BPA Policy 236-260

Email Systems – User Policies

Information Governance

Table of Contents

1. Purpose & Background

A. This policy provides information governance policies and guidance for users of the BPA email system. In addition to user policies and procedures, IT standards for administration of email and the Exchange servers are found in section 8 of this policy.

B. Because email is integral to the way BPA performs its business functions, special considerations are necessary to appropriately manage, maintain and dispose of recorded information in this medium. However, because of its nature, email can present challenges to appropriate management as information assets due to the following (see GAO-08-699T):

1. Information contained in email is not uniform: it may concern any subject or function and document a variety of transactions;
2. Transmitted metadata associated with an email may be crucial to understanding the context of the information;
3. An email message may be part of an exchange between two or more people or even a string of multiple messages concerning a topic; and
4. Without recordkeeping capabilities, email systems may not permit easy and timely retrieval of individual records or sets of related records.

C. Policies, procedures and technologies must be implemented to address these special challenges, meet BPA's regulatory obligations for managing its information assets, and facilitate BPA's information production requirements related to litigation or other requests.

2. Policy Owner

The Executive Vice President of Compliance, Audit, and Risk Management has overall responsibility for this policy. The Agency Records Officer within Information Governance 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 the use of BPA's internal email system.

B. In addition to the information governance policies of this chapter, all email users are responsible for adhering to BPA's policies on Business Use of Information Technology

Services (see BPA Policy 470-6 Limited Personal Use of BPA IT Services) and Cyber Security requirements.

4. Terms & Definitions

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

1. **Electronic Information System (EIS):** Computerized/digital means for collecting, organizing, and categorizing information to facilitate its preservation, retrieval, use, and disposition.
2. **Electronic Recordkeeping System (ERKS):** See Structured Electronic Information System (SEIS); any SEIS that is substantially compliant with either the DoD 5015.2 or the F1000 standards for integrity, security, and disposition.
3. **Federal Record:** 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 Government or because of the informational value of data in them. Materials made or acquired solely for reference, extra copies of documents preserved only for convenience of reference and stocks of publications are not included. - see Federal Records Act, 44 USC §3301
4. **Office of Record:** The organization that, by definition of its mission or function, has primary responsibility for maintenance and retention of the record.
5. **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.
6. **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 IGLM team as part of the System Lifecycle (SLC) process. Electronic Recordkeeping Systems (ERKS) are a sub-set of SEIS that meet additional records compliance requirements.
7. **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.

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

1. **EIS:** Electronic Information Systems
2. **ERKS:** Electronic Recordkeeping System
3. **IGLM:** Information Governance and Lifecycle Management
4. **NARA:** National Archives and Records Administration
5. **PDA:** Personal Data Assistant
6. **PST:** Personal Storage Table
7. **SEIS:** Structured Electronic Information System

5. Policy

A. BPA's IGLM policies are media-neutral. Emails must be managed according to their content, not their format. The objectives of email management are to:

1. Maintain appropriate retention policies for email;
2. Consistently enforce those retention policies;
3. Enable faster access;
4. Effectively organize emails and information;
5. Improve efficiency; and
6. Reduce physical storage.

B. **Use of Personal/Non-Agency Email Accounts to Conduct Agency Business:** BPA does not allow the use of personal/non-agency email accounts to conduct agency business. However, if exceptional circumstances require the use of personal/non-agency email accounts to conduct agency business, users must "cc" their BPA issued email account to ensure the email is captured and managed according to section 5 of this policy.

C. **Email Messages In Outlook**

1. Emails in the primary mailbox (including the default folders of inbox, drafts, sent and deleted) that are transitory recorded information, with no business value, may be deleted immediately. Personnel must actively manage their email by identifying short-term records and Federal records and retaining them according to sections 5.D and E of this policy, within 90 days of creation or receipt. All emails in the primary mailbox will be automatically deleted no later than 90 days after creation or receipt. Deleted emails will be capable of restoration for an additional 30 days.

2. Should emails in the primary mailbox be determined, based on content, to be either short-term or Federal records, additional metadata must be assigned for organization and management purposes. (see sections 5.D and 5.E)
3. IT assigns a standard storage quota for mailboxes. Personnel must actively manage their email to ensure that no Federal records are deleted as a result of exceeding their storage quota. The storage quota may not be increased to retain transitory recorded information for more than 90 days or short-term records for more than three years.

D. **Email as Short-term Records**

1. Emails meeting the definition of a short-term record may be retained within the email system for longer than 90 days by tagging the email with a three year retention policy. Other restrictions based on total storage capacity may apply.
2. The three-year retention may be applied either individually to emails within the inbox or to sub-folders of emails within the inbox. IGLM provides guidance and instructions on its website for managing short-term records in email format within the email system. Users are responsible for ensuring that emails approaching their three-year retention limit are reviewed and, if determined to contain Federal record content, treated as detailed in section 5.E of this policy.

E. **Email as Federal Records**

1. If an email qualifies as a Federal record, users must move it out of the email system and into a location that maintains the email in its original or "native" format, with metadata intact and appropriate integrity, security, and availability controls in place. The Outlook Message Format ".msg" is an approved native format. Users who want to use a different format must receive approval from the IGLM team and the Cyber Forensics and Intelligence Analysis team. Non-.msg formats must meet minimum requirements for metadata retention, including but not limited to retaining:
   a) the name/email address of the sender
   b) the names/email addresses of all recipients
   c) the date the message was sent
   d) the subject line of the message.
2. The preferred electronic information systems (EIS) for managing email Federal record content, in order of preference, are:
   a) An approved and scheduled Electronic Recordkeeping System (ERKS);
   b) An approved and scheduled Structured Electronic information System (SEIS) with a defined, limited, set of Federal record file codes and retention periods;

c) An organization's SharePoint site maintained by the Office of Record; or

d) An organization's shared drive maintained by the Office of Record.

3. Information owners or Offices of Record who plan to use a SEIS must work with information system owners in the IT organization to ensure that any Federal records in email format meets the requirements found under section 5 of this policy.

4. To ensure continued security and availability, Federal record emails cannot be solely managed and maintained on laptops, desktops, local hard drives, personal networked drives or portable media.

F. **Attachments to Emails:** Although attachments to an email may be maintained and stored within the email, attachments must be reviewed on their own merits to determine record status and appropriate storage, and avoid unnecessary duplication.

G. **Personal Storage Tables (PSTs):** PSTs are user-created file folders within Outlook that typically are located on a user's personal network drive or hard drive. Due to the risk of corruption and support concerns, effective March 31, 2013, Agency email users that have been migrated to Outlook 2010 and myPC will have read-only access to their PST files. Email users will no longer be able to add to existing PST files. Use of PSTs has been replaced by a larger primary mailbox for short-term records only. In accordance with section 5.E, all Federal records in email format must be moved from the email system to an electronic information system.

H. **Paper Copies of Email**

1. General. Paper copies of email are discouraged and may only be kept for convenience or reference and treated as a short-term record; that is, destroyed within two years of the created/received date.

2. Federal Records. Paper or other non-native formats are discouraged. In those instances where it is necessary to preserve an email as a Federal record in a non-native format, the Office of Record must document the reasons for not using native format in storing the email as well as the format and location in which the email will be stored.

3. Because functionality and crucial metadata, essential for context and for the integrity of emails is lost when converted to paper format, as of January 1, 2014, emails with Federal record content shall not be maintained in paper format except as a convenience copy. This policy does not apply to Federal records of Emails in paper format existing prior to 2014.

I. **Unmanaged System Mailboxes:** Many BPA systems provide automated email notifications to users (often referred to as "broadcast emails"), which aid in the efficiency of administrative processes. Unmanaged system mailboxes will comply with the retention rules set under section 5.C as well as storage quota set by IT

J. **Public Folders:** Public Folders are a legacy means to collect, organize, and share information with other people in your workgroup or organization using the Exchange email system. Effective January 28, 2013, new Public Folder use will be restricted. Effective April 2, 2018, existing Public Folders will be read-only.

K. **Unified Voice Messaging Systems:** Exchange 2010 is capable of storing voice messages as either text or audio files. Typically, these voicemails can be accessed through email as either a text or as an audio file attached to an email. In either instance, users are required to treat voice messaging within the email system as emails with the same integrity, security, availability and retention as textual emails. See BPA policy 236-13 Overview of Communication Tools, section 8.E.3 for general policies on voicemail recordings.

6. Policy Exceptions

A. **Shared Mailboxes:**

1. Shared mailboxes (such as HELPDESK or HRHelp) are used by organizations as a message center to facilitate support services to agency personnel. As such, they are a limited exception to the policies detailed in section 5.A of this policy. Shared mailboxes must comply with the retention rules set under 5.C as well as storage quotas set by I.T. Any exceptions must be reviewed and approved by the Infrastructure Administrative Services group, the IGLM team and the Office of General Counsel, as outlined in paragraph 3 of this section.
2. Creation of a new shared mailbox using the default policies of section 5.A requires review and approval by the Infrastructure Administrative Services, and scheduling by the IGLM team. Scheduling includes identifying the following:
   a) the business purpose of the shared inbox;
   b) an information owner responsible for compliance with IGLM policy;
   c) all users with access to the shared inbox;
   d) an information asset plan for the shared inbox; and
   e) any exception (approved by IGLM) to the default email policies.
3. Creation of a new shared mailbox with non-default retention rules or storage capacity or changes to existing storage capacity or other capabilities of a shared mailbox, requires review and approval by the Infrastructure Administrative Services group, the IGLM team, and the Office of General Counsel. To request changes the following must be documented:
   a) Information owner for the shared mailbox (usually the manager of the organization providing the service).

b) The business process involved and justification for exception to the default policy.

c) Agreement that the mailbox's information owner is responsible to inform the Infrastructure Administrative Services group when the mailbox information owner changes or the mailbox is no longer required.

d) Acknowledgement that the mailbox will not be used for Federal Records storage.

4. Review and Approval Process

a) Submit the above documentation to the IGLM team through IGLM mailbox.

b) The IGLM team, the Infrastructure Services group, and the Office of General Counsel will review request and document the decision including any exceptions granted. This documentation will be included as part of the scheduling process in paragraph 2 of this section.

B. **Legal Holds:**

1. As provided for in BPA Policy 470-6 Limited Personal Use of BPA IT Services, there is no expectation of privacy when using the BPA email system, even for limited personal use allowed under the policy. Emails are information assets, and the property of BPA. They may be required to be preserved and produced for business purposes, compliance, litigation, and internal, Inspector General or other audits. Emails being maintained in any EIS may have a legal hold placed on them under the authority of the Office of General Counsel (OGC). Legal holds prevent loss through the deletion (including the auto-delete function) or alteration of emails. Mailboxes on legal hold retain email in the mailbox and the deleted items folder (or other administrative database) until the hold is removed.

2. Legal holds are placed by the Cyber Forensics and Intelligence Analysis team ("Cyber Forensics") under the authority of OGC. The user will continue to see the 90-day and three year retention, but those emails will be held on the server. The Cyber Forensics and Intelligence Analysis team may copy emails for review and production purposes.

3. As of October 1, 2016, BPA instituted journaling for all Outlook content using Discovery Core. Discovery Core, through the Consolidated Archive module, preserves a copy of all incoming and outgoing email messages (including cc's, bcc's, and distribution lists), email metadata, calendaring, notes, and task items.

4. All Outlook content retained through journaling is a copy and is used to fulfill BPA's obligation to appropriately maintain record material for responding to FOIA or litigation requests. Personnel using Outlook will not have access to journaling content and must manage and maintain Outlook content in accordance with BPA

policy 236-260 Email for business purposes for continued access in support of business functions.

5. In addition to placing legal holds on mailboxes and journaling, OGC and Cyber Forensics may also direct that existing backup tapes of the email system be held and maintained.

7. Responsibilities

A. **Email Users:** Both senders and receivers are responsible for (1) determining whether the content of an email meets the definition of a Federal record and (2) managing Federal Records appropriately based on that determination.

B. **Shared Exchange Resources (Shared Mailbox, Public Folder) Owners:** The owner of the Shared Exchange Resources is responsible for ensuring compliance with retention periods, access and life-cycle. All users of these Exchange resources are responsible for determining whether the data content meets the definition of a Federal Record. Additionally, the owner of Exchange resources must provide notice to the Exchange Administration team when the resources are no longer required.

C. **IT Infrastructure Administration Services – Email/Exchange Team:** The Email/Exchange team is responsible for implementing the IGLM policies of this chapter including retention periods; providing regular reports for compliance purposes; and managing the email environment in accordance with the service level agreements that have been developed to ensure appropriate information management standards. The Email/Exchange team shall implement legal searches and holds as required by the Cyber Forensics team and OGC. The Email/Exchange team may assign to the Cyber Forensics team those technical capabilities necessary to conduct legal searches and holds.

D. **IGLM Team:** The IGLM team is responsible for developing policy and guidance on managing information assets in email format both within and outside of the BPA email system; training on the policy contained in this and other IGLM Manual chapters as well as Federal regulations; monitoring and auditing use of the BPA email system for compliance; and supporting OGC and the Cyber Forensics team in conducting legal searches, applying legal holds, and addressing e-discovery requirements.

E. **Agency Records Officer (ARO):** The ARO manages the IGLM program for policy, training, and compliance responsibilities. The ARO reviews and approves/denies request for exceptions to policies in this chapter including retention and size limits for inbox, use of .PST files, alternative formats, and storage of information assets in email format.

F. **Cyber Forensics and Intelligence Analysis team ("Cyber Forensics"):** The Cyber Forensics team within the Cyber Security Office is responsible for coordinating with OGC on e-discovery activities including legal search and holds; directing and applying legal

holds for the email system in coordination with the Email/Exchange team; and collecting and managing materials from the email system through journaling or otherwise that may be relevant to litigation, audits, investigations and other similar forensic activities.

G. **Cyber Security Office:** The Cyber Security Office is responsible for development, issuance, and enforcement of policy relating to BPA IT Equipment. Cyber Security's governance is based on federal laws, regulations, DOE Orders and BPA guidelines (BPA Policy 470-6 Limited Personal Use of BPA IT Services).

H. **Office of General Counsel (OGC):** OGC has primary responsibility for e-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 litigation, investigations or other e-discovery activities. The Office of General Counsel maintains the list of active litigation matters as well as lists of those Exchange users and resources that are on legal hold. This responsibility cannot be delegated to the Email/Exchange team.

8. Standards & Procedures

A. The Information Technology organization assigns individual user names, also known as email addresses, for primary mailboxes. "Alias" user names, "Sent As" capabilities or non-primary mailboxes are not permitted except as provided in section 5.I and 6.A of this policy. The standard "Sent on Behalf of" feature is allowed. The Email/Exchange team maintains a list of current users and the "Sent on Behalf of" designees.

B. Per NARA Regulation 36 CFR 1236.22, BPA email messages must be retrievable in their original format with all metadata intact and retain the following metadata regardless of the system in which they are maintained (i.e. primary mailbox folders or other EIS):

   a) Names of senders and all addressee(s);

   b) Date/time stamp the message was sent (or received); and

   c) Attachments that are integral to the message.

C. Emails must be searchable based on the required metadata. The email system shall index the email and associated files for future search and retrieval.

9. Performance & Monitoring

A. The IGLM team within Information Governance, Cyber Forensics, and the Email/Exchange team are responsible for performance standards and monitoring plans contained in this policy.

1. Performance Standards

    a) The email system technical performance standards are maintained by the Email/Exchange team.

    b) 99% of all mailboxes should have an authorized archiving and retention policy applied.

    c) 99% of mailboxes that are required to be on litigation hold have the appropriate hold(s) applied.

2. Monitoring Plans

    a) Email/Exchange team provides annual reports to the IGLM team on:

        i) Mailboxes over 4 GB of content

        ii) Shared mailbox owners

        iii) Retention policy exceptions identified in section 6 of this policy

        iv) PST files [list name, location, size, last used date, owner]

        v) Public Folders in the Exchange 2010 system

    b) Performance metrics that are related to IGLM policy, these Performance Standards, and Exchange service level agreements.

B. The IT organization provides annual reports on:

    1. Backups for the Exchange 2010 system [schedules, success/failure data, disposition, use for system recovery]

    2. Unified Messaging/Voicemail in conjunction with the Exchange 2010 system

    3. OGC provides the Email/Exchange and IGLM teams with list of mailboxes requiring the litigation hold at least every six months.

C. The IGLM team audits email for compliance with IGLM policies on a three-year cycle by identifying organization based on a risk assessment and performing a compliance review.

10. Authorities & References

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

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

C. 36 CFR 1236.10 – 14: Records Management and Preservation Considerations for Designing and Implementing Electronic Information Systems

D. 36 CFR 1236.20 – 28: Subpart C – Additional Requirements for Electronic Records

E. OMB Circular A-130: Management of Federal Information Resources

F. OMB M-12-18: Managing Government Records Directive

G. BPA Policy 470-6 Limited Personal Use of BPA IT Services

11. Review

The IGLM team within Information Governance is the responsible organization for managing this policy's review. This policy is reviewed on a three-year cycle beginning in 2015. 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.

12. Revision History

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

Version Number	Issue Date	Brief Description of Change or Review
1999-1	1999-09-30	Electronic Mail (Email) Policy published
2013-1	2013-09-03	IGLM Manual Chapter 260 published - original chapter replacing Electronic Mail policy
2015-1	2015-05-01	Migration to new BPA policy format. Includes updates re: use of personal email.
2016-1	2016-12-09	Revision to update legal holds on mailboxes/journaling capabilities, 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.
2017-2	2/15/2018	Revision to § 5.J clarifies that Public Folders will be read-only, starting April 2, 2018. As previously written, it was unclear when this would occur. This is a minor revision. The effective date remains unchanged.