table of Contents

1. Introduction

This procedure provides the minimum safeguards and rules of behavior for BPA users who collect, maintain, handle, access, or disseminate Personally Identifiable Information (PII) while performing their official duties. This applies to BPA users wherever they are working, including BPA facilities, remote and telework locations, and travel or local travel status locations.

2. Applicability

These procedures apply when handling BPA information assets that contain personal information.

3. Terms & Definitions

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

B. **Breach:** 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:** 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. Not all incidents are breaches.

D. **Information Asset:** Information that has business value for BPA and must be managed throughout its lifecycle, an information asset may be a record or non-record and may be structured or unstructured data.

E. **Non-Sensitive PII**: a type of PII that represents manageable risk of harm to individuals and is not being used in a context that raises the level of sensitivity. Non-Sensitive PII would include PII that is used for the administration of systems, such as work email address, username, passwords, or security verification questions. Some Non-Sensitive PII may warrant additional protections regardless of its Non-Sensitive status. For example, personal PII should always be treated with greater sensitivity than work-related PII.

F. **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.

G. **Personally Identifiable Information (PII)**: 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. At BPA, for the purposes of privacy compliance documentation (i.e., PTAs and PIAs), PII is assessed in terms of "Non-Sensitive" and "Sensitive" PII.

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

I. **Privacy Act Information:** information that is required to be protected under the Privacy Act of 1974. Information subject to the Privacy Act must be retrieved by a unique personal identifier, such as a name or unique identification number or code. Privacy Act information must be safeguarded and handled in accordance with the requirements and restrictions outlined in the Privacy Act. Any grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger- and voice print or a photograph is considered a record for the purposes of the Privacy Act.

J. **Privacy Act Request:** A request to an agency to gain access to an individual's record, such as by another Federal agency or law enforcement as required by statute; a request by any individual to gain access to his/her record or to any information pertaining to him/her which is contained in the system.

K. **Privacy Act Statement:** A Privacy Act Statement is provided to individuals supplying PII to BPA when that PII is protected by the Privacy Act. Privacy Act Statements include the authority to collect information, whether supplying the information is mandatory or voluntary, the principal purpose(s) for collection, routine uses of the information, and the effect of refusing to provide the information. All Privacy Act statements must be reviewed by the Privacy Office or component Privacy Officer.

L. **Privacy Impact Assessment (PIA):** A documented analysis of how information is handled to: (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining and disseminating PII in an electronic information system or information collection; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

M. **Privacy Notice:** A Privacy Notice is provided to individuals supplying PII to BPA when that PII is not covered by the Privacy Act. Privacy Notices include the purpose of the collection and how BPA will use and secure the information.

N. **Privacy Threshold Assessment (PTA):** The first step of the PIA process. PTAs are structured to assess the collection and intended use of PII. Through the use of threshold questions determines if a full PIA is required.

O. **Sensitive 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*.)

P. **(Privacy Act) 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 identifier assigned to the individual. BPA's Privacy Act Systems of Records are available on BPA.gov.

Q. **System of Records Notice (SORN)**: Notice published in the Federal Register prior to an agency's collection, maintenance, use or dissemination of information about an individual.

R. **Structured Electronic Information System (SEIS):** Electronic information systems (EIS) used by BPA to collect/maintain data or records in a structured format (typically a database).

S. **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.

4. Authorizing Policies

BPA Policy 236-3, *Privacy Program*

5. Roles and 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. Process and respond to Privacy Act requests for records.
5. Work with DOE's Enterprise Privacy Program (EPP) to update existing SORNs or develop new SORNs as appropriate.
6. Acts as a liaison to DOE's Chief Privacy Officer, on matters of local privacy implementation, including the facilitation of PIAs, facilitating compliance reporting, responding to data calls, assisting as needed in privacy breach response, and issues involving SORNs.
7. Works to reduce the unnecessary collection/use of SSNs as an identifier.
8. Manages the process for resolving privacy complaints for BPA, documents, and notifies DOE of unresolved written complaints.
9. Advise, promote, and participate in DOE EPP activities (including, but not limited to privacy compliance documentation, training opportunities, and routine and situational compliance reporting).
10. Facilitate privacy control implementation, assessment and safeguarding functions related to PII, including creating and maintaining privacy compliance documentation such as PTAs, PIAs, SORNs, privacy control implementation plans, incident response plans and any other needed documentation for ensuring privacy risk is managed.

B. **SharePoint Site Content Owner**

1. As defined by the SharePoint Governance Guidance document, this is the person (usually a manager) who owns the content on the SharePoint site and is responsible for its disposition.
2. This role is limited to one person per site and must be a federal employee.
3. Ensures the SharePoint Site Coordinator(s) follows the SharePoint Governance Guidance regarding PII and permissions management.

C. **SharePoint Site Coordinator**

1. As defined by the SharePoint Governance Guidance document, this is the person who manages the day-to-day operations of a site, such as permissions, new libraries, page updates, etc.

2. As a best practice, this role is limited to two people per site.
3. Is responsible for following SharePoint Governance including regularly reviewing site permissions.

6. Rules of Behavior

6.1 General Rules of Behavior for Protecting Personally Identifiable Information

A. Any collection of Social Security Numbers must be reviewed, documented, and approved by the Privacy Office.

B. BPA users who collect, maintain, handle, access, or disseminate PII must ensure that the information is properly protected.

C. Limit the collection and use of PII. New information collections must follow BPA guidance as found in BPA Policy 236-2, *Information Collection*.

D. Only access or use Sensitive PII when there is a business need and authorized by law to use that information for that purpose. Never browse files containing Sensitive PII out of curiosity or for personal reasons.

E. Do not record virtual meetings where sensitive PII will be discussed or shared.

F. Do not share sensitive PII in any instant message, text message, or chat application.

G. Ensure that your use of Sensitive PII is compatible with the original intent of its collection and within the bounds of the notice provided to individuals when the information was provided to BPA. This notice may be in the form of a SORN, a PIA, or a Privacy Act Statement. If you are unsure about whether a specific use is appropriate, BPA users should confirm with BPA's Privacy Office.

H. BPA contractors must have a nondisclosure agreement on file with BPA and complete the mandatory online privacy awareness training course prior to handling Sensitive PII.

I. Refer requests for BPA records from members of the media, the public and other outside entities – including requests from members of Congress – to BPA's Freedom of Information Act (FOIA) Officer and/or Privacy Act Officer.

J. Do not create unnecessary or duplicative collections of Sensitive PII, such as duplicate, ancillary, "shadow," or "under the radar" files. See section 6.5 below.

K. When working with PII, ensure that the information isn't accessible to unauthorized individuals. Secure your computer throughout the day when you step away from it and if working with paper materials ensure they are appropriately secured when not in use. When in the office, double-check the printer before you leave to ensure any information printed is secured. If applicable secure your office door. During normal business hours,

maintain information containing PII in areas accessible only to authorized individuals. After business hours:

1. Secure computers by removing PIV access (or locking if using an RSA token).
2. Put paper materials in a locked drawer or cabinet and/or a locked office or file room.
3. When teleworking, do not print sensitive PII; do not take sensitive PII home unless specifically authorized by your supervisor.

L. Properly destroy materials containing PII, in accordance with your organization's Information Asset Plan and BPA Policy 236-1, *Information Governance and Lifecycle Management*, and by shredding, deleting or other authorized destruction methods that ensure the data or record is unreadable or unrecoverable.

Rules of Behavior for Storing PII

6.2 Sensitive PII on SharePoint or Shared/Network Drives

A. Limited amounts of sensitive PII may be stored on SharePoint or Shared/Network Drives, but access must be controlled and limited, permissions must be regularly reviewed, and information must be disposed of once it is no longer needed.

B. Any PII on SharePoint must be managed in accordance with the SharePoint Governance Document.

C. Collection and storage of Social Security Numbers (SSNs) (including partial SSNs – last four digits) is prohibited unless approved by the BPA Privacy Office and documented in a Privacy Impact Assessment.

D. SharePoint Sites and Shared/Network Drive folders must be marked with a CUI label. See the SharePoint Governance document.

E. Permissions to locations with Sensitive PII on SharePoint must be actively managed by the Site Coordinator:

1. Sensitive PII should be stored on uniquely secured sites, libraries, lists, or folders.
2. Permissions must be restricted to those with a lawful government purpose.
3. Site Coordinator must implement procedures to add and remove access based on lawful government purposes.
4. The Site Coordinator must review permissions regularly, at a minimum quarterly.

F. Permissions to locations with Sensitive PII on Shared/Network Drives must be actively managed by the office of record's manager or supervisor by submitting a ticket in the IT Service Management Portal to add or remove users from access.

G. Personal files should not be stored on SharePoint or Shared/Network Drives. Examples of personal files include personal benefits information, professional certifications, and

personal correspondence. These should be stored in the employee's personal network drive on the File Server (i.e., the H:/ Drive).

6.3 Sensitive PII on Non-BPA Devices

Do not maintain any BPA Sensitive PII on a personal device or non-BPA device.

6.4 Sensitive PII on Removable Media

(For additional information regarding removable media and Sensitive PII, see BPA Procedure 433-1-2, *Identification and Control of Controlled Unclassified Information*.)

A. Removable media includes but is not limited to CDs, DVDs, external hard drives, and USB Flash Drives (also known as thumb drives).

B. In general, Sensitive PII should not be saved on removable media.

C. Removable media that contain sensitive PII data may only be accessed and stored on BPA-issued and controlled devices. These devices must be encrypted.

D. BPA users must not:

1. Leave removable media containing Sensitive PII unattended.
2. Share removable media containing Sensitive PII with unauthorized individuals.
3. Check removable media containing Sensitive PII with luggage when traveling.
4. Leave a USB flash drive containing Sensitive PII in an unattended computer.
5. Attach a USB flash drive containing Sensitive PII to a key ring.

E. BPA users must:

1. Encrypt Sensitive PII contained on removable media.
2. Immediately report any loss or theft of equipment containing PII to their immediate supervisor to initiate the breach notification process.
3. Report any suspicious activity, suspected loss, or theft of PII to a supervisor or the Privacy Office.

6.5 Extracting Sensitive PII from IT Systems

A. End users are strongly discouraged from printing sensitive PII. End users who download or print out sensitive PII from electronic information systems must ensure it is necessary for a business purpose and should destroy the downloads and printouts when no longer needed, in accordance with your organization's Information Asset Plan and BPA Policy 236-1, *Information Governance and Lifecycle Management*.

B. In some instances, it may be appropriate to create new spreadsheets or databases that contain Sensitive PII from a larger file or database, but these new files should be kept

only as long as necessary, and access should be limited. When there is a need to print, copy, or extract Sensitive PII from a larger data set, limit the new data set to include only the specific data elements needed to perform the task at hand. If there is a need to create duplicate copies of sensitive PII to perform a particular task or project, delete or destroy them when they are no longer needed.

6.6 Digitizing Paper Documents Containing Sensitive PII

A. Use caution when digitizing a document that is automatically saved on a shared network drive assigned to the scanner.

B. Take steps, such as password protecting folders, to save the digitized document in a location that can be accessed by only those who need the file to do their job.

Rules of Behavior for Transmitting PII

6.7 Physical Transport of Sensitive PII

A. BPA users who have a business need to transport Sensitive PII from BPA's secured, physical perimeter must have written authorization from his or her supervisor.

B. The authorization must describe the work assignment that requires the use of Sensitive PII and the type of PII data needed to complete the assignment.

C. BPA users who create or maintain physical documents or data-containing physical media containing Sensitive PII must know where the records are at all times.

D. Users must secure Sensitive PII when traveling, either on official travel, to and from off-site meetings, or to and from work locations including teleworking locations.

E. Avoid leaving a mobile device, laptop (regardless of whether it contains PII), portable storage media, or paper documents containing PII in an unattended vehicle. In extraordinary circumstances, if it is not possible to carry them when leaving the car, lock the car, place the laptop and other materials in the trunk so that they are not visible (prior to arrival at the destination if practical).

6.8 Sending Sensitive PII by Email or Fax

(For additional information regarding emails or faxes containing Sensitive PII, see BPA Procedure 433-1-2, Identification and Control of Controlled Unclassified Information.)

A. Consider the sensitivity of the information and the impact of the loss of the PII before choosing to send Sensitive PII via email or fax.

B. Properly mark emails or faxes containing Sensitive PII so that the recipient will be alerted to the need to protect the information.

C. Provide a point of contact should the email or fax be received by someone other than an authorized recipient. Contact instructions may be appropriate, for example: "If you

have received this [email/fax] in error, please notify the sender immediately by reply [email/fax] and [permanently delete this email/destroy this fax] and any attachments without reading, forwarding, saving or disclosing them."

D. Ensure that the email address or fax number is correct before sending the email.

E. Never send Sensitive PII to a personal email account for ease of access to the information when working remotely. (See also BPA Policy 236-260, *Email Management*, which prohibits the use of personal email to conduct agency business.)

F. Encrypting emails containing PII within the BPA email system is not required due to the security that is already in place for internal emails. Emailing Sensitive PII from one BPA account to another BPA account doesn't require encryption or password protection since the information doesn't leave BPA's control. However, the email still needs to be properly marked as identified in BPA Procedure 433-1-2, Identification and Control of Controlled Unclassified Information.

G. If emailing Sensitive PII outside of BPA, ensure the email is encrypted or password protected and send the password in a separate email.

6.9 Sending Sensitive PII by Text Message, Instant Message, or Chat

Do not send sensitive PII by text message, instant message, or in a chat message (including Teams chat).

6.10 Sending Sensitive PII by Mail

A. Small amounts of sensitive PII may be sent via interagency mail systems, United States Postal Service (USPS), or other commercial delivery services, consistent with other provisions of law. In-transit automated tracking and accountability tools can be used to record the location of the Sensitive PII.

B. While Sensitive PII (often this is CUI) documents and matter being mailed must be properly labeled, the wrapping or package containing the CUI must not indicate the presence of CUI. The wrapping or package should indicate "Open by Addressee Only" to ensure it is only opened by the intended recipient.

6.11 Sending Sensitive PII via Interoffice Mail

A. In general, it is best to hand deliver paper documents or electronic media containing PII to another BPA employee or office, but BPA users may send small amounts of PII in paper form through interoffice mail. Use a sealed, opaque envelope labeled "TO BE OPENED BY ADDRESSEE ONLY."

B. Do not send a large volume of PII through interoffice mail. For example, send one employee's personnel action form to that person via interoffice mail, but do not send a stack of personnel action forms for an entire division or organization through interoffice mail.

C. Never send a disk or other portable media containing sensitive/high risk PII through interoffice mail unless the files are encrypted or the portable media is encrypted.

7. Unauthorized Disclosure Procedure

A breach of PII is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where individuals gain access or potential access to PII, whether physical or electronic, for an unauthorized purpose. A breach is one type of incident.

A. For details on how BPA manages other types of unauthorized disclosure incidents, see the Unauthorized Disclosure Coordination Service Level Agreement (SLA) for procedures when a breach or potential breach occurs. This section details the procedures the Privacy Office will follow during a breach. **Examples of incidents that may be categorized as a breach:**

1. Actual or suspected loss, theft, or improper disclosure of PII data in electronic or paper form.
2. Lost or stolen equipment, especially removable media (electronic devices capable of storing and retaining data, such as laptops, mobile devices, USB flash drives, external hard drives or other electronic storage devices) that are known or suspected to contain PII.
3. Inadvertent loss or unauthorized access to employee information consisting of names and social security numbers (including a temporary loss of control).
4. Inadvertent loss or unauthorized access to information relating to the public (including the names and addresses of BPA visitors).
5. Incorrect delivery of PII.

B. **Initial breach reporting sequence**

1. A BPA employee or contractor determines that an unauthorized disclosure of PII may have taken place.
2. The employee notifies the Privacy Office (privacy@bpa.gov) of the suspected incident. Alternatively, the Privacy Office may discover suspected breaches from the Information Protection or Cyber Forensics offices.
3. The Privacy Office, in collaboration with Information Protection and Cybersecurity when appropriate, performs additional fact-gathering as necessary. Facts gathered by the Privacy Office may include:

a) Name and contact information of the original reporting individual(s)

b) Date and time incident was reported

c) Date, time and location of incident

d) Type of data involved (SSNs, passwords, medical records, etc.), including types of owners (internal/employee, member of the public, etc.)

e) Description of the incident:

i) How it was discovered

ii) Types of media (paper, electronically transmitted data, missing or stolen hardware)

iii) Whether any protection was in place or may still be in place – encryption,

iv) Password protection, ability to remote erase, etc.

v) Estimate of number of records and number of individuals involved

vi) Whether the incident has been contained (potential for further data loss)

4. If it is determined that no breach occurred, the incident is noted in the Privacy Incident Log and the Privacy Office notifies parties in communication about the incident that it has been closed. If a breach is confirmed, the Privacy Office notifies IT/Cyber Security, Information Protection, and DOE Integrated Joint Cybersecurity Coordination Center (iJC3). In some circumstances, these offices may be notified before fact gathering is complete. If it is determined that the breach is a Major Incident or a widespread event, DOE will take responsibility for breach response.

C. **Investigation and Containment**

1. If immediate, lawful steps may prevent a breach or reduce the magnitude of a breach, they may be taken at any time. Such steps include remote wiping a device, requesting law enforcement help, etc.
2. Depending on the type of incident (system breach, human error, etc.), the Privacy Office, Information Protection and IT/Cybersecurity may run simultaneous investigations. Access to incident information should be limited on a "lawful government purpose" basis.
3. Widespread internal notification may be necessary for a large breach. This type of notification would be coordinated with DOE.
4. The Privacy Office reviews known information and identifies any factual gaps. Additional information may be submitted to DOE to supplement the initial report.
5. The Privacy Office confirms, as far as possible, what PII is lost or at risk. If the incident is a system breach, this includes reviewing the relevant Privacy Impact Assessment and identifying connected systems.

6. During the investigation, the Privacy Office protects and preserves evidence in its possession with access limited to the Privacy Office and the LG attorney assigned to privacy matters.

D. **Reporting**

1. The Privacy Office reports all breaches to DOE iJC3 via the web portal iJC3 Service Portal - iJC3 Incident Portal.
2. The Privacy Office reports all breaches to the Audit, Compliance and Governance Committee quarterly.
3. The LG Assistant General Counsel reports breaches as necessary to the DOE Office of General Counsel.

E. **Analysis and Determination of Privacy Impact**

1. Using the information gathered and any additional information received from IT/Cybersecurity and Information Protection, the Privacy Office conducts an analysis of the incident and documents it in an Incident Report.
2. The Privacy Office assesses the risk of harm to individuals, including identity theft, breach of confidentiality, potential for blackmail, disclosure of private facts, mental pain, emotional distress, financial harm, disclosure of contact information for victims of abuse, potential for harmful secondary uses of information, humiliation, loss of self-esteem, inconvenience, unfairness, or other harm.
3. The following factors are considered when assessing harm:
   a) Nature and sensitivity of the PII compromised
      i) Data elements – evaluate sensitivity of the elements individually and in combination
      ii) Context
      iii) Private information - may lead to embarrassment, blackmail, etc.
      iv) Vulnerability of populations affected
      v) Permanence (continued relevance of compromised PII over time)
   b) Likelihood of access and use of PII
      i) Security safeguards – encryption, redaction, etc.
      ii) Format and media – USB flash drive vs. magnetic tape, etc.
      iii) Duration of exposure
      iv) Evidence of misuse
   c) Type of breach

i) Intent

ii) Recipient

F. **Notification and Mitigation**

1. The Privacy Office determines whether mitigation steps will reduce the risk of harm.

   a) Countermeasures: Countermeasures, such as expiring potentially compromised passwords or placing an alert in a database containing potentially compromised PII, are fact-specific and should only be offered if BPA has staff available to implement them.

   b) Guidance: Individuals should be provided with guidance on how to mitigate their own harm by, for instance, setting up fraud alerts, changing passwords, etc.

   c) Services: BPA may offer a term of identity theft or credit monitoring, which can be purchased with a P-card using existing GSA accounts.

2. The Privacy Office determines whether notification is warranted.

   a) Notification is required if the impacted PII consists of sensitive PII, such as SSNs, financial information, or health information, which has been sent unsecured outside of BPA's IT network firewall. Notification is also required if there are clear and verifiable indications of compromise or unauthorized access to PII that could result in immediate harm to the individual by a malicious actor.

   b) Notification is warranted if there is at least a moderate risk of harm and notification would not result in unnecessary chilling effect. Notification can have negative consequences, including fear and stress, spending money on unnecessary credit monitoring services, “notification fatigue,” and confusion.

   c) If notification is warranted, the Privacy Office crafts a notification with the following parameters in mind:

      i) Timing. Offer without unreasonable delay but balance the needs of law enforcement and national security. For required notification scenarios the notification must be made within 90 days.

         a. If a systems breach, delay for the time needed to restore reasonable integrity of the system is allowed unless;

         b. Risk that delay will exacerbate potential harm.

      ii) Source. For larger breaches, notification should be issued under the signature of the Front Office. Notification for smaller breaches (for instance those concerning the information of a single person) should be issued by the Privacy Officer. If it is a systems breach, notification can be issued jointly by the CIO and Privacy Officer.

iii) Content. Informal notification may be provided in-person, via telephone, or by another appropriate alternative. Informal notification must be followed by formal notification once the investigation is complete. When BPA provides notice, the CPO (at DOE HQ) must be notified within *24 hours* that preliminary notice has been provided and what information has been provided to the affected or potentially affected individuals (this notification of the CPO is considered to have occurred with the iJC3 report). Notification must be provided in writing, using concise, plain language. All formal notifications must be approved by the SAOP (at DOE HQ) and local OGC, prior to being sent to an affected individual. The following elements should be included:

a. Date and brief description of the incident
b. How incident was discovered
c. Data elements involved
d. Whether information was protected and by what means
e. Steps individuals can take to protect themselves from harm
f. How the agency is mitigating loss and preventing future breaches
g. Contact information for questions. This should include a toll-free phone number if possible.

iv) Method. Notification should almost always be made by mail or email. Notification by phone call is acceptable if urgency dictates immediate and personalized notification; follow up with written notification.

d) The Privacy Office does not advise or opine on the need for disciplinary measures after a privacy incident; this is within the purview of the individual's manager and HR.

G. **Closure of Incident**

1. The Privacy Office evaluates the overall incident response and identifies any missteps or lost opportunities and updates policies or training as necessary.
2. The Privacy Office finalizes any documentation created during the response.

8. Information Governance

Records created or received by the Privacy Office will be maintained on SharePoint.

9. References

A. **Policies**

1. BPA Policy 236-3, Privacy Program
2. BPA Policy 433-1, Information Protection
3. HR Directive 410-2, Employee Records and Privacy
4. BPA Policy 470-3 Protection of Personally Identifiable Information within the BPA Application Portfolio
5. DOE O 333.1 Administering Workforce Discipline
6. DOE O 206.1A Privacy Program
7. BPA SharePoint Guidance

B. **Standards**

1. OMB Memoranda
   a) OMB 17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements, (Nov 4, 2016)
   b) OMB 17-06, Policies for Federal Agency Public Websites and Digital Services, (Nov 8, 2016)
   c) OMB 17-09, Management of High Value Assets (Dec 9, 2016)
   d) OMB 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan 3, 2017)
2. NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organization (Jan. 9, 2015)

10. Review

This procedure will be reviewed each time BPA Policy 236-3, *Privacy Program* is reviewed. The EVP of Compliance, Audit, and Risk is authorized to modify and reissue this procedure as necessary.

11. Revision History

This chart contains a history of the revisions and reviews made to this document.

Version **Number**	**Issue Date**	**Brief Description of Change or Review**
1.0	11/6/2019	Initial version.
1.1	12/12/2022	Revision based off SharePoint governance and encryption policy.
1.2	2/16/2022	Revision to incorporate updated encryption policy.
1.3	11/25/2025	Revision for publication of DOE O 206.1A