BPA Policy 236-13

Electronic Records Management

Table of Contents

1. Purpose & Background

A. This policy establishes requirements for electronic records management at BPA; electronic records management is the application of records management principles to electronic records and systems.

B. All Federal agencies are required to manage their records in an electronic format with limited exceptions approved by the National Archives & Records Administration (NARA).

C. Federal regulatory requirements for electronic records include:

1. Incorporating management of electronic records into BPA's records management activities,
2. Integrating records management and preservation considerations into the design, development, enhancement, and implementation of electronic information systems; and
3. Appropriately managing electronic records.

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

A. This policy sets requirements for all electronic information assets except email and other electronic messages. The policy applies to all Electronic Information Systems (EISs) created, acquired, licensed, managed, or maintained by BPA; EISs include all Structured Electronic Information Systems (SEISs), and all EISs capable of storing and maintaining electronic information such as SharePoint sites, shared drives, and other electronic storage locations.

B. Email and other electronic messages are addressed in BPA Policy 236-260, *Email Management* and BPA Policy 236-14, *Overview of Communication Tools.*

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 nonrecords 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 NARA for BPA and the General Records Schedule (GRS) from NARA.

2. **Data:** Set of characters or symbols to which meaning is or could be assigned. Data is an information asset and can be a record.
3. **Disposition:** Actions that are taken when records are no longer needed to conduct the regular current business of the agency.
4. **Disposition Authority (DAU):** The legal authorization for the retention and disposal of records as approved by NARA. For nonrecords, the disposition is established by the creating or custodial agency (36 CFR 1220.18). The application of approved schedules is mandatory except as provided under specific circumstances (see 36 CFR 1226.16 and 36 CFR 1226.18).
5. **Electronic Information System (EIS):** An information system that contains, and provides access to, computerized Federal records and other information. (36 CFR 1236.2)
6. **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.
7. **Electronic Recordkeeping System (ERKS):** Electronic Recordkeeping Systems (ERKS) are a sub-set of SEIS that meet additional records compliance requirements.
8. **Inactive Records**: A record that is no longer being used or updated for agency business functions but has not exceeded its retention schedule (therefore not eligible for disposition).
9. **Information**: Data that is organized, structured, and in context with a particular meaning.
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 nonrecord and may be structured or unstructured data.
11. **Information Asset Plan (IAP):** An inventory of an organization's information assets to include records and nonrecords. The IAP 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. **Large Aggregate Flexible Schedule:** A form of retention schedule and DAU 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.

13. **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.

14. **National Archives & Records Administration (NARA):** The Federal agency responsible for guidance and assistance to Federal officials on the management of records and 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.

15. **Nonrecord:** Informational materials that do not meet the statutory definition of "records" (44 U.S.C. 3301), have been excluded from coverage by the definition. 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).

16. **Office of Record:** The organization, by definition of its mission or function, that has primary responsibility for maintenance and retention of the record.

17. **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.

18. **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).

19. **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

        i. does not include -

1. library and museum material made or acquired and preserved solely for reference or exhibition purposes; or
2. 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.

20. **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.
21. **Shared Drives**: Also known as network drives, shared drives refer to managed shared servers which provide electronic storage space for authorized users to house federal records in supported file formats (UERM Glossary).
22. **Structured data**: Structured data refers to data that is stored in defined fields. Categories for structured data include database formats, spreadsheets, and statistical data that is the result of quantitative research and analysis, and scientific data collected by instrumentation tools during the scientific process (UERM Glossary).
23. **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).
24. **Temporary Record:** Federal records NARA approves for either immediate disposal or for disposal after a specified time or event (36 CFR 1220.18).
25. **Universal Electronic Records Management Requirements (UERM)**: The Universal ERM Requirements identify high level business needs for managing electronic records. They are baseline ERM program requirements derived from existing statutes, standards, NARA regulations, policy, and guidance. They are a starting point for agencies to use when developing system requirements. These requirements address born-digital and digitized analog records.
26. **Unstructured Electronic Records**: Records created using office automation applications such as electronic mail and other messaging applications, word processing, or presentation software (36 CFR 1236.2).
27. **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. **AFP:** Agency File Plan

2. **A-SAORM:** Administration Senior Agency Official for Records Management
3. **CAR:** Compliance, Audit, and Risk
4. **EIS:** Electronic Information System
5. **ERM:** Electronic Records Management
6. **ERKS:** Electronic Recordkeeping System
7. **IGLM:** Information Governance & Lifecycle Management
8. **IGOT:** Information Governance Oversight Team
9. **NARA:** National Archives and Records Administration
10. **OPSEC:** Operations Security
11. **SEIS**: Structured Electronic Information System
12. **UERM:** Universal Electronic Records Management Requirements

5. Policy

A. Information is a vital business asset. All information assets are (1) protected against unauthorized access, use, alteration, alienation, or deletion, and are (2) searchable, retrievable, and usable for as long as they are maintained to support agency business processes.

B. Electronic information assets, including data, must be managed throughout the information asset lifecycle in accordance with BPA Policy 236-1, *Information Governance & Lifecycle Management.*

C. 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*.

D. BPA supports multiple EISs for maintaining electronic information assets, including SharePoint, shared drives, and SEISs. Managers and supervisors must identify the appropriate EIS for their organization's information assets to best support their business processes and the information asset lifecycle. All EISs must comply with the requirements in this policy, and Section 9 of this policy describes unique requirements related to each type of EIS.

E. The EIS must be identified in the organization's IAP in accordance with BPA Policy 236-1, *Information Governance & Lifecycle Management.*

F. Records are a category of information assets, and data can also be a record. Electronic records must be managed in accordance with the records management requirements. All

EISs must comply with the requirements in this policy, and Section 9 of this policy describes unique requirements related to each type of EIS.

G. Content Manager is the agency's official Electronic Recordkeeping System (ERKS) and satisfies NARA's UERM. All inactive permanent electronic records must be maintained in Content Manager.

H. Metadata must be captured for all electronic records, consistent with the requirements in Section 8.3 of this policy.

I. Information Owners and Managers/Supervisors must ensure compliance with electronic records management requirements, including implementing the following as part of the capital planning and systems development life cycle process or at the soonest possible lifecycle refresh:

   1. Record management controls consistent with the requirements in Section 8.1 of this policy;
   2. Ensuring that all electronic records will be retrievable and usable for as long as needed to conduct agency business (i.e., for their NARA-approved retention period;
   3. Protecting against technological obsolescence consistent with the requirements in Section 8.5 of this policy; and
   4. Associating all records with the approved records schedules that pertain to each record and ensuring that records are maintained and disposed in accordance with NARA-approved records disposition schedules, unless a legal hold is in place.

J. Records must be preserved beyond their approved retention periods when they have been placed under a destruction hold, freeze, or moratorium for purposes of audits, inspections, investigations, litigation, Freedom of Information Act and Privacy Act compliance, or similar obligations. See BPA Policy 220-3, *Discovery and Legal Hold.*

K. Public/external social media platforms, or alternate tools/applications used for official government business that result in the creation of a record, require appropriate capture and management in accordance with a NARA-approved records disposition schedule.

L. Records created or received via websites and portals used for government business, website administration, operations and maintenance records must be captured and managed in accordance with a NARA-approved record schedule.

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. See Section 6.B in BPA Policy 236-1, *Information Governance & Lifecycle Management* for information about personal files/papers.

7. Responsibilities

A. **Administration Senior Agency Official for Records Management (A-SAORM)**:

1. Serves as an executive sponsor setting BPA's element specific vision and strategic direction for BPA's records management program.

2. Advocates for the agency-specific records management program and ensures that it documents the organization's activities and decisions.

3. Ensures the agency has policies and processes to protect records in any format against unauthorized removal or loss and informs agency staff of their reporting responsibilities as defined in NARA regulations and guidance.

4. Ensures records management policy is developed and provides direction on established records management goals and objectives agency wide.

5. Ensures compliance with NARA requirements for electronic records, including fully managing permanent electronic records for eventual transfer and accessioning to NARA.

6. Reports annually to NARA on the status of records management at BPA (in the annual SAORM report).

B. **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.

C. **Chief Data Officer (CDO):**

1. Responsible for Agency-wide data governance, defining data strategy, data management, data quality, and the exploitation of information.

D. **Agency Records Officer:**

1. 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.

2. Oversee 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.

E. **Executives, Managers and Supervisors:**

1. Responsible for recorded information generated by their organizations' activities.

2. Ensure electronic records are managed in accordance with IGLM policy and other information governance policies within their designated areas.

3. Advise employees in their organizations of appropriate and inappropriate storage locations for the electronic records they handle.

F. **BPA Users:**

1. Adhere to policies, principles, and procedures that help maintain the availability, effectiveness, security, and confidentiality of BPA's information assets.
2. Users have responsibility for electronic records that they create, receive, or have some impact upon.

G. **Contracting Officers:**

1. Ensure contracts with outside vendors include 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).

H. **Information Owners:**

1. Ensure SEISs comply with requirements in Section 9.1 of this policy.

I. **SharePoint Site Content Owners:**

1. Responsible for ensuring their SharePoint Site is managed in accordance with Section 9.2 of this policy and in accordance with the SharePoint Governance document.

J. **SharePoint Site Coordinators:**

1. Responsible for SharePoint site design, permissions management, and day-to-day operations in accordance with Section 9.2 of this policy and in accordance with the SharePoint Governance document.

8. Standards and Procedures

8.1 Records Management Controls (36 CFR 1236.10)

A. The following types of records management controls are needed to ensure that Federal records can provide adequate and proper documentation of agency business for as long as the information is needed. These controls can be met manually through documented processes and procedures; semi-automated, leveraging built-in retention capabilities; or automated, leveraging built-in records management features and functionality.

B. The following controls are required for all electronic records:

1. Reliability controls that ensure a full and accurate representation of the transactions or activities and can be depended upon during subsequent transactions or activities.

2. Authenticity controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

3. Integrity controls such as audit trails to ensure records are complete and unaltered.

4. Usability mechanisms to ensure records can be located, retrieved, presented, and interpreted.

5. Content mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.

6. Context mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity.

7. Structure controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

BPA must comply with the requirements found in the Universal Electronic Records Management Requirements (UERM) that contain the above controls and other Federal records management requirements. The UERM is a baseline set of requirements for all systems, including standalone systems, cloud-based systems, SaaS, (M365, SharePoint, AWS, Azure, or any location that electronically holds federal records) as part of the BPA

system development lifecycle process. Information Owners must complete the BPA Compliance Baseline checklist that identifies how the EIS meets the requirements found in the UERM.

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); and
3. 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.

D. Once the record has been captured, the associated metadata must be fixed and kept as transactional evidence.

E. 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:

i. 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.

ii. Ensure electronic forms are designed using software for screen fillable data entry, utilize digital signatures, and promote fully digital workflows.

iii. 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.

iv. 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).

v. Ensure verification of successful records transfers (including metadata) after migration.

8.4 Cloud or Third-Party Services

A. The controls described in Section 8.1 are required for all electronic records, including those stored in commercial or government cloud environments, managed services, or on-premises environments. The manager/supervisor or Information Owner is responsible for putting controls in place to monitor changes to third-party terms of service that may affect management of the records.

B. If the cloud services are changed or updated, BPA must continue to meet its records management responsibilities by migrating the records to another system or repository. The system receiving the migrated records must have appropriate security and records management controls in place to manage the records throughout the entire lifecycle, including preventing the unauthorized access or disposal of records.

9. Unique Requirements for Storage Locations

9.1 Structured Electronic Information Systems (SEIS)

A. SEISs, and the information assets contained within them, must be managed in accordance with BPA Policy 236-300, *Enterprise Data Governance*.

B. The Information Owner must be the manager of the Office of Record for an SEIS and is responsible for ensuring that SEIS and the information assets contained within them are consistently identified, declared, classified, managed, maintained, and disposed.

C. Records management controls described in Section 8.1 must be present in SEISs to ensure the reliability, authenticity, integrity, usability, content, and context of BPA records

created or received in its business processes. These controls and electronic record keeping functionality requirements are documented in NARA's Universal Electronic Records Management Requirements (UERM). If the SEIS does not satisfy NARA's UERM the records must be captured in a system that does.

D. SEISs must have an associated Electronic Information System-Description and Retention Schedule form ("EIS Form") on file with IGLM that identifies the Information Owner; the Information Assets in the system; the means of adding data (inputs) and extracting data (outputs); interoperability with other SEIS; required retentions and disposition; and the data for which the SEIS is the Source of Record (SOR).

9.2 SharePoint Sites

A. All content, permissions, and configuration of a SharePoint site must be defined and managed in accordance with the SharePoint Governance document.

B. One SharePoint Site Content Owner, typically the manager of the Office of Record or team lead delegate, must be designated and is responsible for ensuring SharePoint sites are maintained in accordance with the SharePoint Governance document.

C. DOE has collaborated with NARA and determined that SharePoint meets UERM requirements, so records are permitted to be maintained on SharePoint sites. The SharePoint Site Content Manager must implement the records management controls described in Section 8.1 of this policy to ensure electronic records in SharePoint provide adequate and proper documentation of agency business for as long as the information is needed.

D. Inactive permanent records and inactive temporary records with a retention period longer than 7 years must be stored in Content Manager.

9.3 Shared/network drives

A. On its own, a shared drive does not provide the functionality of an electronic recordkeeping system or meet the requirements in NARA's UERM. Through a combination of manual and automated policies and procedures a shared drive can be a recordkeeping system. Managers/supervisors must implement the records management controls described in Section 8.1 of this policy to ensure electronic records in a shared drive provide adequate and proper documentation of agency business for as long as the information is needed.

B. Managers/supervisors should clearly document a shared/network drive record keeping procedure that addresses naming conventions, metadata, and retentions for the materials stored in them as part of their IAP.

C. Inactive permanent records and inactive temporary records with a retention period longer than 7 years must be stored in Content Manager.

9.4 Other locations

A. Workstation PCs/Laptops (Hard Drive/Desktops):

1. Hard drives (the "My Documents" folder) or the desktop location on workstation PCs and laptops are often used for initial drafts. However, any work-related information assets initially created or maintained on a hard drive/desktop must be moved to an appropriate storage location in accordance with the organization's IAP within ninety days and the appropriate metadata and retention schedule applied.
2. Laptops have an additional security risk because of the potential for loss or theft when taken offsite from BPA locations. Because laptops have virtual private network (VPN) capabilities allowing access to BPA network servers and SharePoint sites, most materials necessary for employees to accomplish their work is easily accessible. Therefore, laptop users must maintain only the minimum information assets on the laptop that is necessary to appropriately perform their responsibilities when offsite of the agency.

B. Near-line data storage includes electronic media such as USB drives (also referred to as thumb drives or flash drives), CDs, DVDs, optical disks, diskettes, etc. They are generally considered to be those devices that store electronic information and require information technology to access. Because of their small size and portability, these devices must not be used to organize and maintain an organization's information assets. More specifically, USB drives are not to be used as the primary storage for Federal records. They can be used to maintain duplicate copies of essential records in accordance with the protection requirements in BPA Policy 236-16, *Essential Records Program.*

C. Offline data storage consists of backup tapes and disaster recovery tapes. Backup and disaster recovery tapes are the responsibility of the IT organization. They shall not be used by organizations to maintain the information assets, particularly Federal records for which they are responsible.

10. Performance and Monitoring

A. IGLM will evaluate organizations' compliance with the above requirements by:

1. Conducting records management program evaluations annually 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.

11. 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. 44 USC 3303: Federal Records Act – Disposal of Records

F. 18 USC 2071: Criminal sanctions for unauthorized removal/destruction of Federal records

G. 36 CFR Chapter XII Subpart B, National Archives and Records Administration – Records Management

H. DOE O 243.1C, Records Management Program

I. OMB/NARA Memo 19-21: Transition to Electronic Records

J. OMB Circular A-130: Managing Information as a Strategic Resource

K. BPA Policy 236-260, *Email Management*

L. BPA Policy 236-300, *Enterprise Data Governance*

M. BPA Policy 433-1, *Information Security*

N. BPA Policy 473-2, *Information Technology Systems and Services Policies*

O. NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, SI-12 Information Management and Retention

P. BPA Data Strategy

Q. NARA Universal Electronic Records Management Requirements (UERM)

12. 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.

13. Revision History

Version Number	Issue Date	Brief Description of Change or Review
2012-1	2012-11-05	Published completed original chapter, cmfrost.
2013-1	2013-09-03	Updated formatting, sect. 07, cmfrost.
2015-1	2015-08-07	Migration to new BPA policy format.
2017-2	2017-03-22	Revision to remove ERMS, add Discovery Core, update IGLM Program Organization change from Agency Compliance & Governance to Information Governance, update the definition of a short-term record and migration to the new BPA policy format, cmfrost. This was a minor revision subject to policy working group and Labor Relations review. [T. Ono]
f2019-3	2019-03-11	Added OMB Circular A-130 Language re: digital and electronic signatures
2024-1	01/14/2025	Major revision, combining 236-13 and 236-200 and covering all electronic records. Includes new requirements for use of Content Manager for specific records and incorporation of records management controls in all electronic information systems.