**Directory and Messaging Services**  
**Enterprise Exchange 2013**

<table>
<thead>
<tr>
<th><strong>Title:</strong></th>
<th>Access to Exchange ESI by Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose:</strong></td>
<td>General Communication</td>
</tr>
<tr>
<td><strong>Number:</strong></td>
<td>2015-11</td>
</tr>
<tr>
<td><strong>Date Effective:</strong></td>
<td>06/15/2015</td>
</tr>
<tr>
<td><strong>Date Expires:</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Scope:</strong></td>
<td>Enterprise Exchange 2013</td>
</tr>
<tr>
<td><strong>Authority:</strong></td>
<td>C.G.S. § 4d-7</td>
</tr>
<tr>
<td><strong>Distribution:</strong></td>
<td>Agency IT Managers</td>
</tr>
<tr>
<td><strong>Audience:</strong></td>
<td>Agency Legal, IT and FOI Staff</td>
</tr>
</tbody>
</table>

**Summary**

From time to time, DAS/BEST receives inquiries into the availability of certain electronically stored information (ESI) associated with one or more accounts that may reside on the state’s Enterprise Electronic Mail system (Exchange). This bulletin is intended to provide agencies with an understanding of what ESI is available in Exchange and how access to Exchange ESI may be granted to support an agency’s FOI or eDiscovery needs.

**Exchange ESI**

Exchange ESI exists in the following formats: electronic mail messages, calendar events, contacts, notes, and tasks. Each of these items are unique content types in Exchange. Exchange ESI can also include other content embedded as physical attachments, such as a document or image that did not originate within Exchange. Exchange ESI is stored in a proprietary Exchange database that is located on an Exchange server. Each user, or account-holder, is assigned a dedicated mailbox that may contain some or all Exchange content types.

**Ownership of Exchange ESI**

Account-holders are considered the custodians of their mailbox and are responsible for managing its content in accordance with applicable regulation or policy governing record retention practices. Agencies have control over the Exchange ESI associated with their agency and are best positioned to understand the nature and type of content that may be stored in an account-holder’s mailbox.

DAS/BEST has no custody or control over Exchange ESI except for that which may be required for the proper administration and management of the Exchange environment. Accordingly, DAS/BEST does not review or evaluate Exchange ESI for responsiveness on behalf of an agency for matters related to FOI or eDiscovery.
Exchange User Accounts

The account-holder is the individual responsible for making decisions on the disposition of mailbox content in accordance with applicable federal, state or agency record retention requirements. Unless otherwise disposed\(^1\) of by the account-holder, all data should remain online. Within Exchange, a mail account can either be active or disabled, as described below.

**Active Accounts**

An Active Account is one that is assigned to an active state employee or contractor and where that account is capable of sending and receiving mail, scheduling events, and has access to the other features of Exchange.

**Disabled Accounts**

A Disabled Account is one that is associated with an account-holder who is no longer assigned to the agency and where the account was disabled by an authorized member of the agency staff or by someone on the DMS team at the request of the agency.

**DAS/BEST does not take any action to disable an account until formally requested to do so by the agency, even if we become peripherally aware that an employee or contractor has left an agency.**

A mail account is disabled by removing the account-holder’s ability to access the account. The account-holder’s former email address is also modified slightly to protect against duplicate account names, and the account is hidden from view in the Global Directory. It’s possible for a single individual to have more than one disabled account. This happens when, for example, someone has worked for multiple agencies.

**If individual transfers to another agency they are no longer authorized to have access to their disabled account without the permission of their prior agency.**

**Important Information**

Since 2002, the enterprise Exchange service has maintained the practice of retaining all disabled accounts online, as part of the Exchange environment. Once an account is disabled, the content in that account is no longer under the control of the original account-holder and the content remains preserved.

With the exception of content previously disposed of or archived by the account-holder, these disabled accounts should contain all content either originated or received by the account-holder. This repository of information is available to agencies upon request for the purposes of compliance with FOI, eDiscovery or other agency needs.

---

\(^1\) Please refer to the sections titled *Deleted Mail in Exchange* and *Outlook Archiving and Exchange ESI* for more information.
Confidential, Regulated or Restricted ESI in Exchange

Exchange content may contain ESI that is considered sensitive, confidential, or may be regulated or restricted by federal or state law. Some examples of Exchange ESI that may fall into this category are:

- Content that is considered a legal work product, covered by attorney-client privilege;
- Data that is considered personally-identifiable (PII);
- Information or data that may be exempted from FOI, by statute or a FOI Commission ruling;
- Content associated with state citizens that is considered confidential;
- Information or data pertaining to students or faculty (FERPA), or
- Information related to the state’s IT security practices, procedures or configurations.

Agencies should assess the risks related to the possible presence of regulated, restricted or confidential when authorizing individual(s) within their agency to access agency mail accounts.

Individuals Authorized to Access Exchange ESI

Apart from the account-holder themselves, no other individual is normally authorized to access the Exchange ESI of another account-holder without the prior approval of their agency head.

Each agency has been asked to identify to DAS/BEST those individuals within their organization who, as a part of their job duties, has been granted permission to access the agency’s Exchange ESI, should such a need arise. These permissions will be reviewed with the agency head or their designee on an annual basis and the agency can make adjustments as may be needed from time to time.

Any individual identified by their agency as noted above, will be given permissions to access the DAS/BEST FootPrints eDiscovery services for the purpose of submitting requests for:

- Extracts of Exchange ESI
- Request for Legal Hold(s)
- Request for Administrative Hold(s)

In addition to the any individuals identified by an agency head as authorized to access Exchange ESI on behalf of their agency, DAS/BEST may also be required to produce ESI for individuals or organizations who possess the appropriate statutory authority to access public records, such as the Auditor of Public Accounts (C.G.S. § 2-90). Whenever practicable, DAS/BEST will request that those individuals or organizations work with the relevant agency when they require access to Exchange ESI.
Requesting Access to Account-holder ESI

Should an agency require access to Exchange ESI for the purposes of FOI or eDiscovery, the following procedure applies. For the purposes of these instructions, a Requester is defined as any individual in the agency who has been granted the prior authority by their agency head or designee to access an account-holder’s mailbox on behalf of their agency.

Agencies request this access by completing a Request for Service (RFS) using the online DAS/BEST Service Catalog. The use of FootPrints will ensure that your agency’s request will be processed in a timely manner, allows the requester to track the progress of the request and it provides an audit trail of the permissions we have granted.

1. The Requester logs in to FootPrints. If a Requester has never logged into FootPrints before, they will be asked some additional information to create a FootPrints account.

2. For most customer accounts, once you log in, you will be prompted to select the Workspace you want to use. For the purpose of this Bulletin, you’ll want to select “eDiscovery Services”.

   If you do not get prompted to select a Workspace or if “eDiscovery Services” is not found in the Workspace list and BEST has confirmed that you were granted eDiscovery Services permissions, please contact the Help Desk at (860) 622-2300 (Option 9) and report the issue.

3. At the FootPrints home page, click on the “Service Catalog” menu button.

4. From the Service Catalog, locate the “Search Services” field in the upper right corner of the Service Catalog web page. Do not use the search field located in the upper center. Type the value “Exchange ESI” in this field and press enter. This will locate all services related to Exchange eDiscovery Services.

5. Select the service titled “I need to request the extraction Exchange ESI”. From here you will then be presented with a service description page. Click on “Request this Service” located in the upper left corner if the web page. The RFS form should then display.

6. Complete the RFS by validating your contact information under the “Contact Information” section and supplying the relevant information under the “eDiscovery Query” and “Exchange ESI Extract” sections. You can add any additional information in the “Request Description” section. If you have a large number of accounts (e.g., more than ten), we ask that you submit the names on a spreadsheet that can be attached to the RFS. This will aid in reconciliation, so no accounts get overlooked. If available, also attach a copy of the formal Litigation Hold notice to the RFS.

7. Press the Save button to submit the request. DAS/BEST will complete this request within five (5) business days.

---

1 http://footprints.ct.gov/MRcgi/MRentrancePage.pl
2 If a Requester cannot locate or access these services, they may not be authorized by their agency for such access or may have not been added to the workspace by DAS/BEST.
DAS/BEST may also grant access to Exchange account-holder ESI to individuals who possess the legal or statutory authority to access state records. Where practicable, DAS/BEST will request that those individuals direct any such requests through the agency having control over they Exchange ESI they seek to access.

<table>
<thead>
<tr>
<th>Important Information</th>
<th>When requesting Exchange ESI services, agencies are asked to use the services listed under eDiscovery Services in the Service Catalog and not to use the normal Exchange services.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Using the eDiscovery Services will help ensure that the content of these requests is not accessible to individuals who do not possess access to the eDiscovery Services workspace.</td>
</tr>
</tbody>
</table>

**Exchange ESI Delivery Methods**

DAS/BEST provides agencies with Exchange ESI, using the parameters provided by the agency and as executed using the eDiscovery feature of Exchange 2013. This tool is specifically designed for eDiscovery purposes and ensures that Exchange ESI is produced in a consistent and reliable manner.

Upon receipt of a formal RFS, DAS/BEST can deliver Exchange ESI to your agency in the following ways, accessible only to those on the agency-head approved list. Permissions to these delivery end-points are controlled by means of Security Group administered by DAS/BEST.

**Discovery Mailboxes** – One of two shared mailboxes dedicated to your agency’s eDiscovery. These are [AGY].Legal.Discovery and [AGY].Admin.Discovery. Extracts can be delivered to one of these mailboxes, depending on the nature of the request. These shared mailboxes makes access and review quite easy through Outlook.

**Agency Transfer Location** – Each agency will have access to a dedicated network file share specific to your agency and accessible only by those on the approved list. This share is can be drive-mapped as needed. The location is `\exec\dfs\edaas`, under which is a folder specific to your agency. This content is delivered in the form of one or more PST files, depending on the number of accounts involved in the query.

**Copy to CD/DVD** – DAS/BEST can copy the ESI to a CD/DVD as may be needed for delivery to an outside party.

---

1 Discover Mailboxes cannot be accessed using OWA.
Exchange System Backups

Each week, DAS/BEST runs a process to back up the entirety of the Exchange environment. This activity is part of the DAS/BEST Disaster Recovery program and is designed specifically to provide a mechanism for restoring the Exchange service in the event of a catastrophic loss of part or all of that environment.

DAS/BEST retains each weekly set of Exchange backups for a period not to exceed four (4) weeks, at which time they are considered no longer useful for a system restoration and are dropped. This retention practice ensures that there is adequate redundancy in the event that any given set of backups become corrupted or are otherwise unusable for the restoration of the Exchange environment.

Consistent with the Connecticut State Library’s General Letter 2009-02, **backup tapes are not intended for, nor acceptable as a means for the retention of electronic messages and are therefore not available as a source of public records.**

Understanding Deleted Mail in Exchange

When an account-holder makes a determination that a given Exchange item is no longer needed or does not fit the definition of a public record, they can decide to delete that item from the system. Exchange will retain a deleted item(s) in the system for a maximum of 150 days before becoming irretrievable. When an account-holder deletes an item, the following actions occur:

- The item(s) moves into the Deleted Items folder. This folder can be easily accessed by the account-holder for recovery purposes. An item must move to the Deleted Items folder to be considered deleted.
- The item(s) remains in the Deleted Items folder for no more than 30 days from the date it was deleted, at which time Exchange automatically purges the item from the folder, unless purged sooner by the account-holder.
- The item(s) then move to the Recover Deleted Items folder where the item(s) remain available to the user for another 120 days. The account-holder can easily recover data from this hidden folder using the Recover Deleted Items function in Outlook or OWA.
- After 120 days in the Recover Deleted Items folder, the item(s) are then physically deleted from the system and become irretrievable.

**Important Information**

If an account has been the subject of an In-place hold and that hold was implemented using the Exchange In-place Hold feature, Exchange ESI **will remain immutable** based on the requirements of the hold. This hold on ESI will remain in place until the agency or AG authorizes the removal of the hold.

Please to the “Preservation of Exchange ESI” in the Resources Section, below.
Outlook Archiving and Exchange ESI

The Microsoft Office Outlook application provides an account-holder with the ability to automatically archive or manually move Exchange ESI to an offline file called a Personal Storage Folder (PST). When Exchange ESI is archived or moved to a PST, the content is no longer accessible through Exchange. Unfortunately, there is no mechanism in Exchange to control this capability in Outlook.

If a PST file is lost, misplaced or unintentionally deleted, the agency will have lost access to this data for FOI or eDiscovery needs. In some cases, the loss of a PST may be considered a reportable security incident. Therefore, it is the responsibility of every agency to maintain the appropriate custody and control over PST files and to comply with any relevant federal or state regulation or policy governing record retention and to ensure that the data contained in the PST files remains available for FOI or eDiscovery needs.

DAS/BEST strongly recommends that agencies discourage the use of Outlook archiving or the creation of PST files for the purpose of storing Exchange ESI apart from the Exchange environment.

Resources

DAS/BEST FootPrints Service Management System

Electronic Mail Records Management Policy

Requesting the Preservation of ESI by DAS/BEST

Connecticut State Library’s General Letter 2009-02