LITIGATION PLAYBOOK

Client Name

PRIVILEGED & CONFIDENTIAL

Litigation Readiness Playbook

Discovery is an essential yet increasingly complex aspect of litigation. To enhance an organizations discovery practices and preparedness, Innovative Driven has developed the Litigation Readiness Playbook for M365. The Playbook contains a series of guidelines that, when followed, will facilitate compliance with discovery requirements and increase the likelihood of better litigation outcomes. The Playbook is collectively comprised of this document, together with the following materials:

- Litigation Assessment
- Litigation Workflow

Table of Contents

The Importance of Discovery Preparedness

Discovery is designed to be a straightforward, self-executing process in which the parties to litigation exchange information relating to their claims and defenses or the subject matter of the litigation. The of this information exchange is to prepare for dispositive motion practice, settlement negotiations, and trial. It can also facilitate an informal resolution of disputes between the parties.

While the discovery process is intended to be simple, the reality is quite different. Discovery is riddled with complexities in both strategy and tactics. This is evident in dealings with litigation adversaries who often share as little information as possible about their claims or defenses while arguing their opponents are wrongfully doing the same thing. Parties also struggle with internal challenges such as seeking to identify and produce relevant information. While the sheer volume of potentially discoverable information contributes to the problem, a party's inability to produce relevant documents frequently results from its lack of discovery preparations.

Discovery preparedness is one of the best ways to address these complexities and thereby enhance the position of your organization in litigation. With better planning, relevant information can be:

- Retained more easily, eliminating troubling questions surrounding preservation failures.
- Identified and analyzed more quickly, leading to a better understanding of the strengths and weaknesses of client litigation positions.
- Produced with greater efficiency, which leads to lower discovery costs.

Client preparation for discovery usually involves implementing information governance ("IG") measures and a litigation readiness plan. IG measures such as data mapping and records retention policies facilitate the identification of relevant information in litigation. Policies that govern employee use of smartphones and tablets, personal cloud applications, and email and messaging application accounts can also simplify the retrieval of discoverable information.

These upstream, proactive measures facilitate downstream, discovery preparedness for clients when coupled with a litigation readiness plan. A client litigation readiness plan should include:

- A litigation hold policy and reasonable preservation practices.
- Technologies that can expedite the analysis of information.

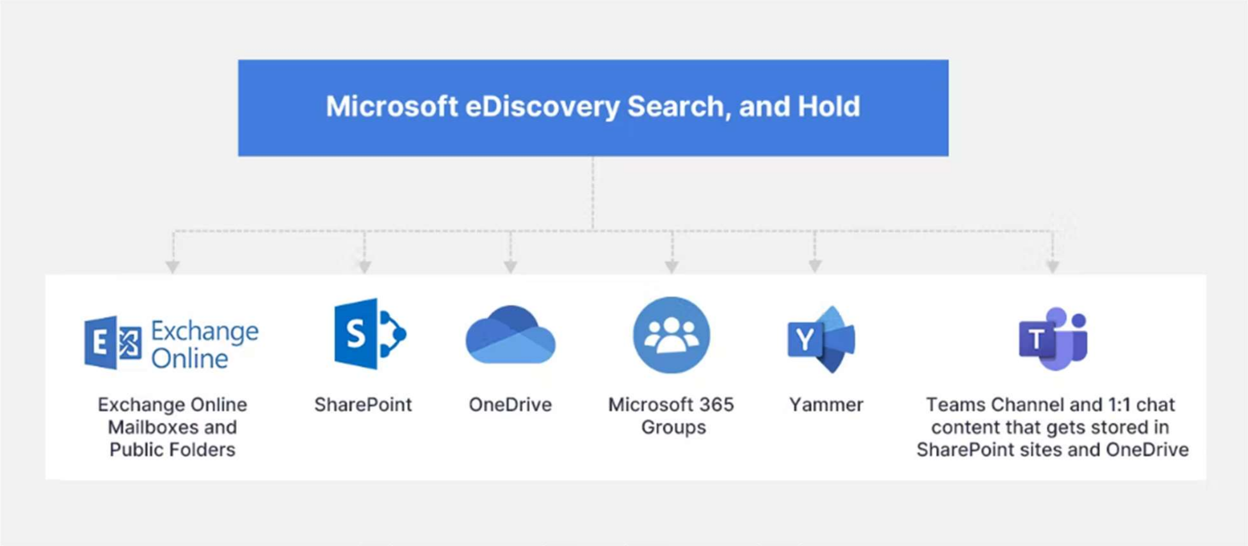
In summary, if an organization can actively manage their information through IG measures and a litigation readiness plan, they will likely obtain better litigation outcomes than if they neglected those measures.

Microsoft eDiscovery Overview

Microsoft eDiscovery lets administrators and eDiscovery managers create cases to collect and preserve necessary data. Users with relevant permissions can run a search to identify content stored in different Microsoft services. Organizations can also place a hold on specific locations to preserve sensitive files, documents, or messages indefinitely. Once a hold is placed, the file then becomes inaccessible to the owner and collaborators, and it cannot be modified or deleted until the hold is removed.

Data Sources Covered by Microsoft eDiscovery

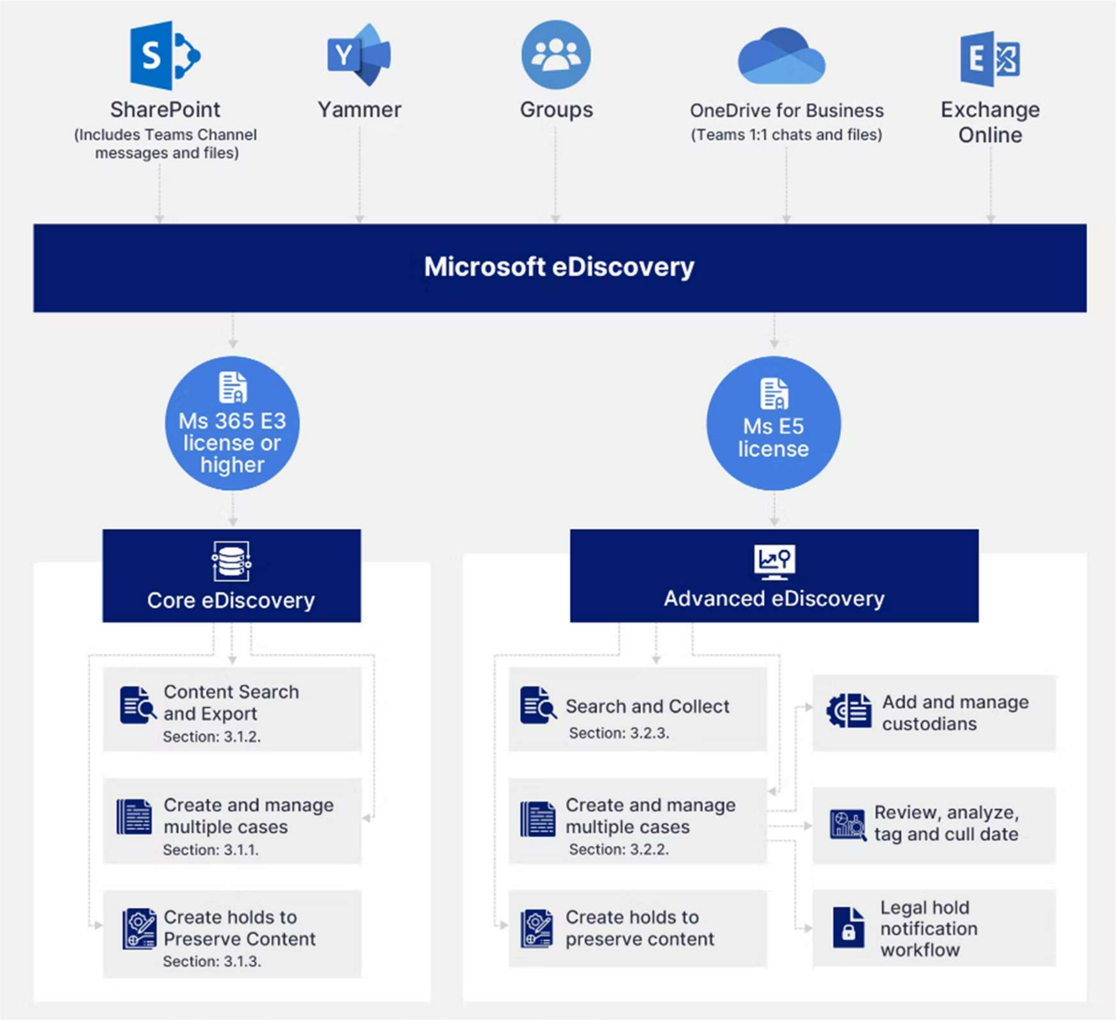
Microsoft eDiscovery helps organizations search and preserve content stored in Exchange Mailboxes and Public folders, SharePoint Sites, OneDrive for Business, Groups, and Yammer. Messages and files shared within a Microsoft Teams Channel (including a private channel) get stored in Exchange Online mailboxes and SharePoint Sites associated with the team, respectively. The messages and files shared on 1:1 chat is stored in individual users' mailboxes and OneDrive accounts.


Microsoft eDiscovery Search, and Hold
Exchange Online
Exchange Online Mailboxes and Public Folders
SharePoint
OneDrive
Microsoft 365 Groups
Yammer
Teams Channel and 1:1 chat content that gets stored in SharePoint sites and OneDrive

Types of eDiscovery available

Microsoft eDiscovery includes Content Search, Core (Standard) eDiscovery, and Advanced (Premium) eDiscovery. The below diagram illustrates the basic features available with either.

- In a Core eDiscovery case, organizations can run content searches, and place holds to preserve content indefinitely.
- Using an Advanced eDiscovery case, organizations can collect, review, analyze, and export data, manage custodians, and add notification workflows to communicate with these custodians.
- Using the eDiscovery search tool available with Core (Standard) and Advanced (Premium) eDiscovery, organizations can search for content across Microsoft 365 data sources and export the search results to a local computer.


SharePoint
(Includes Teams Channel messages and files)
Yammer
Groups
OneDrive for Business
(Teams 1:1 chats and files)
Exchange Online
Microsoft eDiscovery
Ms 365 E3 license or higher
Ms E5 license
Core eDiscovery
Advanced eDiscovery
Content Search and Export
Section: 3.1.2.
Create and manage multiple cases
Section: 3.1.1.
Create holds to Preserve Content
Section: 3.1.3.
Search and Collect
Section: 3.2.3.
Create and manage multiple cases
Section: 3.2.2.
Create holds to preserve content
Add and manage custodians
Review, analyze, tag and cull date
Legal hold notification workflow

Basics of M365 eDiscovery Tools

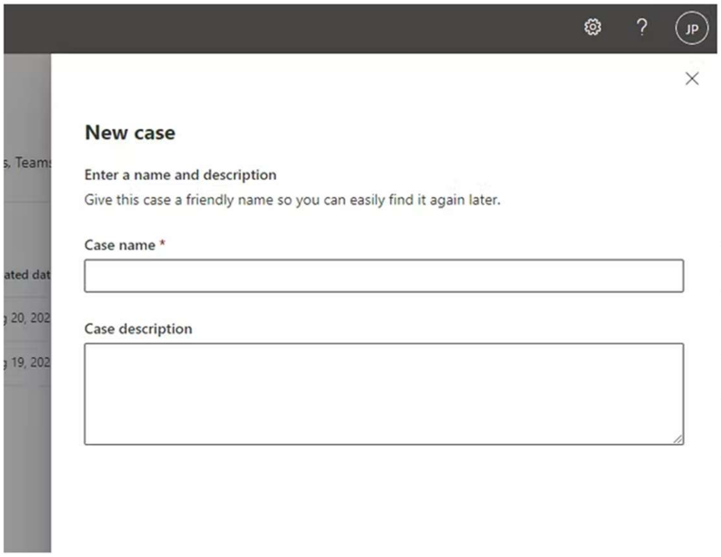
Microsoft has a core set of eDiscovery tools with features that vary based on the license available to the user. In this section we look at the different versions along with so handy guides to get you through basic tasks.

M365 Core (Standard) eDiscovery

Microsoft Core (Standard) eDiscovery builds on the basic capabilities of the Content Search tool. Core (Standard) eDiscovery allows administrators and users with relevant permissions to create an eDiscovery case, search for content located in different Microsoft services, preview and export the search results, add managers to the case, place holds, etc.

How to Create a Case

- Step 1:
- Step 2:
- Step 3:



New case

Enter a name and description

Give this case a friendly name so you can easily find it again later.

Case name *

Case description

REMAINING SECTIONS LEFT BLANK INTENTIONALLY

M365 Advanced (Premium) eDiscovery

Microsoft Advanced (Premium) eDiscovery builds on the existing case management, preservation, search, and export functionalities of Core eDiscovery. With Advanced (Premium) eDiscovery, administrators can identify, collect, review, analyze, preserve, and export content relevant to any internal or external investigations. They can also collect data from any service, move it into review sets where they can add filters, search the content, tag and analyze it, and remove irrelevant content. from further review.

Advanced (Premium) eDiscovery also helps manage custodians and legal hold notification workflows to communicate with custodians involved in any specific case.

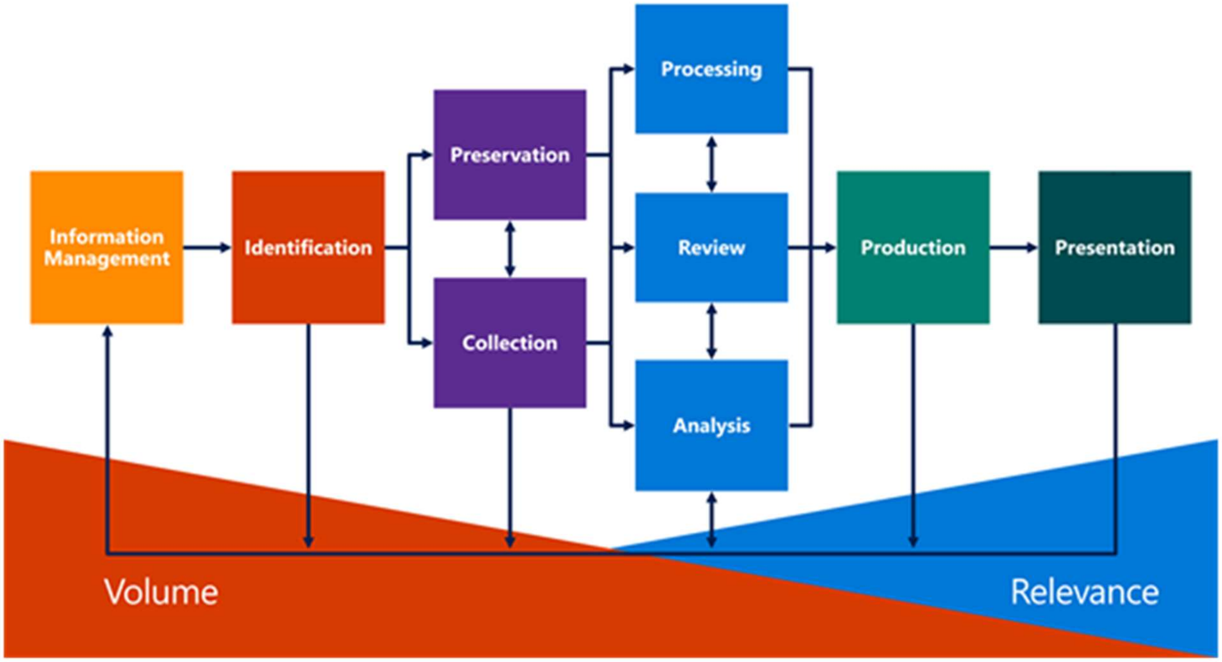
REMAINING SECTIONS LEFT BLANK INTENTIONALLY

eDiscovery Workflow

The Microsoft Purview eDiscovery (Premium) solution builds on the existing Microsoft eDiscovery and analytics capabilities. eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export content that's responsive to your organization's internal and external investigations. It also lets legal teams manage the entire legal hold notification workflow to communicate with custodians involved in a case.

eDiscovery (Premium) can help your organization respond to legal matters or internal investigations by discovering data where it lives. You can seamlessly manage eDiscovery workflows by identifying persons of interest and their data sources, seamlessly apply holds to preserve data, and then manage the legal hold communication process. By collecting data from the source, you can search the live Microsoft 365 platform to quickly find what you need. Intelligent, machine learning capabilities such as deep indexing, email threading, and near duplicate detection also help you reduce large volumes of data to a relevant data set.

The **Electronic Discovery Reference Model (EDRM)**, shown in the following figure, summarizes the typical phases in the eDiscovery process for identifying relevant content and reducing the volume of content to present.



Advanced eDiscovery supports the EDRM Workflow

When an organization responds to legal investigation, the workflow around identifying, preserving, and collecting potentially relevant content is based on the people in the organization who are custodians of relevant data. In eDiscovery, these individuals are called data custodians (or just custodians).

Content locations where case custodians don’t have administrative control but may be owners of relevant data, are known as non-custodial data sources. In a advanced eDiscovery case, legal teams can add individuals in their organization as custodians, and identify and preserve content in custodian and data source management tool in Advanced eDiscovery, organizations can secure collect electronically stored information and preserve it from inadvertent deletion.

The information governance features in Office 365 help you intelligently manage content in a proactive manner to respond to both internal and external compliance requirements. You can respond to eDiscovery requests more quickly, easily, and cost-effectively. The Office 365 Security & Compliance Center is a central location where you manage information governance and eDiscovery across all of your Office 365 data assets. Use it to:

Import content into Office 365 so that you can manage it. For on-premises content stored in Exchange or file shares, Office 365 provides an import service. For external content from social and messaging apps, document collaboration tools, and vertical apps (such as CRM or financial sites), some Microsoft partners provide connectors that support different third-party file formats.

Apply information governance to Office 365 content. Information governance helps ensure that content is managed in a way that supports your compliance needs. It lets you proactively set retention policies on your Office 365 content in mailboxes, public folders, and sites. You can preserve important content and delete content when you no longer need it. Or for specific investigations, you can preserve just the content associated with an eDiscovery case by putting the content on hold. This hold overrides any retention policies that would otherwise apply.

Create and manage eDiscovery cases. eDiscovery cases facilitate investigations and restrict access to them. When you create a case, you can manage it as follows: add members and give them specific permissions to control the types of actions they can perform in an investigation; place content source locations associated with the case on hold; preserve on-hold content indefinitely, until you remove the hold, without saving content to a separate archive; specify a date range and keywords to narrow the content that's preserved; run broad or targeted queries; prepare content for deeper processing and analytics with Advanced eDiscovery; and export content for review and production.

Preserve content in place. On-hold content remains in place, where it's located in Office 365, so that custodians—the content creators—can continue to access it. The content—email, messages, calendars, and files stored in Exchange Online, SharePoint Online, and OneDrive for Business—remains accessible to custodians, without duplication or stubbing. When you preserve content in Office 365, it's preserved in an immutable form. If someone modifies or deletes on hold content, the system preserves the original version in a secure location. Office 365 preserves only the content that the policy or custodian has tried to delete, so there's no duplication. It saves one definitive copy, and you don't use additional disk space for extra copies.

Run simple or complex search queries. Office 365 eDiscovery search lets you query all your organization's Office 365 content or focus searches on particular content source locations used by relevant custodians. To search efficiently, you don't need to copy your content to a consolidated external repository. Search all mailboxes and public folders in place in Exchange Online, all SharePoint Online sites, and all OneDrive for Business source locations in a single search.

Quickly analyze content for relevance. Advanced eDiscovery helps you analyze large data sets and find content that's most relevant to a case. It can also organize your content, making the legal review process easier and more efficient.

Export content for review. You can export files from Office 365 search results in their native format. Advanced eDiscovery additionally exports content in a format that third-party review applications can directly ingest.

Audit activities in Office 365. You can monitor security and bolster the defensibility of your eDiscovery results by logging user and administrator activity in Exchange Online, SharePoint Online, and OneDrive for Business. Log files are stored for 90 days in Office 365. For longer term storage, download the log files using the Management Activity API. View reports in Office 365 Security & Compliance Center or create custom reports by using the Management Activity API.
NOTE: The Security & Compliance Center is fully scriptable using PowerShell, enabling you to manage your Office 365 Security & Compliance Center settings from the command line. For more information, see Office 365 Security & Compliance Center PowerShell.

M365 Discovery Workflow for Client

~~The following figure illustrates the information governance and eDiscovery features of Office 365.~~

REMAINING SECTIONS LEFT BLANK INTENTIONALLY

Collecting Relevant Information

Once the client identifies custodians and data sources within its possession, custody, or control that likely possess relevant information and steps have been taken to preserve such information, the client can work to collect that information for search and review purposes. Relevant information generally includes electronic data or paper documents. It may also be found in any number of other forms including equipment, furniture, automobiles, fixtures, etc., depending on the nature of the legal action at issue.

[redacted]

Proceeding with the collection of relevant information in this manner should yield a more effective and less costly discovery process.

The Search and Review Process

After the collection is complete, the collected information must be processed and reviewed to isolate relevant information (for production purposes) from other irrelevant materials. The traditional method for accomplishing this objective is a document-by-document review conducted by outside counsel.

The proliferation of ESI has forced lawyers and litigants to abandon the notion that all documents within the universe of potentially responsive information can be exclusively reviewed by humans. Instead, search methodologies and analytical tools are now used to cull the information universe and narrow the scope of potentially relevant documents to be reviewed for responsiveness. Common search methodologies and analytical tools include search terms, concept searching, email threading, and technology-assisted review.

M365 Collections and Review Sets

[redacted]

[redacted]

Search Terms

Search terms allow the parties to determine whether a document within the universe of potentially relevant information contains a particular word or set of words encompassed by a specific search term. While search terms can be an effective method for identifying relevant documents, they have several known limitations that often reduce their effectiveness. Because search terms focus on the precise word or set of words, they do not account for context. This may result in the search results being over-inclusive, under-inclusive, or both.

Microsoft KQL and Search

[redacted]

[redacted]

[redacted]

Concept Searching

Concept searching can help lawyers obtain understanding on the usage and context of particular terms by custodians and thereby gain greater insights into the substance of the documents for the matters at issue in the litigation.

Like search terms, concept searching evaluates the text of particular words. However, concept searching goes beyond the mere evaluation of words and instead expands the quality of a particular search by examining the context in which those words appear in a document, paragraph, sentence, or word.

A service provider with an electronic discovery platform should be able to perform different types of concept searches including the use of thesaurus to identify synonyms or other related terms. The provider can also use a more advanced statistical method to analyze proximity, *i.e.*, how close particular words are to others.

Email Threading

Many emails contain various strings, chains, or branches of earlier messages involving all, some, or just a few of the recipients. Reviewing all messages produced from various custodians who either sent or received those emails can be a time consuming process. It is also inefficient in terms of trying to understand the context of messages exchanged custodians and their relation to other messages in the overall email string.

Email threading technology organizes messages into more coherent conversations. Threading technology identifies the latest message in the chain, connects in side messages, and provides a more holistic method to review an entire email conversation while eliminating the need to review redundant messages.

Technology-Assisted Review

Technology-assisted review—known as TAR— is a computerized process for selecting and ranking a collection of documents. TAR is particularly useful for processing through massive amounts of data to identify relevant information for production and key documents for preparing a matter for disposition.

With TAR, advanced computer technology applies decisions regarding relevance that counsel have made on a subset of documents to the remaining documents in a set of client materials. TAR technology incorporates machine learning, which enables counsel to teach the technology how to distinguish relevant from irrelevant information. The more documents that counsel correctly designates as relevant, irrelevant, or privileged, the more accurate the predictions are that the technology can make regarding the balance of the unreviewed documents.

Defending the Search Process

Client should be prepared to establish the defensibility of their use of search methodologies and analytical tools. At a minimum, this requires responding parties to take a statistically valid sample of the documents they have not produced to ensure that relevant information has not been mistakenly withheld from discovery. Client should also sample the production to confirm it contains the relevant information represented to be in the production. Such a step will also enable the client to gauge the quality and nature of any nonresponsive information in the production set.

Federal courts have approved the use of search methodologies and analytical tools, finding them to be a reasonable and proportional use of technology to comply with discovery obligations. While state courts have not provided specific approval of these methodologies and tools, they are routinely used in state court litigation. Moreover, if challenged by requesting parties, it is expected that state courts will approve the defensible use of these tools given their reliance on federal jurisprudence regarding discovery issues. While parties maintain the prerogative to use these tools as they see fit to accomplish productions of relevant information, courts encourage them to do so transparently and cooperatively with litigation adversaries.

Clients and service providers should have a thorough understanding of how these methodologies and tools work and the way they should be implemented. This will enable cleint to more realistically accomplish cost effective document productions that satisfy discovery obligations.

REMAINING SECTIONS LEFT BLANK INTENTIONALLY

Termination Procedures

At the close of litigation, client should ensure that litigation adversaries and their counsel have returned or destroyed all documents that were on behalf of the client in litigation. While such a step is typically self-executing and is included as a matter of course in protective orders, not every party or counsel complies as quickly or as precisely with this provision as they should. Client should insist upon receiving a signed certification from adversaries within 30 days of the termination of litigation confirming they no longer possess information belonging to the client.

The release of a litigation hold should be executed consistent with a client's information retention policies and practices. For example, information produced in litigation may yet need to be retained pursuant to the client's records retention schedule. Before advising the client to proceed with the disposition of information, the client should determine whether such information has satisfied the delineated retention periods in the client's information retention policy or practices.

Similar considerations apply when the client is involved in other litigation and accordingly may be subject to other litigation holds. The release of a litigation hold on one matter must not affect custodians whose information is also on hold for a different legal matter. Before counseling the client to proceed with the disposition of information, the client should consider whether such information is subject to another existing litigation hold.

Releasing a Hold in M365

[redacted]

[redacted]

- **REMAINING SECTIONS LEFT BLANK INTENTIONALLY**