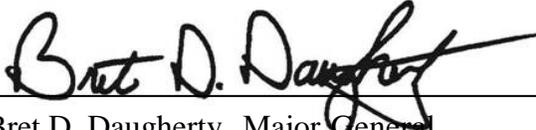




## Department Policy No. DIR-005c-13

<b>Title:</b>	Email and Calendar Items
<b>Authorizing Source:</b>	<a href="#">Title 40 RCW</a> , <a href="#">Ch. 434-610 WAC</a> , <a href="#">Ch. 434-615 WAC</a> , <a href="#">Ch. 434-626 WAC</a> , <a href="#">Ch. 434-640 WAC</a> , <a href="#">Ch. 434-662 WAC</a> , <a href="#">Ch. 434-663 WAC</a> , <a href="#">Ch. 434-677 WAC</a> , and <a href="#">Ch. 434-690 WAC</a>
<b>References:</b>	DIR-005-08, WMD Form 0009-13, WMD Form 0011-13
<b>Information Contact:</b>	Washington Military Department Records Officer Building 1 (253) 512-8108
<b>Effective Date:</b>	September 11, 2013
<b>Mandatory Review Date:</b>	September 11, 2017
<b>Revised:</b>	New
<b>Approved By:</b>	 Bret D. Daugherty, Major General The Adjutant General Washington Military Department Director

### Purpose

To ensure that Washington Military Department (WMD) email and calendar items are preserved, stored, retained, transferred, destroyed, and disposed of in accordance with Washington State law, administrative codes, and Secretary of State Guidelines.

### Scope

This policy applies to all WMD email and calendar items that are created, received by, or maintained by the WMD in connection with the transaction of public business. Any WMD employee or volunteer who creates, receives, or maintains WMD email and calendar items must comply with this policy.

### Policy

Emails and calendar items are subject to the same records retention requirements that apply to any other electronic or non-electronic records. The retention period for an email or calendar item is based upon its content according to the General Records Retention Schedule or the WMD Unique Records Retention Schedule.

WMD employees use Microsoft Outlook software to manage email and calendar items. Within the first 30 days of sending or receiving email, or adding calendar items, email and calendar items reside on a WMD Exchange server. After 30 days, non-deleted sent or received email and calendar items automatically move from the Exchange server to the Symantec Enterprise Vault (“vault”) system hosted by Consolidated Technology Services (CTS). Users continue to use Outlook to access, search, and organize vaulted email and calendar items until the email or calendar item “expires” (is automatically deleted from the vault) when its retention period is met. Users can identify email that has not been vaulted by its envelope icon, and vaulted email by its icon, which shows an arrow pointing to a box.

Email and calendar items shall be managed in accordance with these guidelines, except in cases of a legal, public records request, audit, or other hold on the records:

**A. Email and Calendar Items With Minimal Retention Value (GS 50002)**

1. Users shall delete email and calendar items with minimal retention value (see definition) within 30 days of the date created, sent, or received, before the email or calendar item enters the vault.
2. Users may retain email and calendar items with minimal retention value longer than 30 days if the email or calendar item is being used as a reference or continues to serve a business purpose.
3. Once a vaulted email or calendar item with minimal retention value no longer serves any purpose, the user shall move the email or calendar by clicking, dragging, and dropping it into the retention folder with the shortest retention period. This will ensure the email or calendar item is “expired” and fully deleted from the vault.
4. Users shall not use Outlook’s “delete” function to delete vaulted email or calendar items, since this will not remove it from the vault.

**B. Email and Calendar Items With a Retention Period of 30 or More Days**

1. Users shall review the General Records Retention Schedule and WMD Unique Records Retention Schedule, and become familiar with each record series the User works with. Some email and calendar items may fit within one of the correspondence record series listed below, but others may be part of a topic-specific record series that includes correspondence as well as non-correspondence records (for example, subject files or legal issues files). The descriptions below are for illustrative purposes; you must consult the retention schedules for full descriptions and up-to-date retention information.
  - a) General Correspondence (GS 09005)
    - i. This record series includes routine correspondence concerning day-to-day office administration and activities, and is to be retained for 30 days after the date of the document, and then destroyed.
  - b) Program Correspondence (GS 09022)
    - i. This record series includes internal and external communications to or from employees (including contractors and volunteers), that are made or received in

connection with the transaction of public business, and that are not covered by a more specific record series. These records are to be retained for two years after the communication is received or provided, and then destroyed.

- c) Executive/Official Correspondence (GS 10007)
  - i. This record series includes internal and external communications to or from the agency's elected official(s) and/or executive management concerning policy issues, concerns, actions or issues, and that are not covered by a more specific record series. These records are to be retained for four years after the communication is received or provided, and then transferred to the Washington State Archives for appraisal and selective retention.
2. Email will automatically enter the vault 31 days after it was sent or received.
3. Users may manually place items into the vault prior to the 31<sup>st</sup> day by selecting the item and clicking the Store in Vault icon on the toolbar; or by selecting the Tools menu and clicking Enterprise Vault > Store in Vault.
  - a) If an item was manually vaulted by mistake, and is pending ingestion into the vault, the User may "undo" the action by clicking the Cancel Operation icon on the toolbar, or by selecting the Tools menu and clicking Enterprise Vault > Cancel Operation.
4. Once items are vaulted, the User must ensure the item is in the appropriate retention folder based on the item's retention series and retention period.
  - a) Users will automatically receive retention folders for the most common retention periods, including but not limited to:
    - i. 0001 day retention – for records with minimal retention value, or records that have met their retention period and should be immediately destroyed
    - ii. 001 year retention – for records with minimal retention value that will remain active within a one-year period, or records with a retention period of up to one year
    - iii. 007 year retention – this applies to all items in the Inbox, subfolders of the Inbox, and subfolders of the mailbox that are not stored under another retention folder. It is the default retention period for vaulted items.
  - b) Users may request additional retention folders from the Records Officer to accommodate other retention periods by completing a Request for Email Retention Folder form (WMD Form 0011-13). If the User has email or calendar items designated Archival or Possibly Archival, the User will be provided a 100 year retention folder upon request.
5. Users will move items to the appropriate retention folder by clicking, dragging or dropping the item into the folder; or by right-clicking the item and selecting "Move to Folder."

### **C. Draft Email**

1. Email in the Outlook "Drafts" folder will not automatically move to the vault.

2. The “Drafts” folder is intended for temporary storage of email drafts only, and may not be used for any other purpose.
3. Users must review the contents of this folder and delete unneeded drafts on a frequent basis.

**D. Email in the “Deleted Items” Folder**

1. Email in the Outlook “Deleted Items” folder will not automatically move to the vault.
2. The “Deleted Items” folder is intended for temporary storage of deleted items, and may not be used for any other purpose.
3. Users must empty the contents of the “Deleted Items” folder either upon exiting Outlook or on a frequent basis to keep this folder’s contents at a minimum.

**E. Personal Storage Files (PST)**

1. Users may not create PST files unless they have been approved by their division director or designee, and the WMD Records Officer, to do so for an approved purpose or a specific business function.
  - a) Approved purposes include, but are not limited to, fulfilling public records requests, completing management-directed audits, or complying with requests by or requirements of the Attorney General’s Office, State Auditor’s Office, Secretary of State’s Office, or another agency performing an audit, regulatory, administrative, or similar duty.
2. To request the ability to create PST files, a User shall complete WMD Form 0009-13 and submit it to their Division Director or designee. If approved, the Division Director or designee will submit the form to the WMD Records Officer for IT coordination and approval.

**F. Legal Holds on Email or Calendar Items**

1. The Public Records Officer or designee, and the Risk Manager or designee, have the authority to place a hold on the expiration of email or calendar items subject to an open public records request or pending or anticipated litigation, and to remove that hold when the request is complete or all legal actions are final.
2. If a hold on email or calendar items exists, the Public Records Officer or designee will, to the extent necessary:
  - a) Direct certain employees to manually vault email or calendar responsive to the hold; and/or
  - b) In coordination with the Information Technology Division and/or Consolidated Technology Services, automatically ingest certain User’s email and calendar items into the vault; and
  - c) Perform searches of vaulted email and calendar items through Symantec Discovery Accelerator software and, through the software, place a hold on certain search results to suspend expiration of those emails and calendar items.

## **G. Searching the Vault**

1. Users may search for items in their vault by:
  - a) Clicking the Search Vaults icon on the toolbar, or by selecting the Tools menu and clicking Enterprise Vault > Search Vaults.
  - b) Completing the fields in the form to search for items.

## **H. Sharing Permissions to Outlook Folders**

1. Users may opt to share access to their Outlook folders with other WMD employees. This may be useful for centrally locating email on certain topics within an office, or collaborating on common projects or job functions.
2. To share a User's Outlook folder with a coworker, the User may:
  - a) Open Outlook, and select and right-click the folder you wish to share.
  - b) Click Change Sharing Permissions, and then click Add.
  - c) Search for your coworker's name, and click Add.
  - d) Choose the appropriate permission settings.
  - e) Click Apply and OK.
3. To view an Outlook folder that was shared by a coworker, a User may:
  - a) Open Outlook, and select the Tools menu.
  - b) Click Options.
  - c) Select the Mail Setup tab, and click Email Accounts.
  - d) Click Change, and then click More Settings.
  - e) Select the Advanced tab, and click Add.
  - f) Type the name of the coworker who shared their Outlook folder with you in this format: [last name], [first name] (MIL), and click OK.
  - g) Now you should see the coworker's mailbox listed under "Open these mailboxes."
  - h) Click OK.
  - i) Click Next, then Finish.
  - j) Scroll to the coworker's mailbox name on your left navigation pane, and click "+" to expand the mailbox. You should see the folder(s) your coworker has shared. Depending on the permission level your coworker assigned you, you may view, add to, move, delete, and/or edit the contents of the folder.