U.S. General Services Administration (GSA)

GSA Order: Email and Information Technology (IT) Device Data Retention Policy
CIO 1828.2A
Office of Digital Infrastructure Technology and Office of Corporate IT Services
IDTX@gsa.gov

Purpose:

This policy provides guidance for implementing and managing the records retention of General Services Administration's (GSA) email messages, attachments, and IT device data as required by OMB M-19-21, Transition to Electronic Records, and the Federal Records Act, as amended.

Background:

1. OMB M-19-21, *Transition to Electronic Records* provided that "Federal agencies have been required to manage all (permanent and temporary) email records in an electronic format since 2016 and are expected to continue to do so."

2. On January 5, 2023, NARA Bulletin 2023-02 expanded its existing guidance on retaining the emails of High-Level Officials (known as Capstone officials) to similarly apply to other types of electronic messages for preservation. For recordkeeping purposes, GSA has two categories of email records scheduled with the National Archives and Records Administration (NARA) based on the role of the email account user. The schedule was originally submitted to NARA in November 2016.

3. GSA complies with the Federal Records Act by ensuring all agency records are preserved according to agency records schedules. In some cases, this may mean records are preserved in more than one place. The role-based capture of emails does not eliminate the requirement that employees with their individual GSA email accounts maintain complete recordkeeping files in their appropriate, subject, case or project file.

4. This Order provides guidance on how determinations are made regarding the retention and management of email and IT device data.

5. IT devices include but are not limited to GSA-furnished computer workstations, laptops, and mobile devices such as cell phones and tablets. IT device data include electronic records, files, and texts stored on IT devices.

Applicability:

1. This Order applies to all GSA employees, political appointees, contractors, and

other individuals who possess a GSA IT device(s) and/or a GSA-supported email account.

2. The Office of Inspector General (OIG) is exempt from this Order. The OIG has set up its own email records management policy, using the same GSA records schedule for its email system.

3. This Order applies to the Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act.

4. This Order does not supersede any elements of GSA Directive CIO 1820.2 Records Management Program. This Order does not eliminate the requirement that employees maintain complete recordkeeping files with the inclusion of records created or received in email.

Cancellation:

This Order cancels and supersedes CIO 1828.2 Email Retention Policy, dated October 27, 2021.

Summary of Changes:

This order provides for consistency with Federal requirements and program implementation changes. This order:

1. Expands the management and retention of records to IT device data
2. Updates outdated references and links

Roles and Responsibilities:

The Office of GSA IT is responsible for:

1. Retrieval, storage, and management of email and IT device data in accordance with this order and GSA records retention schedule.

The Office of General Counsel (OGC) is responsible for:

1. Coordinating with GSA IT, records officers, and OHRM to implement the preservation of departing employee information that is subject to a litigation hold.
2. Ensuring that any materials of departing employees are preserved in a manner which identifies the matter, specific litigation hold, and the individual (custodian) who was the source.
3. Communicating and issuing litigation hold notices and releases to all parties involved.

Signature

/S/_____ _4/21/25_____

DAVID SHIVE
Chief Information Officer
Office of GSA IT

Date

Explanation of Email and IT Device Data Retention Schedule:

Within GSA, the policy for the management and retention of email records and associated GSA-furnished IT device data varies between High-Level Officials (10 categories as defined by NARA NA-1005) and all others, such as other employees and contractors.

1. **Email Records Retention**. The following records retention schedules apply:

    a. **High-Level Officials**. Sent and received emails and associated attachments for High-Level Officials are considered “permanent” records. These records will be retained and decommissioned after 15 years. Following the 15 year retention period, the records will be transferred to NARA electronically for permanent retention.

    b. **All Other GSA Employees and Contractors**. Sent and received emails and associated attachments will be retained for 7 years and destroyed at the end of each fiscal year at the end of the 7th year. If users feel that any email needs to be kept longer than 7 years, they must take action to save a copy of that email in a system outside of GSA’s email system. To save email, users can convert them to PDF and store them appropriately for other business or reference purposes.

    c. **Litigation holds**. Email records held for litigation or investigative purposes will be retained until the investigation is completed. At the end of the fiscal year, when the litigation hold is lifted, email records greater than 7 years or 15 years, as applicable, shall be destroyed or transferred to NARA. Otherwise, email records that have not reached their 7 or 15 year high retention requirement, as applicable, after the litigation hold is lifted, shall be retained.

    d. **Business Reference Use Extension**. Users are reminded and encouraged to regularly review email retained for business reference use to determine if there is still a business need to retain the email or if it may be destroyed. If a user feels that specific email needs to be preserved longer than the 7 or 15 years (for High-Level Officials), then that user may retain specific electronic messages for business reference use. GSA users can find details about how to retain specific email for business reference use on GSA Email Management on InSite.

2. **IT Device Data Retention**. The following retention schedules apply:

    a. **High-Level Officials**. Upon departure of High-Level Officials, IT devices including computer workstations, laptops, and mobile devices such as cell phones and tablets; will be placed in secured physical storage with an associated Chain of Custody document.

i. **Physical equipment.** Physical IT devices for High-Level Officials are retained for a period of 2 years and disposed of following a minimum of 2 fiscal years of secure storage.

ii. **IT device data**. Electronic records, files, and texts on IT devices for High-Level Officials are considered "permanent" records. Upon High-Level Officials' departure, all data will be retrieved from IT devices and stored securely on a network drive folder. These records will be decommissioned after 7 years and then transferred as necessary to NARA electronically for retention.

iii. **Network and personal drive data**. All data for High-Level Officials stored on network drives are considered "permanent" records. Upon High-Level Officials' departure, all data will be retrieved from network and personal drives and stored securely on a network drive folder. These records will be decommissioned after 7 years and then transferred as necessary to NARA electronically for retention. Network drives are automatically backed up daily. Network drives are also archived on a monthly basis and transferred to a third party facility for storage for a period of 7 years.

b. **All Other GSA Employees and Contractors**. Upon departure of the GSA employee or contractor, IT devices including computer workstations, laptops, and mobile devices such as cell phones and tablets will not be retained.

i. **Physical equipment**. Physical IT devices of other GSA employees and contractors will not be retained and will be refurbished immediately.

ii. **IT device data**. Electronic records, files, and texts on IT devices for other GSA employees and contractors will be erased and refurbished immediately in accordance with the GSA Offboarding Process.

iii. **Network and personal drive data**. All data files for other GSA employees and contractors are retained and ownership of the files are transferred to their GSA supervisor or to a designated employee identified by the GSA supervisor. Network drives are automatically backed up daily. Network drives are also archived on a monthly basis and transferred to a third party facility for storage for a period of 7 years.

c. **Litigation holds.** Physical IT devices, local and network drive data held for litigation or investigative purposes will be retained until the investigation is completed. At the end of the fiscal year, when the litigation hold is lifted, IT device data shall be destroyed for all other GSA employees and contractors. For High-Level Officials, IT device data that

have not reached their 7 year retention requirement, as applicable, after the litigation hold is lifted, shall be retained.

3. **Exceptions**. Exceptions to this policy must be in the form of a federal regulation or a presidential executive order. If there are positions that are considered exempt from this policy, such exemption must be approved by the Email Records Governance team. The Email Records Governance team is composed of representatives from OHRM, the Office of General Counsel, and GSA IT (appointed by the heads of these offices as necessary) and will be convened and managed by the Agency Records Officer to confirm and document the decision to exempt the position from this policy. The Agency Records Officer shall be contacted at records@gsa.gov to start such a review.

Summary of Email and IT Device Data Retention Schedule:

Data Type	High-Level Official	All Other GSA Employee or Contractor
Email	15 years	7 years
Physical Equipment (computer workstations, laptops, cell phones, and tablets)	2 years	Data is deleted and device is refurbished immediately
IT device Data	7 years	Data is deleted and device is refurbished immediately
Network and Personal Drive Data	7 years	Data is backed up daily and archived monthly on tape and transferred to a third party facility for 7 years. Specific employee data is transferred to a designated employee identified by GSA supervisor upon departure

Authorities:

1. 44 U.S.C. Chapters 21, 29, 31, and 33
2. 36 CFR Chapter XII, Subpart B – Records Management

3. OMB M-12-18, Managing Government Records Directive
4. OMB M-19-21, Transition to Electronic Records
5. OMB M-23-07. Update to Transition to Electronic Records
6. NARA Bulletin 2023-02. Expanding the Use of a Role-Based Approach (Capstone) for Electronic Messages
7. CIO 2160.2B CHGE 4 GSA Electronic Messaging and Related Services Policy