eRecords Request Selection Descriptions

Below is a description of the type of records customers can expect to receive for the different selections on the eRecords Request Form. These descriptions are meant to reduce confusion and assist in making the most appropriate selection for the needs of your organization. Please be advised, DTI is able to provide the data requested but is unable to conduct forensic analysis. Customers will need to ensure they have a way to read and interpret the data they are requesting.
****Allow a MINIMUM of 7-10 business days for completion.****

1. **Email and Voicemail:** DTI will provide email and voicemail content that resides in the applicable mailboxes, as well as deleted email content that falls within the 12-month retention policy. Additionally, mailboxes can be placed on legal hold ensuring existing content is preserved until the hold is released. A legal hold placed on a mailbox will also place all private Teams chats (1:1 or group chats) on legal hold. Lastly, if non-consensual access is required to a mailbox for continuity of business purposes (retirement, separation, extended medical leave), DTI can setup a mail-forwarding rule for new emails and can provide a file containing previous emails. In such cases, please contact eRecords Administration for instructions.

2. **Proxy Logs:** DTI will provide proxy logs that represent all web activity that the employee's computer conducted. This is more than just the employee's browsing activity. These logs will show activity from the host simply being connected to the Internet, such as automatically downloading updates, advertisements that load during web browsing, etc. Providing a specific web address can significantly reduce fulfillment time and the volume of records returned.

3. **Phone Logs (EVS – Cisco):** DTI will provide call detail records that come from the State's Enterprise Voice Cisco IP Telephony Phone System (EVS-Cisco) that is managed by the DTI Telecom Voice Team. DTI retains call records from this phone system for a period of 12 months. A phone number for the search MUST be provided in the Search Terms field of the request form.

   DTI does not have access to cell phone logs for State-owned or personal devices. For cell phone logs for State-owned devices, the customer will need to contact their agency contact for cell phones.

4. **Okta Logs:** DTI will provide user login activity to the State of Delaware's Identity and Access Management application and other applications that have been onboarded to it. Okta logs are not only able to show when users log into id.delaware.gov, but also when they log into an application from id.delaware.gov. * Note: the logs only track initial login; They do not track the entire time the user was in the application, nor does it track user activity within the application.

5. **Firewall Logs**: DTI will provide firewall logs which represent connections from the employee workstation to IP addresses of other devices. Similar to proxy logs, this could represent not only employee web browsing, but also IP addresses of advertisement sites, entities used for automatic updates (e.g. Microsoft), etc.

6. **OneDrive/ SharePoint Online Sites:** DTI will provide content stored in the applicable OneDrive and/or SharePoint Online Site(s), as well as deleted content that falls within the 12-month retention policy. Additionally, OneDrive content and/or SharePoint Online site(s) can be placed on legal hold ensuring existing content is preserved until the hold is released. MUST provide Site URL/Name in the "Search Terms/Additional Information" box.

7. **Teams Chat:** DTI will provide Microsoft Teams chat messages including content shared through the chat (OneDrive/SharePoint Online). This includes deleted chats that fall within the 12-month retention policy. Additionally, a legal hold placed on a mailbox will also place all private Teams chats (1:1 or group chats) on legal hold.

8. **ServiceNow Information:** DTI will provide a report from ServiceNow on: Any requests previously submitted through the ServiceNow application, requests submitted by or for the user for technology services/goods provided by DTI, and the user's interactions with DTI's ServiceDesk. The report can contain, but is not limited to, a request number, type of request (e.g. Password reset, business case, etc.), description, opened and closed date.

9. **User Home Drive:** DTI will provide files and folders from an individual's home/personal drive. This does not include files from a network share that is accessed by an entire team, or Teams or E-Mail documents. When the employee separates from an agency, the account (unless the user is transferring to another agency) is retained for 30 days unless otherwise requested for retention by the agency. DTI is unable to access this information for non-ITC agencies. Non-ITC agencies will need to submit their request to their IT Support Team.

10. **SSL/VPN Logs:** DTI will provide authentication logs for the Pulse Secure SSLVPN with dates/times and geolocation data for events where the user connected to or disconnected from the SSLVPN client. The SSLVPN is most commonly used for remote work.

11. **Teams Workspaces:** DTI will provide content stored in the applicable Microsoft Teams workspace(s), as well as deleted content that falls within the 12-month retention policy. Additionally, Microsoft Teams workspaces can be placed on legal hold ensuring existing content is preserved until the hold is released. MUST provide Teams workspace name in the "Search Terms/Additional Information" box.

12. **Network Drives:** DTI will provide files and folders from requested network share(s). This does not include files from a user's Home Drive, but rather data that is accessed by an entire team stored on an agencies file server. MUST provide server name and folder path in Search Terms field. This data is managed by the agency and its employees and is subject to change at their discretion.