

BPA Policy 236-1

Information Governance & Lifecycle Management

Table of Contents

1. Purpose & Background	2
2. Policy Owner	2
3. Applicability	2
4. Terms & Definitions	3
5. Policy.....	6
6. Policy Exceptions	8
7. Responsibilities	8
8. Standards & Procedures	13
9. Performance & Monitoring	15
10. Authorities & References	15
11. Review	16
12. Revision History	17

1. Purpose & Background

- A. The head of each Federal agency is required by the Federal Records Act to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities (44 USC § 3101). This policy, in conjunction with additional BPA policies in the 236 (Information Governance) series implements these requirements and extends the requirements to include all information assets.
- B. Information assets received, created, or compiled by the officials and employees of BPA in the transaction of Government business and appropriate for preservation are property of the U.S. Government. The unlawful destruction, removal or personal use of records is criminal misconduct (18 USC § 2071).
- C. This policy authorizes Bonneville Power Administration's (BPA's) Information Governance and Lifecycle Management (IGLM) program.
- D. The purpose of the IGLM program is to oversee the management of BPA's information assets by:
 - 1. Providing policies and procedures to ensure the appropriate creation, maintenance, and disposition of BPA information assets.
 - 2. Ensuring compliance with Federal information management requirements by assisting BPA organizations in their information management responsibilities, assessing agency information governance practices, and managing the BPA records repository; and
 - 3. Protecting the legal and financial rights of BPA by appropriately identifying, organizing, and maintaining records as evidence of BPA's organization/functions, decisions, business transactions, policies, and procedures.

2. Policy Owner

The Executive Vice President of Compliance, Audit, and Risk Management (EVP CAR) has overall responsibility for this policy. The Agency Records Officer within Information Governance develops, implements, and manages this policy on behalf of the EVP CAR.

3. Applicability

This policy relates to all users who create, maintain, and dispose of BPA business-related information.

Organization Information Governance	Title Information Governance & Lifecycle Management	Unique ID 236-1		
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 2

4. Terms & Definitions

A. As used in this policy, the following terms and definitions apply:

1. **Agency File Plan (AFP):** The systematic method of identifying specific types of records and non-records that are maintained by BPA. It includes their descriptions retention instructions, and disposition authorities. The Agency File Plan maps to the Large Aggregate Flexible Schedule approved by National Archives & Records Administration (NARA) for BPA and the General Records Schedule (GRS) from NARA.
2. **Data:** A re-interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing. Electronically stored information or recordings and analog formats. Examples include documents, databases, and audio/visual recordings of events. (www.dama.org). Data is an information asset.
3. **Digitization:** The act of scanning an analog document into an electronic format, as well as the series of activities that results in a digital copy being made available to end users.
4. **Digital Signature:** Encrypted data produced by a mathematical process applied to a record using a hash algorithm and public key cryptography. The encrypted data constituting the digital signature is sometimes used as an electronic signature, is sometimes used as part of a process to authenticate a person or device and is sometimes used to verify the integrity of the record.
5. **Disposition:** Actions that are taken when records are no longer needed to conduct the regular current business of the agency.
6. **Disposition Authority:** The legal authorization for the retention and disposal of records as approved by NARA. For non-records, the disposition is established by the creating or custodial agency. (36 CFR 1220.18)
7. **Electronic Information System (EIS):** An information system that contains, and provides access to, computerized Federal records and other information. (36 CFR 1236.2)
8. **Electronic Record:** Information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record under the Federal Records Act. The term includes both record content and associated metadata that the agency determines is required to meet agency business needs.
9. **Electronic Signature:** A method of signing an electronic document that identifies and authenticates a particular person as the source of the signature and indicates such person's intent to sign the document. For the purpose of BPA policy, electronic

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 3	

signature applies to both Digital Signatures (see sect. 4.A.3) and scanned versions of hard copy signatures.

10. **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.
11. **Information Asset Plan (IAP):** An inventory of an organization’s information assets to include records and non-records. The Information Asset Plan contains information about the assets managed by the organization, the disposition, the retention period of the assets, the date range of the assets, location, and other aspects of each organization’s information assets.
12. **Information Governance & Lifecycle Management (IGLM):** A concept that describes the policies, strategies, processes, practices, services, and tools used by an organization to manage its information assets through every phase of their existence, from creation or receipt, through their useful life to final destruction or disposition to an institution approved for archival deposit of Public Records by the National Archives and Records Administration (NARA). IGLM is also the team within BPA responsible for BPA’s Records & Information Management Program.
13. **Information Lifecycle:** Phrase used to describe the identification, maintenance, and disposition of an information asset.
14. **Large Aggregate Flexible Schedule:** A form of retention schedule and disposition authority allowed by NARA for Federal records, consisting of items covering multiple related series (types) of records. BPA uses a large aggregate flexible schedule (“The Big Bucket”) that is arranged by business function. The Big Bucket maps to the Agency File Plan, which is arranged by sub function and retention.
15. **Metadata:** Structured information about any recorded information such as date and time it was created, the author, organization, or other data. This also includes descriptions of content, structure, data elements, interrelationships, indexing and other characteristics of the data, information, and records.
16. **National Archives & Records Administration (NARA):** The Federal agency responsible for guidance and assistance to Federal officials on the management of records; assistance in the determination of the retention and disposition of records. They also provide storage for agency records in records centers; they receive, preserve, and make available permanently valuable Federal and Presidential records. NARA also publishes the General Records Schedule, which is included in BPA’s Agency File Plan.
17. **Non-Record:** Informational materials that do not meet the statutory definition of “records” (44 U.S.C. 3301), have been excluded from coverage by the definition, or

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 4	

are no longer being maintained as a record. These may include extra copies of documents kept only for reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibit (36 CFR 1220.18).

18. **Office of Record:** The organization, by definition of its mission or function, that has primary responsibility for maintenance and retention of the record.
19. **Permanent Record:** Any federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States, even while it remains in agency custody. The term also includes all records accessioned by NARA into the National Archives of the United States (36 CFR 1220.18). All unscheduled records are also considered permanent.
20. **Personal Files:** Also called personal papers, these 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).
21. **Record:** As defined in 44 U.S. C. § 3301:
 - (1) Includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them; and
 - a) does not include—
 - b) library and museum material made or acquired and preserved solely for reference or exhibition purposes; or
 - c) duplicate copies of records preserved only for convenience
 - (2) Recorded Information: includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.
22. **Retention:** The practice by which organizations maintain records for set lengths of time, and then employ a system of actions to either redirect, store or dispose of them.
23. **Temporary Record:** Federal records NARA approves for either immediate disposal or for disposal after a specified time or event (36 CFR 1220.18).

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 5	

24. **Unscheduled Record:** Federal records whose final disposition has not been approved by NARA. Such records must be treated as permanent until a final disposition is approved (36 CFR 1220.18).

B. As used in this policy, the following acronyms apply:

1. **ACGC:** Agency Compliance and Governance Committee
2. **AFP:** Agency File Plan
3. **A-SAORM:** Administration Senior Agency Official for Records Management
4. **CAR:** Compliance, Audit, and Risk
5. **CUI:** Controlled Unclassified Information
6. **EIS:** Electronic Information System
7. **FOIA:** Freedom of Information Act
8. **HLO:** High Level Officials
9. **IGLM:** Information Governance & Lifecycle Management
10. **IGOT:** Information Governance Oversight Team
11. **NARA:** National Archives and Records Administration
12. **OPSEC:** Operations Security

5. Policy

A. Information Assets Management

1. Information is a vital business asset. The information asset lifecycle of creation, receipt, maintenance, use, and disposition is integrated into all BPA business processes. BPA will appropriately manage its information assets in all phases of the lifecycle in accordance with prescribed laws, regulations, directives, and processes to ensure adequate and proper documentation of BPA’s organization, functions, policies, decisions, procedures, operations, or other activities. (See also section 8.1 below)
2. Users must maintain proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency (44 USC § 3101).
3. Information assets are subject to legal discovery, Freedom of Information Act (FOIA) requests, and regulatory audits and should be stored in an accessible manner to allow for these actions.

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist		Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt		Date 06/12/2024	
				Version 3.0	
					Page 6

4. Users must ensure that information assets requiring additional security under their control are properly identified and protected in accordance with BPA Policy 236-3, *Privacy Program* and BPA Policy 433-1, *Information Security*.
5. BPA maintains an inventory of Information Asset Plans (IAPs) that provide the identification, location, and retrieval of all categories of information assets created and received in the course of official business. Each organization must submit up-to-date Information Asset Plan (IAP) data to IGLM for their organization on at least a tri-annual basis.
6. BPA maintains an Electronic Information System (EIS) inventory that identifies and documents specific system components on which the information is processed and stored and will schedule for retention the information assets of those systems. Systems are scheduled during the development phase of purchase or build and must be updated when the system is upgraded, retired, or when changes occur within the system.

B. Records Management

1. Records are a category of information asset; as a Federal agency, BPA must manage its records in accordance with Federal records management regulations. Federal regulatory requirements are the same for the management of physical records, electronic records, and data.
2. Users must create, retain, and manage records electronically to the greatest extent possible with appropriate metadata.
3. Users must store records in a manner that ensures ease of access, retrieval, readability, and control for the life of the record.
4. Users must store permanent and temporary records separately (36 CFR 1222.34).
5. Users must store records and non-records separately (36 CFR 1222.34).
6. Electronic recordkeeping functionality must be either maintained or built-in to the system technical requirements management process for new or existing systems used to create or receive records. If such system functionality is not available within electronic information systems (EIS), records must be captured in a system that satisfies NARA’s Universal Electronic Records Management (UERM) Requirements. See also BPA Policy 236-13, *Overview of Electronic Information Systems* and BPA Policy 236-300, *Enterprise Data Governance*.
7. Records must be maintained and disposed in accordance with NARA approved records disposition schedules unless a legal hold is in place.
8. Organizations must recognize the legal validity of electronic and digital signatures.

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 7	

6. Policy Exceptions

- A. Exceptions to this policy may be necessary based on legitimate business needs or legal or compliance requirements. Any exceptions must be documented by the Office of Record and approved by IGLM.
- B. Personal files/papers of BPA users are not used to conduct agency business. They are generally not required to be managed according to BPA Policy 236-1 and the 236 series of BPA policy. Similar to the policy on personal use of agency IT equipment (see BPA Policy 270-6 Business Use of BPA IT Services and Equipment), limited personal files/papers are allowed. If an employee does maintain personal files/papers at work, they must be treated as follows:
 - 1. Personal files must be clearly designated as such and must be maintained separately from the organization’s information assets (36 CFR 1220.20(b)) in user’s personal network drive.
 - 2. Information about private (non-agency) matters and agency business must not be mixed in outgoing agency documents, such as correspondence and messages.
 - 3. If information about personal matters and BPA business both appear in a received document, the document is a Federal record. A copy of the document with the personal information deleted or redacted may be made and treated as the Federal record.
 - 4. Materials labeled “personal,” “confidential,” or “private,” or similarly designated, and used in the transaction of public business, are Federal records. The use of a label such as “personal” does not affect the status of Federal records (see 36 CFR 1220).

7. Responsibilities

A. Administrator:

- 1. Under the Federal Records Act, the Administrator has ultimate responsibility for compliance with this policy and is the Administration Senior Agency Official for Records Management (A-SAORM) for BPA.
- 2. Assigns functional responsibility to the Audit, Compliance & Governance Committee (ACGC) for ensuring BPA’s IGLM policy and program are in compliance with regulatory obligations.

B. Audit, Compliance & Governance Committee (ACGC):

- 1. The overarching committee with responsibility for monitoring the IGLM program and policy. It is supported by the IGOT.

C. Information Governance Oversight Team (IGOT):

Organization Information Governance	Title Information Governance & Lifecycle Management	Unique ID 236-1		
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 8

1. Chartered by the ACGC, the IGOT is responsible for ensuring that IGLM policies, principles, and standards are communicated, implemented, and understood within BPA, and for sponsoring specific information governance projects.

D. Chief Compliance Officer:

1. The Chief Compliance Officer is responsible for developing and encouraging good information handling practices amongst all members of BPA.
2. This individual will work with other ACGC members and managers whose responsibilities include information management.
3. The Chief Compliance Officer is a voting member of the IGOT.

E. Chief Information Officer:

1. Establishes and fosters ongoing collaboration between the IGLM and information technology (IT) communities to effectively manage electronic records, promote coordination in the use of information asset management applications across the agency, and ensure IT systems' compliance with IGLM program policies.
2. The Chief Information Officer is voting member of the IGOT represented by the Enterprise Shared Services Manager.

F. Chief Data Officer (CDO)

1. A senior executive responsible for Agency-wide data governance, defining data strategy, data management, data quality, and the exploitation of information.
2. BPA's Asset Manager serves in this function.
3. The Chief Data Officer is a voting member of the IGOT.

G. Office of General Counsel (OGC):

1. Issues legal hold memoranda when necessary to support actual or anticipated litigation or other legal matters, coordinating searches for purposes of discovery, and determining when such holds are lifted in accordance with BPA Policy 220-3, *Discovery and Legal Holds*.
2. Organizes, manages, and oversees the collection, preservation, review, and production of recorded information for legal processes.
3. Provides assistance and guidance for the IGLM program regarding regulations governing management of records and information including retention schedules.
4. The Assistant General Counsel for General Law is a voting member of the IGOT.

H. Agency Records Officer:

1. Chairs the IGOT.

Organization Information Governance	Title Information Governance & Lifecycle Management	Unique ID 236-1		
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 9

2. Is responsible for the overall development and maintenance of the IGLM program for BPA according to the principles in this policy. This includes drawing up guidance, promoting policy compliance, and bringing forward policies to the IGOT and the EVP of CAR for review and approval.
3. Reports to the ACGC on BPA’s Information Governance programs and policies as well as allocating resources to the IGLM program.
4. On behalf of the A-SAORM, submits a schedule identifying retention periods for the records in the custody of BPA to NARA for approval. This is Large Aggregate Flexible Schedule (also known as the *Big Bucket* schedule).
5. Ensures an up-to-date Agency File Plan and Large Aggregate Flexible Schedule are posted on IGLM’s SharePoint page off BPA Connection for consistent records retention across the Agency.
6. Oversees the development and implementation of internal controls to ensure eligible permanent records are retained long enough and protected from technological obsolescence to meet the historical needs until legal custody is transferred to NARA upon expiration of retention.
7. Approves guidance and annual training to personnel about information asset laws, regulations, and policies.
8. Reviews and approves or denies exceptions to the electronic recordkeeping requirement.
9. Conducts and documents Records Exit Interviews of departing HLO (High Level Officials).
10. Acts as a liaison with the Department of Energy and NARA.

I. BPA Library:

1. Responsible for distributing information resources that are relevant to BPA’s interests and educating the BPA workforce and public about BPA’s history and current business state.
2. Works with the ARO to ensure historical records, archival holdings, photographs, maps, architectural/engineering drawings, and other record materials are identified, scheduled, and properly preserved to support the proper preservation of BPA’s historical records.
3. Prepares and provides to the ARO an annual inventory and file plan of any records held in any on site BPA collection with historical, archival, and library value.
4. Refuses offered records from BPA personnel due to reorganizations or employee departures. The BPA Library will notify the ARO if any Federal records are offered or

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 10	

delivered to their custody. The ARO will determine if a wrongful disposition (18 USC § 2071) has occurred.

5. Manages collections of BPA records according to the NARA-approved records schedules. All permanent records must be transferred to NARA in accordance with the approved NARA schedules. BPA Historians, Archivists, and Librarians do not have authority to alter or delay a federal records schedule.
6. Ensures that no documents containing personal identifiable information (PII), protected health information (PHI), controlled unclassified information (CUI) or any other classified information is entered into library holdings.

J. Information Security:

1. Is responsible for supporting agency implementation of DOE O 471.7, Controlled Unclassified Information (CUI) through BPA’s Information Security (INFOSEC) Program including CUI, which outlines guidelines for identifying, marking, controlling, sharing, and destroying non-record copies of CUI documents and reporting mishandling or misuse following BPA Procedure 433-1-2 Identification and Control of CUI.
2. Is responsible for implementing Classified Matter Protection and Control (CMPC), which identifies, and controls classified information for purposes of national security.
3. Is responsible for implementing Operations Security (OPSEC) which identifies Critical Program Information requiring safeguard and control measures because it reveals an operational vulnerability.
4. These programs areas under Information Security collaborate with IGLM, Cyber Security, IT, Compliance, and others on security related matters pertaining to BPA’s information assets.
5. The Personnel and Information Security Supervisor is a voting member of the IGOT.

K. Continuity of Operations:

1. Continuity of Operations provides essential records support to the Primary Essential Records Liaison (PERL). See BPA Policy 236-16, *Essential Records Program*.
2. The Continuity of Operations Supervisor is a voting member of the IGOT.

L. Executives, Managers and Supervisors:

1. Are responsible for applying IGLM policy to recorded information within areas of their responsibility and ensure recorded information is managed in accordance with the IGLM policy and other information governance policies.
2. BPA managers and supervisors are expected to lead by example by promoting a culture that properly values, protects, and uses information and data.

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 11	

3. Ensures that their staff receive training, are aware of the requirements of appropriate information governance policies and apply the correct procedures and controls relevant to their work.
 4. Ensures information assets are maintained and disposed of in accordance with their organization’s IAP.
 5. On at least a 3-year cycle, submits IAPs to IGLM that document all categories of information assets created and received in the course of official business.
 6. Ensures departing employees identify and transfer information assets in their custody to an appropriate custodian in an accessible format.
 7. Advises employees in their organizations of appropriate and inappropriate storage locations for the records they handle. Employees are not to use their personal network drives for any BPA business related files.
- M. Ensures analog records are digitized according to the requirements of 236-1-1, Digitization. **BPA Users:**
1. All users have a personal responsibility for adhering to policies, principles, and procedures that help maintain the availability, effectiveness, security, and confidentiality of BPA’s information assets.
 2. Users have responsibility for information assets that they create, receive, or have some impact upon.
 3. All users must complete mandatory IGLM training on their responsibilities for managing information assets as government property.
 4. Ensure upon departing from the agency, they identify and transfer information assets in their custody to an appropriate custodian in an accessible format.
- N. **Contracting Officers:**
1. Service Level Agreements and contracts with outside vendors must include the responsibilities for the management of records and information and address all relevant aspects of information governance. For further guidance see the Bonneville Purchasing Instructions (BPI).
- O. **Mail and Media Services:**
1. Provides digitization/scanning services to the Office of Record. (see BPA Procedure 236-1-1, *Digitization*)

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 12	

8. Standards and Procedures

8.1 Information Lifecycle:

A. BPA manages all its information assets through the information lifecycle:

1. Identification is the beginning of the lifecycle and includes the creation and/or receipt of recorded information in any medium and determination of continuing business value by identifying the appropriate file code from the Agency File Plan.
2. Maintenance addresses how and where recorded information is retained. Retention means keeping recorded information for the appropriate amount of time, taking into account legal, regulatory, financial, operational, and historical requirements. Maintenance also includes ensuring appropriate access, searchability, sharing, and use of recorded information in support of business functions.
3. Disposition is the end of the lifecycle and covers action taken regarding recorded information that is no longer needed to conduct regular, current business. Disposition includes the physical destruction/deletion of recorded information, transfer of records to Federal agency storage facilities or records centers, and transfer (including legal ownership) of permanent records to NARA.

8.2 Metadata Requirements for Records

- A. Metadata for a record must, where possible, consist of:
1. A description of the content of the record;
 2. The structure of the record (form, format, and relationships between record components);
 3. And the business context in which the record was created, relationships with other records and metadata, identifiers and other information needed to retrieve the record, and the business actions and events involving the record throughout its lifecycle.
- B. Records systems must define metadata to enable the identification and retrieval of records; associate records with changing business rules, policies, and mandates (e.g., associate records with records owners, authorizations, and rights with regards to the records; associate records with their business activities; and track processes carried out on records).
- C. The metadata for a record must be protected from unauthorized deletion and must be retained or destroyed in accordance with the record's appropriate authorized retention schedule.

Organization Information Governance	Title Information Governance & Lifecycle Management	Unique ID 236-1		
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 13

- D. Once the record has been captured, the associated metadata must be fixed and kept as transactional evidence.
- E. Analog records that require digitization must follow NARA regulation on the proper procedure for digitization, including metadata, which varies depending on either the permanent or temporary status of the record.
- F. When dispositioning permanent records, metadata must be preserved and included with the transfer.

8.3 Technological Obsolescence Mitigation for Records

- A. To protect records against technological obsolescence, regardless of the storage environment and media, BPA must:
 - 1. Determine if the NARA approved retention period for the records will be longer than the life of the system. If so, agencies must migrate the records and their associated metadata before retiring the current system.
 - 2. Ensure hardware and software can retain the electronic records’ functionality and integrity regardless of the storage environment. To retain functionality and integrity, BPA must:
 - a) Keep the records in a usable format until their authorized disposition date. If records must be converted for migration, records must be maintained and disposed of in the authorized manner after conversion.
 - b) Ensure electronic forms are designed using software for screen fillable data entry, utilize digital signatures, and promote fully digital workflows.
 - c) Plan for technology obsolescence, and ensure updated hardware and software remains compatible with current data formats as necessary and data is preserved as a federal record until disposition requirements are met.
 - d) Maintain a link between records and associated metadata when converting or migrating. This includes capturing all relevant associated metadata at the point of migration (for both the records and the migration process).
 - e) Ensure verification of successful records transfers (including metadata) after migration.

8.4 Digitization

- A. Before undertaking a digitization project, the Office of Record should consider the following:
 - 1. Volume of the collection;
 - 2. Cost to digitize;

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist		Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt		Date 06/12/2024	
				Version 3.0	
				Page 14	

3. Need for availability (sharing) of the documents;
 4. Quality of the originals (including handwritten notes, degradation of original medium, etc.); and
 5. Need to preserve the originals after digitization for historical or other purposes.
- B. The Office of Record must develop a digitization project plan to meet the requirements stated in BPA Procedure 236-1-1, *Digitization*.

9. Performance and Monitoring

- A. IGLM will self-evaluate the IGLM program to ensure the program meets the regulation requirements for an agency records management program:
1. Review the Agency File plan annually to ensure the records control schedules and general records schedules citations are current.
 2. Review the Large Aggregate Flexible Schedule every 5 years to ensure accuracy.
 3. Review IGLM policies on a 3-year basis since last publication to ensure BPA’s IGLM policies cover all BPA business-related information assets.
 4. Review information governance mandatory training content annually and ensure that the training is current and relevant.
 5. Review the IGLM procedures annually to ensure the procedures are current.
 6. Conduct records management program evaluations at least every 2 years through surveillance or assessment. Evaluations may cover an individual element or the full program to ensure compliance with applicable Federal laws, regulations, DOE Orders, and NARA requirements and bulletins.

10. Authorities and Reference

- A. 44 USC ch. 31 § 3101 et seq., *The Federal Records Act*
- B. 18 USC § 2071, Concealment, removal, or mutilation generally
- C. 44 USC 3102: Establishing agency programs for management of, effective controls over, and appropriate disposal of records of temporary value.
- D. 44 USC 3105: Establishing safeguards against removal/loss of Federal records.
- E. 36 CFR Chapter XII Subpart B, National Archives and Records Administration – Records Management
- F. 44 USC 3303: Federal Records Act – Disposal of Records
- G. 5 USC § 552a et seq., The Privacy Act of 1974

Organization Information Governance	Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 15

- H. 18 USC 2071: Criminal sanctions for unauthorized removal/destruction of Federal records
- I. DOE O 243.1C, Records Management Program
- J. OMB/NARA Memo 19-21: Transition to Electronic Records
- K. OMB Circular A-130: Managing Information as a Strategic Resource
- L. BPA Policy 236-13, Overview of Electronic Information Systems
- M. BPA Policy 236-14, Overview of Communication Tools
- N. BPA Policy 236-15, Overview of Physical Media
- O. BPA Policy 236-16, Essential Records Program
- P. BPA Policy 236-200, Managing Unstructured Data as Information Assets
- Q. BPA Policy 236-260, Email Management
- R. BPA Policy 236-300, Enterprise Data Governance
- S. BPA Policy 236-2, Information Collection
- T. BPA Policy 236-3, Privacy
- U. BPA Policy 236-30, Freedom of Information Act (FOIA)
- V. BPA Policy 433-1, Information Security
- W. BPA Policy 473-2, Information Technology Policies
- X. BPA Policy 470-8 Business Use of BPA IT Services and Equipment
- Y. BPA Policy 472-1, Use of Social Media/Web 2.0 Tools
- Z. [BPA Data Strategy](#)

11. Review

The IGLM team within Information Governance is the responsible organization for managing this policy’s review. This policy is reviewed on a 3-year cycle from date of last publication. All IGLM policies are reviewed when revisions are introduced to BPA Policy 236-1, *Information Governance and Lifecycle Management* or other policies governing information management. Editorial updates to the policy and attachments may be made without IGOT and Policy Working Group review and approval.

Organization Information Governance		Title Information Governance & Lifecycle Management		Unique ID 236-1	
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024	Version 3.0	Page 16	

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
1.0	2/13/2012	BPAM 1150 published and supersedes BPAM 1122
1.1	6/2/2015	Migration of content to new BPA policy format. BPA Policy 236-1 published and supersedes BPAM 1150
1.2	5/6/2015	Revision to update IGLM Program organization change from Agency Compliance & Governance to Information Governance. Format updated to new standard.
1.3	6/17/2021	Sunset review, minor revision reconstituting the definition of <i>record</i> as it appears in 44 USC 3301 and a few other small edits
2.0	09/15/2022	Combined 236-1, <i>Information Governance & Lifecycle Management</i> , 236-11 <i>Information Lifecycle Management</i> , 236-12 <i>Large Aggregate Flexible Schedule and Agency File Plan</i> and 236-160 <i>Digitizing Records from Physical Media</i> . Incorporates changes from DOE O 243.1C and findings from a 2020 National Archives and Records Administration (NARA) inspection.
3.0	06/12/2024	Includes reference to procedure 236-1-1, <i>Digitization</i> and aligns policy roles with the procedure and other policy.

Organization Information Governance	Title Information Governance & Lifecycle Management	Unique ID 236-1
Author Candice Palen, Supervisory Government Information Specialist	Approved by Thomas McDonald, EVP Compliance, Audit, & Risk Mgmt	Date 06/12/2024
		Version 3.0
		Page 17