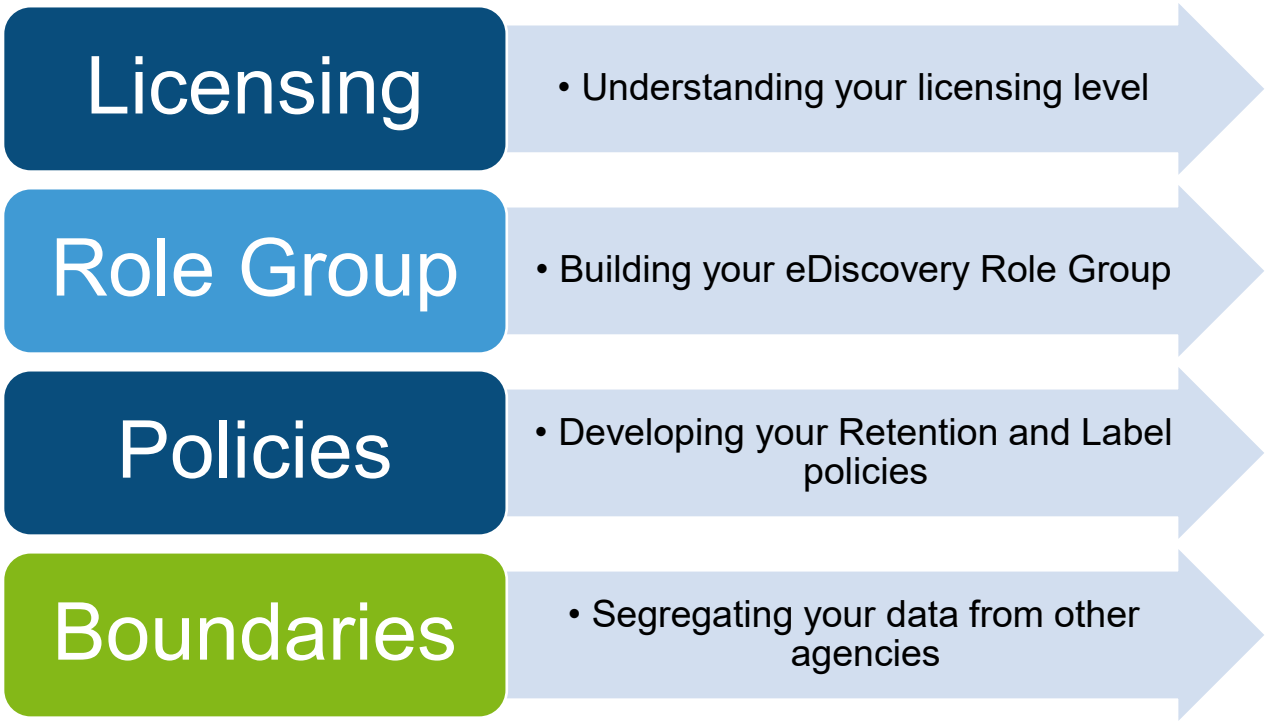
Getting Started with O365 Records & eDiscovery

This document provides the details needed to configure the O365 tenant for your ability to preserve your records and use eDiscovery in the Security & Compliance center.



Version 1 | 6-26-2020

Licensing

It is important to understand your O365 license level, its features, and how to license your users and data in a way that meets your needs[1].

G3 license

- Core eDiscovery (basic search, export, and legal holds)
- Standard retention policies and retention labels.

G5 license or G3 with Compliance addon:

- Core eDiscovery plus Advanced eDiscovery features (review)
- G5 policies plus Auto-applied and Event-based labels

1. To perform eDiscovery against a user's dataset, the user must be licensed, not just the searcher. For example, if you need to perform advanced eDiscovery against your agency, all users you search against must have the G5 license.

Role Group

A Role Group is a list of roles that are applied against an Active Directory group and the members within. Each agency will be members of 2 eDiscovery role groups:

eDiscovery Manager

- All eDiscovery managers are members of this role group, which grants users access to the Security & Compliance center and grants them the access and rights within the tenant.
- The following roles are currently implemented for the eDiscovery Manager role: Case Management, Compliance Search, Export, RMS Decrypt, Custodian, Communication, Review, Preview, and Hold.
- For more information on the various roles, please visit this document. (https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide)

eDiscovery Manager - AGY

- This role group is agency-specific and is used for the Compliance Boundary (see last section).
- Tenant administrators will assign this role group to an Azure Active Directory group. (The group and users must be sync'd to the tenant). We prefer to use the agency's already-defined Exchange on-premise eDiscovery role, which is usually found in this format in your domain: U-S-AGY Delegated Discovery Administrators. An agency may supply a different group for the tenant administrator to use.

Policies

Policies come in several flavors like Retention, Label, Event-based, or Auto-apply. This document will focus on Retention and Label policies. For information on Event-based[2] or Auto-applied[3] labels, please see the footnotes below.

Retention Policies are used to immediately apply a retention to a document when it is created. For example, this would be your overall mailbox retention policy. **Label Policies** are user-driven retentions that allow a user to choose which retention to apply to a document or folder.

To begin, an agency should evaluate their records management policies and perhaps make adjustments. Review your Enterprise Vault policies and decide if they will meet your needs in O365. For example, an agency may wish to deploy a transitory label to allow users to delete non-record data that has automatically inherited the default retention policy.

Policies will be assigned to an AAD group, like how policies are assigned in Enterprise Vault. WaTech can assist the agency with pulling together the Vault Policy Form to develop a plan in O365.

Exchange Policies: Both retention and label policies are available. Customers should create AAD groups for the tenant admin to assign the policies to.

SharePoint Policies: Currently, labels have been predefined. SharePoint site administrators can choose which labels to employ in their sites or libraries.

OneDrive Policies: Currently, labels have been predefined. Agencies can choose an AAD group to assign the labels to.

Teams Chat Policies: Retention policies are coming for both Teams Chat (1v1) and Teams Channel Chat.

2. https://docs.microsoft.com/en-us/microsoft-365/compliance/event-driven-retention
3. https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-labels

Boundaries

Compliance boundaries are how agencies can keep their data segregated from other agency access. Tenant administrators will create the compliance filters and assign them to the eDiscovery Manager role for your agency. Data exists in 2 distinct locations in O365: Exchange and SharePoint.

Tenant administrators need the following information to build your tenant boundaries:

- Company field in user's AD Account
- All Primary SMTP Addresses
- Top level site URL for SharePoint sites and Teams

Company Field: The agency should have standardized entries in their Company Field in Active Directory. The filter script can use wildcards. Example company fields: 'watech*' or 'watech – division*'.

Primary SMTP Addresses: An agency may have one or more primary addresses in their agency. Only the Primary addresses are needed and only those that should be part of the compliance boundary, and thus not searchable. For example, if you have a sub-agency that may become autonomous after moving to O365, you may wish to not include them.

SharePoint and Teams URLs: Agencies should standardize the naming of their Teams by using their Agency acronym as the beginning of a Teams name. See example below.

{Mailbox_Company -like 'watech'
-or Mailbox_PrimarySMTPaddress -like '*@watech.wa.gov'
-or Mailbox_Company -like 'ocs'
-or Mailbox_PrimarySMTPaddress -like '*@ocs.wa.gov'}

{Site_ComplianceAttribute -like 'WaTech'
-or Site_Site –like 'https://stateofwa.sharepoint.com/sites/watech*'
-or Site_Site –like 'https://stateofwa.sharepoint.com/teams/watech*'}