BONNEVILLE POWER ADMINISTRATION

BPA Policy 236-200

Managing Unstructured Data as Information Assets

Table of Contents

1. Purpose & Background

A. This policy provides information governance methodologies and guidance for Unstructured Data Management (UDM) to ensure compliance with National Archives and Records Administration (NARA) regulations on lifecycle management of Federal Record material in electronic format and use of a BPA Electronic Recordkeeping System (ERKS) under those regulations.

B. BPA uses a variety of unstructured data formats to create, receive, manage, and maintain its information assets. The nature of unstructured data allows great flexibility in supporting business processes and creating work product; but, that same flexibility can present challenges for the agency to appropriately manage, maintain, and dispose of information assets in unstructured data formats, such as:

1. Information in unstructured data formats may not be uniform and the content may concern any subject or function.
2. The content (and therefore its business value) may not be immediately discernible from the file name.
3. Important Metadata for understanding the context in which the information asset was created or received may not be easily accessible or could be missing.
4. Without recordkeeping capabilities, easy and timely retrieval of information contained in unstructured data formats (whether individually or in sets of related information assets) may be difficult.
5. Ensuring that record material is appropriately disposed according to its scheduled retention period as required by the Agency File Plan is not an inherent part of unstructured data format applications.
6. Unstructured data formats used to maintain long-term records (e.g., ten-year retention or more) may become obsolete, such that the content contained in those formats is effectively lost.

C. Meeting BPA's regulatory obligations for managing its information assets, as well as facilitating BPA's production of information as required through litigation, Freedom of Information Act (FOIA) or other requests, requires that policies, procedures, and technology standards are implemented that will appropriately address UDM challenges.

D. The objectives of UDM are to:

1. Maintain consistent, enforced retention policies;
2. Enable faster access to information;
3. Effectively organize emails and information;

4. Improve efficiency in managing, maintaining, and disposing of information assets; and
5. Reduce physical storage of information assets.

2. Policy Owner

The Executive Vice President of Compliance, Audit, and Risk Management has overall responsibility for this policy. The Agency Records Officer develops, implements, and manages this policy on behalf of the Executive Vice President of Compliance, Audit, and Risk Management.

3. Applicability

A. This policy sets requirements for managing BPA's unstructured data as information assets.

B. This policy applies to all information assets in unstructured data form that are created, managed or maintained by BPA including, but not limited to, those using the Microsoft Office Suite of products (e.g. Word, Excel, etc.), email, and digital image formats (e.g. .pdf, .gif, .tiff, etc.).

4. Terms & Definitions

A. **Discovery Core:** BPA's Electronic Recordkeeping System (ERKS), which manages, tracks, locates, and holds unstructured data to comply with current federal and legal requirements for information governance, discovery, and FOIA.

B. **Electronic Information:** Recorded information in electronic format (requiring computer technology to retrieve or access); digital content. Electronic Information includes both the content of the information asset and associated Metadata.

C. **Electronic Information System (EIS):** Computerized/digital means for collecting, organizing, and categorizing information to facilitate its preservation, retrieval, use, and disposition. These systems contain and provide access to Federal Records and other information.

D. **Electronic Recordkeeping System (ERKS):** See Structured Electronic Information System (SEIS); any SEIS that is substantially compliant with the DoD 5015.2 standard for integrity, security, and disposition.

E. **Exchange Journaling:** The process of copying all email communications in real time for the purposes of regulatory compliance and data retention for discovery, FOIA, regulatory audits, and SES Capstone only.

F. **Federal Record:** Recorded information in any medium, made or received by an agency of the United States Government 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 government or because of the informational value of data in them. Materials made or acquired solely for reference and extra copies of documents preserved only for convenience of reference and stocks of publications are not included. *See*, *Federal Records Act*, 44 USC §3301.

G. **Information Asset Plan (IAP):** A profile of the organization's information assets by process. Documents the "who, what, where, when and why" of each information asset type, and in turn, helps identify business value and management requirements.

H. **Metadata:** Structured information about any recorded information such as date and time the recorded information was created, the author, organization, or other data. This also includes descriptions of content, structure, data elements, interrelationships, indexing, and other characteristics of data and information and records.

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

J. **Short-Term Record:** Recorded information that may provide some evidence of the agency's organization, functions, or activities, but is in an incomplete or draft form. Short-Term Records have a retention period of no more than three years.

K. **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). These systems are required to have a complete, approved Structured Electronic Information System Schedule form (1324.02e) submitted to the Information Governance and Lifecycle Management (IGLM) team as part of the System Lifecycle (SLC) process. Electronic Recordkeeping Systems (ERKS) are a subset of SEIS that meet additional records compliance requirements.

L. **Transitory Recorded Information:** Recorded information with no continuing business value. This may also include recorded information made or acquired solely for reference, extra copies of documents preserved only for convenience, and stocks of publications. Transitory Recorded Information has a retention period of no more than ninety days.

M. **Unstructured Data:** Electronic information created using office automation applications such as email and other messaging applications, word processing, presentation, or similar software.

N. **Unstructured Data Management (UDM):** Policies, services and tools that aid in appropriately managing electronic information that is not contained in a database or

SEIS. UDM is designed to manage unstructured data throughout the information lifecycle.

5. Policy

A. This policy is media-neutral, meaning that unstructured data must be managed according to its content, not its format.

B. Users creating or receiving information assets in unstructured data formats must organize, manage, maintain, and dispose of them in a consistent fashion throughout BPA. This may be accomplished through functionality that is built into Electronic Information Systems (i.e., an archiving/indexing application) by transferring information assets to an Electronic Recordkeeping System (ERKS) or some combination of both. This policy is designed to accommodate systems or other technology solutions for efficiency and effectiveness, and to ensure internal controls for compliance with laws and regulations applicable to government information assets.

C. To fulfill BPA's regulatory obligations and meet the requirements of OMB Memo M-12-18, BPA's ERKS (Discovery Core) is implemented in the following locations on the BUD network:

1. SharePoint;
2. Network drives, including user files on myPC; and
3. Email.

D. Discovery Core shall be used to appropriately structure, organize, manage, and dispose of information assets in electronic form through the following six modules and their functions:

1. <u>IDOL</u>: A processing layer connecting to the BUD network locations identified in the IAPs (paragraph E below);
2. <u>Control Point</u>: A repository for indexing, analyzing, and applying policies;
3. <u>Content Manager</u>: A repository for Federal Records and their Metadata;
4. <u>Consolidated Archive</u>: A repository for journal capture of Exchange content for the purposes of FOIA, Discovery, and Capstone management (see, BPA Policy 236-261, *SES Email Content Management Through Capstone*) only;
5. <u>Legal Hold and eDiscovery</u>: An integrated solution to analyze, review, track, and respond to litigation notices and/or FOIA requests; and
6. <u>Universal Search</u>: An enterprise-wide tool that provides end-users the capability to search for short-term and Federal Record material being maintained as unstructured data across the Discovery Core domain. This includes content the end-user has permission to access in the BUD network locations identified in paragraph E below.

E. **Information Asset Plans (IAPs)**

1. IAPs, as developed by the IGLM Team and Offices of Record, are used to determine Federal Record content and provide the structure for applying required Metadata in Discovery Core for the management of those records.
2. Because incomplete or inaccurate IAPs may result in Federal Records being wrongly categorized or the misapplication of security restrictions, all Offices of Record are required to maintain current, approved IAPs with the IGLM team for all of their Federal Record content including that which is managed through Discovery Core.

6. Policy Exceptions

A. **Administrative exceptions:** The IGLM team regularly reviews the Federal Records within Discovery Core. If Federal Records within Discovery Core are identified and verified as having incorrect Metadata or having been incorrectly declared as Federal Records, appropriate corrections may be made administratively as authorized by the Office of Record, approved and performed by the IGLM team. All such authorizations, approvals, and actions must be documented and maintained by the IGLM team.

B. **Legal holds on unstructured data**

1. BPA information assets are government property and may be required to be preserved and produced in litigation; an Inspector General or other audit; or as required for compliance or business purposes. In addition, as provided for in BPAM 1110, *Business Use of Information Technology Services*, there is no expectation of privacy when using BPA IT equipment, even for personal use. As a result, information assets being maintained in any EIS – including email or networked drives – may have a legal hold placed on them. Legal holds prevent loss through the deletion or alteration of information assets. Information assets in Discovery Core subject to legal hold are retained through a preservation/collection function using the Legal Hold/E-Discovery modules.
2. Legal holds are placed by the Cyber Forensics and Intelligence Analysis team (Cyber Forensics) under the authority of the Office of General Counsel (OGC). The user may continue to have access to the information asset, but will be unable to delete or alter the preserved/collected copy, regardless of its retention period.

C. **Exchange Journaling:** For the purposes of legal holds (including regulatory audits), FOIA holds, and SES Capstone only, Exchange journaling has been enabled. A copy of all Outlook data (incoming and outgoing messages including cc and bcc messages, and calendar, tasks and notes items) will be maintained in the Consolidated Archive module of Discovery Core for three years.

7. Responsibilities

A. **Unstructured Data Users:** All users who create, receive, or access information assets in unstructured data format are responsible for determining whether the content of those information assets meets the definition of a Short-Term Record or a Federal Record as well as appropriately managing the information asset consistent with the requirements of Discovery Core and all applicable IGLM policies.

B. **Office of Record:** Each Office of Record is responsible for consistently categorizing, organizing and managing its information assets in its IAP throughout the information lifecycle in Discovery Core.

C. **Managers/Supervisors**

1. Ensure information assets within their organization are consistently identified, declared, classified, managed, maintained, and disposed in accordance with their organization's IAP; and
2. Submit IAPs to IGLM for the Federal Records and other information assets within their custody on a minimum of a three-year cycle.

D. **Agency Records Officer**

1. Manages the IGLM program policy, training, and compliance responsibilities;
2. Is the Information Owner of Discovery Core, and in that capacity sits with the Information System Owner on the managed support steering committee for Discovery Core;
3. Reviews and approves/denies requests for exceptions to this policy including classification, retention, disposition, and the taxonomy for Discovery Core consistent with the Large Aggregate Flexible Schedule and Agency File Plan; and
4. Approves IAPs for use in conjunction with Discovery Core.

E. **Information Governance and Lifecycle Management (IGLM) Team**

1. Has programmatic responsibility for developing policy and guidance on managing information assets in unstructured data format in Discovery Core;
2. Gives training on the policy contained in this policy and others in the BPA Policy 236-series, as well as federal regulations;
3. Monitors and audits unstructured data management by Offices of Record for compliance;
4. Manages the records within Discovery Core;
5. Maintains IAPs for each Office of Record;

6. Supports OGC and the Cyber Forensics team in conducting legal searches, applying legal holds, and addressing discovery requirements; and
7. Manages the records within Discovery Core.

F. **Information System Owner, Discovery Core**

1. Sits, with the Information Owner on the managed support steering committee for Discovery Core;
2. Assists in regular reporting for compliance purposes; and
3. Manages Discovery Core in accordance with the service level agreements and managed service contracts to ensure appropriate technical support according to Information Technology (J).

G. **Cyber Forensics and Intelligence Analysis Team (Cyber Forensics)**

1. Coordinates with OGC on discovery activities for litigation and investigations, and the FOIA Officer on searching collections within Discovery Core;
2. Directs and places legal holds in Discovery Core in coordination with the Office of General Counsel; and
3. Collects and manages materials from Discovery Core that may be relevant to litigation, audits, investigations and other similar forensic activities.

H. **Cyber Security Office:** Develops, issues, and enforces policy relating to BPA IT Equipment. Cyber Security's governance is based on federal laws, regulations, DOE Orders, and BPA guidelines. (See, BPA Policy 434-1, *Cyber Security Program*.)

I. **Office of General Counsel:** OGC has primary responsibility for discovery including directing the scope of legal holds and searches, and coordinating with the Cyber Forensics team to identify, preserve, and collect electronically stored information that may be relevant to litigations, investigations, or other discovery activities. The Office of General Counsel maintains the list of active litigation as well as lists of those users and resources that are on legal hold. This responsibility cannot be delegated to other organizations. (See, BPA Policy 220-3, *Discovery and Legal Holds*.)

8. Standards & Procedures

This section provides an overview of the standards and procedures for information assets being managed using Discovery Core. Detailed procedures will be documented in BPA Procedure 236-200-1 – *Discovery Core Operations* and the runbooks used for the Discovery Core Modules.

A. **Short-Term Records and Transitory Recorded Information:** Users may manage and maintain information assets meeting the definition of either Transitory Recorded

Information or Short-Term Records in any EIS (including SharePoint sites or networked drives) for their retention periods (90 days and three years, respectively).

1. **Transitory Recorded Information:** Because of the lack of business value in Transitory Recorded Information, users should delete such material as quickly as possible, but in any case within ninety days of creation or receipt. Generally, such material should not be stored in the same EIS or location as Short-Term Records and must not be managed or maintained with Federal Records. All users must actively manage any Transitory Recorded Information they create or receive to ensure it is deleted in a timely manner.
2. **Short-Term Records:** No more than three years after creation or receipt, users must dispose of a Short-Term Record either by deleting it or by allowing Discovery Core to declare it a Federal Record. A Short-Term Record may be declared "in place" or migrated to an archive appropriate for managing Federal Records.

B. **Federal Records**

1. Discovery Core identifies and declares Federal Records three years after the last modified date allowed for Short-Term Records. A Federal Record is declared in Discovery Core by assigning a unique identifier and administratively "freezing" the record so that it cannot be altered or deleted other than through the disposition process (with exceptions outlined below).
2. Availability on at least a "read-only" basis for all users of electronic information systems who have a business need for Federal Records in Discovery Core is the default access status. However, restricted access through permissions management is applied as appropriate. This may include, but is not limited to, restricting access to Federal Records per the Privacy Act, or records containing Personally Identifiable Information (PII), Critical Cyber Asset Information (CCAI), Controlled Unclassified Information (CUI), and proprietary or other sensitive information. Each Office of Record, working with the IGLM team and Operational Security (OPSEC), must identify information assets in Discovery Core that require restrictions to ensure access is limited only to authorized users. Appropriate restrictions are then placed on those records through Discovery Core.

C. **Migration of records to Discovery Core**

1. The IGLM team is responsible for developing and implementing operational plans to identify Federal Records using IAPs currently stored outside Discovery Core and for migrating those records into the system to comply with this policy. For the initial Discovery Core setup, identification and migration projects are coordinated with each Office of Record, sequenced according to risk factors identified for the Federal Records, and reviewed on a regular basis by the Information Governance Oversight

Team (IGOT). The ongoing migration of Federal Records into Discovery Core is automated and monitored by IGLM and the Cyber Forensics and Analytics team.

D. **Paper copies of electronic records:** Crucial metadata, essential for context and the integrity of an information asset in unstructured data format, is lost when converted to paper format. Therefore, Federal Records created or received in electronic format should generally be kept in native format and paper copies of those records are treated as convenience copies.

9. Performance & Monitoring

A. The IGLM team within Information Governance and the Discovery Core Steering Committee are the responsible organizations for the performance standards and monitoring plans contained in this policy.

1. **Performance Standards**

a) Discovery Core technical performance standards are maintained by the steering committee for managed support of the system.

b) Of Federal Records in the Discovery Core records management application, 99 percent have a completed classification.

c) Of Federal Records in Discovery Core identified as being subject to litigation hold, 99 percent have the appropriate hold(s) applied.

2. **Monitoring Plans**

a) Performance metrics (including, but not limited to uptime, indexing, success/failure data, disposition, use for system recovery) related to managed support of the system as determined by the steering committee; and

b) Performance metrics (including, but not limited to policies, dispositions, searches, FOIA requests, and litigation holds) developed by the IGLM, Cyber Forensics, and the managed support team for content being managed within each Discovery Core module.

B. OGC provides the IGLM team with a list of litigation holds at least every six months to ensure Federal Records under those holds are appropriately retained.

C. The IGLM team audits Discovery Core and Offices of Record for compliance with IGLM polices on a three-year cycle by identifying organizations based on a risk assessment and performing a compliance review.

10. Authorities & References

A. 44 USC 2904, 3101, 3102, 3105, *Federal Records Act*

B. 36 CFR 1235.44 – 50, *Requirements for the transfer of electronic permanent records to NARA*

C. 36 CFR 1236.1 – 6, *Subpart A – Electronic Records Management - General*

D. 36 CFR 1236.10 – 14, *Records Management and Preservation Considerations for Designing and Implementing Electronic Information Systems*

E. 36 CFR 1236.20 – 28, *Subpart C – Additional Requirements for Electronic Records*

F. OMB Circular A-130, *Management of Federal Information Resources*

G. OMB Memorandum M-12-18, *Managing Government Records Directive*

H. BPA Policy 236-1, *Information Governance and Lifecycle Management*

I. BPA Policy 236-13, *Overview of Electronic Information Systems*

J. BPAM 1110, *Business Use of Information Technology Services*

11. Review

The IGLM team within Information Governance is the responsible organization for this policy. This policy is reviewed on a three-year cycle beginning in 2019. 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.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
2013-2	10/11/2013	Published complete original chapter, cmfrost.
2.0	03/04/2019	Published revision to include migration to the new policy template and the implementation of the Discovery Core system, cpalen.