IRON MOUNTAIN®

THE IMPACT OF MS TEAMS ON LAW FIRM IG

2020 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

AUTHORS:

KAREN ALLEN
Manager, Information Governance Technology
Morgan Lewis & Bockius LLP, Co-lead

REGGIE POOL, ESQ
Senior Director
HBR Consulting, Co-Lead

SCOTT CHRISTENSEN
Vice President
Olenick

BETH FAIRCLOTH
Client Services Director
JONES DAY

BRIAN J. DONATO
CIO, Vorys, Sater
Seymour and Pease LLP

KATHERINE WEISENREDER
Information Governance Compliance Manager
Cooley LLP

GREG WEIGEL
Co-Founder, Chairman
Teravine, Inc.

JOHN ZAHRADNICK
Solution Consultant
InOutsource

BRYN BOWEN
Principal
Greenheart Consulting Partners

PURPOSE OF THIS PAPER

This paper explores topics that law firms should consider to appropriately govern the use of Microsoft Office 365 Teams®. It is intended to provide an initial overview of Teams and provide guidance around the Information Governance (IG) concerns when adopting Teams at a law firm. We have identified several key areas relevant to the law firm IG practitioner, focusing on primary configuration options and application settings. Each of these areas is supported by discussions around key functions and available configurations that would be applicable to the law firm's implementation of Teams as a replacement for Skype for Business chat, voice and meetings. We also address its use as a new collaboration solution leveraging Teams workspaces with channels, channel messaging, file management and app functionality.

Each major topic is followed by a set of **key takeaways** that summarise the primary considerations that you, as a law firm IG professional, can use as a high-level checklist on your own journey in the implementation of Teams.

The paper ends with a brief discussion of law firm specific governance considerations that affect the implementation of Teams, but also fall outside of the normal operational parameters of Teams lifecycle management (that are described in the paper's earlier sections).

Editor's Note – We use Teams (capitalised) for the product Microsoft Teams and team(s) (lower case t) to mean the workspace(s) you create within Teams

TEAMS

DESCRIPTION

Microsoft Teams is a cloud-based team collaboration software that is part of the Microsoft 365 suite of applications. It is Microsoft's core cloud-based unified communications offering, and it competes with similar products such as Slack, Cisco WebEx Teams and Google Hangouts. As a business communications app, Teams enables local and remote workers to collaborate on content in real time and near-real time across different devices, including laptops and mobile devices. Microsoft Teams also offers a single point of integration with other Microsoft 365 applications, including Exchange, OneDrive, SharePoint and Planner, pulling functionality and sharing content across these and other applications

RAPID ADOPTION

Many firms implemented Skype for Business as a basic collaboration platform, enjoying features such as instant messaging, voice and video calling and presence. Microsoft has announced the end of service date for Skype for Business Online is July 21, 2021, driving firms to make business decisions regarding their future collaboration platform of choice. The Microsoft 365 licensing that many firms have in place makes Teams a logical choice for their future business collaboration platform.

Generational changes are also playing a role in why law firms are considering Teams. As younger, tech-savvy individuals enter the business, they crave more modern collaboration tools to be used to communicate internally as well as with clients. For these individuals, telephone and email are no longer the preferred means of business communication.

Client adoption is also driving change. As businesses continue to adopt Teams, expect their law firms to also embrace Teams for ease of collaboration. Teams can extend the ability for clients they expect to communicate with a firm via external access using chats and meetings, further cementing client expectations that their lawyer is "always available". Firms are finding that without their own instance of Teams, or an alternative collaborative platform, their attorneys work within the client's Teams environment. The result: the attorney's work product is now stored and managed outside of the firm's control.

Last, and certainly not least, the global pandemic of 2020/2021 has played a significant role in expanding the use of Teams. Firms that had not yet decided about their future collaboration platform were suddenly put in a position of needing to implement Teams quickly to support their new "work from home" workforce. Microsoft has responded by adding capacity to support more simultaneous audio and video calls at once, and an array of new features to remain competitive in the marketplace.[1]

ADOPTION CONSIDERATIONS

Even with all the drivers for adoption, a firm should understand the risks and give due consideration before a full-scale embracing of Teams. Teams is very different than other desktop applications. It requires a substantial commitment for licensing along with dedicated staff to keep up with the ever-changing Microsoft 365 ecosystem. Firms must also recognise that it forces decisions about the use of Exchange Online, OneDrive and SharePoint.

For firms that may have restrictions in place regarding placing client data in a cloud environment, there are considerations regarding how certain should be implemented. In some cases, internal configuration settings teams features can and should be applied. In other cases, there may be usage restrictions that are controlled by good policies, but not enforceable using the technology. On the positive side, firms have reported some unexpected gains in efficiency and capability with their remote lawyers and staff quickly learning to be more self-sufficient.

FOUNDATIONAL GOVERNANCE

The first step in developing a framework for Teams is to examine the firm's policies, procedures and guidelines regarding general information management and then interpret them for the specific Teams feature.

When a Team is created, by default, the following are also created: a new Microsoft 365 group, SharePoint Online site and document library, Exchange Online shared mailbox and calendar, and a OneNote notebook. These applications support the functionality of Teams and are created regardless of which feature sets have been enabled within Teams. As with any software implementation involving the creation or transfer of data, a specific framework should be developed to govern these various applications as they are all potential storage locations for Teams' data. Below, we briefly discuss considerations for each policy/process area:

PROVISIONING PROCESS

Key to ensuring that users can take full advantage of Teams functionality while observing basic IG guidelines, is to streamline and centralise the provisioning of Teams so that there is consistency and clarity to the requestor, the process and the end user. Whether the Teams site is created through automation (e.g., through an NBI process) or through a manual request process (perhaps centralised through the Help Desk), there should be a defined process where the final creation of the Team is subject to a review and approval. The approval process, which typically falls on the Information Governance (IG) team, allows the IG professional a chance to validate the request itself (e.g., is a Team needed?), the team types (Public or Private), the use of Teams templates, the naming convention and the Teams initial membership (including guest access). Each of these decision points are described in greater detail below.

PUBLIC AND PRIVATE TEAMS

One big decision that must be made for each team is whether it is Public or Private. Creating a Public team means any firm member can both search for and see the team and also join the team without needing to request access. Public teams are exposed to everyone in Microsoft 365. Creating a Private team, means membership can be tightly controlled by role-permissions. Private teams, however, are not discoverable by firm members and access is managed by the team creator at the time of creation or by invitation. On the positive side (for law firm IG professionals), teams are Private by default.

PUBLIC TEAMS

Firms with a more open security model may choose to create Public teams. Public teams are visible to everyone from the Teams gallery and you can join them without getting approval from the team owner.

A firm should carefully consider when Public teams should be allowed as they provide little to no access controls. Because of this, IG professionals should identify and weigh the consequences of creating a Public team when developing the firm's Teams strategy.

ORG-WIDE TEAMS
Organisation-wide team is a type of Public team for which all firm members are automatically added to the team, allowing everyone in a small to medium-sized firm to be a part of a single team for collaboration. With org-wide teams, global admins can easily create a Public team that pulls in every user in the organisation and keeps the membership up to date with Active Directory as users join and leave the organisation. Only global admins can create org-wide teams and currently, an org-wide team is limited to organisations with no more than 10,000 users. There's is a limit of five org-wide teams per tenant.

PRIVATE TEAMS

As mentioned above, the default configuration for a team is Private. If this is not changed, any team created will be Private and is not viewable by firm members that are not part of that team.

Creating Private teams and tightly restricting those who can be an owner or member may better support a stricter security model, especially in the initial roll out when end-users may not understand the full ramifications of their changes to the team.

For client work, Private teams should be strongly considered. Like an inclusionary policy in the firm's DMS, a Private team can be configured to ensure that business users cannot add themselves to teams from which they should be screened. Existing members can request that new members be added from within the native interface, if enabled, which makes it easy for users and creates a workflow for the Teams admins.

Third party tools, or custom solutions, will be required to support the enforcement of these security screens, for example, by comparing group membership with security groups captured elsewhere.

KEY TAKEAWAYS

A team can be changed from Private to Public, but changing the privacy settings should be thoughtfully decided, because Public means Public!

TEAMS TYPES

When you create a new team, you should consider how you tie your IG requirements into a repeatable process. Teams supports the use of templates to define a standard configuration, including sets of channels upon creation. (Teams are sub-divided into channels.) By default, you get one and owners can create more. A template for a Litigation team, for example, might have pre-defined channels for depositions, briefs and strategy. Teams templates can also define other objects such as folder structures under a Channel's Files tab and even the automatic provisioning of Apps.

Law firms are likely to support several categories of Teams:

- Operational teams, focused on internal administrative operations, and open only to members of the firm.
- Practice area teams that provide a collaborative space for the various practice groups, such as Litigation, corporate or Intellectual Property.
- Client teams that cover the client relationship and perhaps serve as a repository for discussion about institutional knowledge useful for all who work with the client.
- Client Matter teams focused on a specific matter for the client.

As discussed above, some of these teams will be Private out of necessity. For instance, a matter team includes only members of the firm who work on the matter regularly. Increasingly, firms are setting up client matter teams and inviting the clients and/or co-counsel to participate as guests, allowing them to participate in specific channels or co-author documents. *NOTE: This type of Guest access can be applied to both Public and Private Teams.*

CLIENT-MATTER TEAMS - MATTER CENTRIC VS. CLIENT CENTRIC

When Teams was first announced, many IG practitioners started envisioning a perfect combination of a team and the legal DMS. Like matter workspaces, a team would be created for each client matter, allowing collaboration and coauthoring across the firm, for matter work being done in any of the firm's practice areas. Unfortunately, it is not quite that simple.

The creation of a team per matter should be thoroughly reviewed as part of the provisioning process. Creating a matter team seems straightforward, however this could easily become cumbersome within the UI and create more teams, groups and other infrastructure than the firm may wish to manage.

There is also the consideration of the number of teams that are available to the firm. Currently, each tenant is limited to 500,000 teams (and an individual firm employee can only be a member of 1,000 teams at one time). Any Teams configuration strategy, especially those contemplating a matter-centric approach, will need to incorporate these limitations in the planning process.[2]

CLIENT CENTRIC AND PRIVATE CHANNELS

An alternative to Matter Centric teams could be a client-centric approach with channels for individual matters. However, even within a Private team, channels are public to all team members by default. This can be overcome if private channels are enabled. With a private channel, only people who are owners or members of the private channel can access it. Anyone, including guests, can be added as a member of a private channel as long as they are already members of the team. This drastically reduces the number of teams and provides comparable levels of security to ensure information cannot be accessed inadvertently. That said, it may not work for practice groups with less matter centricity, for instance some Intellectual Property groups. *Note: The ability to create private channels can be managed at the team level and at the organisation level.*

KEY TAKEAWAYS

The firm should define the types of types of teams for use. This aids with streamlined creation of teams, as well as expectations from users on the characteristics of the different types of teams they can expect to work with.

Law firms should specifically examine the characteristics of teams which handle client matters. Key considerations are internal and external facing components, and usage guidelines.

Use policies to control which users in your organisation are allowed to create private channels. Once you've set the policies, team owners can turn off or turn on the ability for members to create private channels in the settings for a team.

NAMING CONVENTIONS

There are several options and decisions involved in naming a team. These choices depend on the firm's approach to both teams provisioning and integration with existing processes/systems.

GROUPS NAMING POLICIES

Natively, the only real limitation on naming a team is the actual length of the team name, Microsoft (and potential 3rd party tools) provide some options in terms of enforcing specific naming rules or conventions. As Teams lies on top of an Office 365 Group, there are Group naming rules that can be leveraged by the firm, including blocked words and forced prefix-suffix options.

BLOCKED WORDS

Group naming rules allow the firm to designate a list of words that are reserved and cannot be used during team creation. While this does limit the use of these restricted words, a firm's IT department can assist in creating these unique teams for each core department (as required) and the policy blocks any other attempt at creating a team or Group with that name.[4]

PREFIX/SUFFIX OPTIONS

An additional feature that can be prescribed by the Group naming policy is the enforcement of a custom prefix or suffix to a Group name. You can use prefixes or suffixes to define the naming convention of groups (for example: "US – Litigation - _Engineering"). The policy can enforce a specific prefix and/or suffix to the group name and alias of any Office 365 group created by firm members, for example: <Finance>-<group>-<Seattle>. Both prefix and suffix can include custom text strings or dynamic AD attributes and can be used to include client and/or matter identifiers as part of the Team name.[5]

KEY TAKEAWAYS

Put time into determining team names you want to reserve or create at the initial roll-out (Operational, Department/Practice Area). *See Team Types and Templates*

If you are not using a 3rd party tool to provision/name a team, consider leveraging native O365 Group naming features to block/reserve specific words from use as part of a team name.

TEAMS MEMBERSHIP

Teams workspaces have several security options that interact with each other. Two primary considerations are to decide on the team's Public or Private status (See Public and Private teams above) and on team membership (owners, members, and guests).

There are three different membership types within a team: owner, member and guest. Being a member of one team does not prevent you from being the owner of another, and vice versa. The assignment of these roles may depend greatly on the context of the team. For sake of discussion, we could generalise that context into buckets: a client or matter based team, a team created to collaborate on client work, and an internal team which can range from departmental groups, social groups and other ad hoc needs. Firms may choose stricter rules and more standard provisioning of matter teams while allowing certain users more flexibility in the creation and management of internal teams. However, your firm's security model will likely play a larger part in this determination.

Groups are largely considered the preferential method of granting access to IT resources and Teams is no different. For Teams, groups are generally managed with either the Microsoft 365 admin centre, Azure AD, PowerShell or an on-premises Active Directory Domain Service. Each of these offers the functionality to add users, create groups and manage group membership. Manual updates to group membership in Microsoft 365 admin centre may take time to be seen in front-end applications such as Teams. How you populate these groups will depend on how you choose to leverage Teams within your organisation.

KEY TAKEAWAYS

Most organisations use Microsoft Groups to manage access rights. This is the most streamlined and future-looking management option. Custom options require more manual intervention, monitoring and maintenance.

Law firms should specifically evaluate the firm's security model, including considerations and conversations around the types of teams the firm may deploy. Consider what types of users may require stricter access rights.

MEMBER ROLES AND RESPONSIBILITIES

There are a variety of roles that should be defined and agreed upon to enable good governance for a successful and scalable Teams implementation.

OWNERS

Teams member and guest access is controlled by the team owner or by an administrator. The team owner can invite firm members to join the team, and firm members can request to join a Public team. Per Microsoft, "Team owners manage certain settings for the team. They add and remove members, add guests, change team settings and handle administrative tasks. There can be multiple owners in a team."[6] You must consider who should hold this important role: it is recommended that each team has multiple owners who are active members of the team.

It's important to note that a team with a single owner can get 'abandoned' if the owner is no longer an active user. To insulate against a team owner departing the firm, some firms take the approach of having system accounts as owners. This approach may have merit depending on how your firm uses Teams. While it does provide a layer of insulation to ensure all teams can be managed by IT and reduces the risk of abandoned teams when owners leave, there are additional considerations for this strategy, such as team owners receive email notices requiring action regarding the team. Also, since the team owner isn't a person, it must be determined who will monitor any other aspects of the team that requires an owner response, as in the case of a public team where firm members may request to join.

In addition to member functionality, owners can edit or delete a team, delete private channels, add members and promote members to owners. See appendix B to compare owner and member permissions.

MEMBERS

Microsoft defines team members as "... the people in the team. They talk with other team members in conversations. They can view and usually upload and change files. They also do the usual sorts of collaboration that the team owners have permitted. Like team owners, team members can have specific rights controlling what they can do in a team."[7] While member permissions differ from the more expansive team owner administrative roles, there are some key capabilities that should be noted, such as the ability to add, edit or delete a standard channel, add private channels, request or add members to the team and the ability to add apps. These rights can be adjusted by the administrator and the team owner.

GUESTS

A guest is someone who is not an employee or member of your firm, and who does not have an account in your Microsoft tenant. Guests may include clients, vendors, suppliers or consultants; essentially anyone who is not part of the firm can be added as a guest in Teams. This means that anyone with a business account (that is, an Azure Active Directory account) or consumer email account (with Outlook.com, Gmail.com or others) can participate as a guest in Teams with access to teams and channel experiences.[8] *Note: In Teams, guests are clearly identified. A guest's name includes the label (Guest), and a channel includes an icon to indicate that there are guests on the team.*

Guests have several limitations on what they can do in a team. Microsoft provides a detailed table comparing the Teams functionality available for an organisation's team members and its guests.[9]

ADDITIONAL ROLES

There are few Teams roles that, while not technically a team member, have responsibilities that are important to note.

CREATORS

By default, anyone can create a team. While 'creator' is not an official role within Teams, you need to enact standards around how teams are created, documented and named. Firms should strongly consider restricting and centralising teams creation to specific groups or individuals within the firm.[10] It is not uncommon to see either the IT or IG group take on this role, especially during the early phases of Teams adoption.

Many organisations leverage existing workflows, such as IT ticketing systems, to allow employees to request a team. This allows a level of control around the type of team that is allowed based on the request, the initial team ownership and team membership.

ADMINISTRATORS

Certain tasks may be dependent on Microsoft 365 roles to accomplish. For example, file permissions for members and guests reflect whatever your admin has set in your SharePoint settings.

KEY TAKEAWAYS

Organisations should evaluate the main roles involved in Microsoft 365 and Teams, then define what those roles mean to the organisation and how each may be applied.

Law firms should especially consider the implications of membership/ownership of the different types of teams. Consider: what are the implications of ownership/membership in an external-facing team which is central to a client matter?

Guest access is included with all Microsoft 365 Business Standard, Microsoft 365 Enterprise, and Microsoft 365 Education subscriptions. No additional Microsoft 365 license is necessary.

SETTINGS MANAGEMENT

Teams provides a wide variety of options for configuring exactly what a team member can and cannot do. Microsoft refers to these settings as Policies. While most of these configurations deal with general governance, and are therefore beyond our scope, a few of them touch on Information Governance structure. For example, allowing meeting records might be desirable in some circumstances, but could also be an IG nightmare if not handled carefully. Similarly, the ability to add Apps to Teams is great for extending the functionality of Teams, but each app presents different IG challenges. Apps can be restricted in Teams to only approved apps. The primary configuration options with IG implications are listed below.

TEAMS ADMINISTRATION POLICIES

The Office 365 Admin Centre is used to control the organisation-wide settings and features that are available from an application and policy perspective. These control the functionality available through the Teams application and what can be done in Teams channels, files and apps.

Organisation-wide settings apply to the following categories of permissions and controls:

- External Access – allow communication with other Skype for Business or Teams instances
- Guest Access – set guest permissions around Teams access, calling features, meeting, and messaging functionality
- Team workspace settings – set organisation-wide Teams permissions around notifications and feeds; tagging; email integration; files management; tabs configuration; devices and search.

MESSAGING POLICIES

Messaging policies are used to control which chat and channel messaging features are available to owners and members (and guests) in Microsoft Teams. You can use the global default policy that's created automatically or create and assign custom messaging policies. Firm members automatically get the global policy unless you create and assign a custom policy. You can edit the settings in the global policy or create and assign one or more custom policies to turn on or turn off the features that you want.

Some of the key configuration options include:

- Enable/disable Teams Chat
- Modify or delete chats and channel messages (consider retention policies and eDiscovery considerations)
- Use of giphys, memes and stickers
- Enable audio messages in chats and channels
- Add and remove users from chat's (include or exclude chat history).[11]

It is recommended that you investigate options available in the default policy and set to the least restrictive option that still maintains your governance objectives. Other more restrictive policies can be created and assigned as necessary.

MEETINGS POLICIES

Meeting policies are used to control the features that are available to meeting participants for meetings that are scheduled by users in your organisation. You can use the global default policy that's automatically created or create and assign custom policies. Some of the key configuration options include:

- who can schedule meetings (private and channel)
- allow transcripts and meeting recordings
- controls and sharing
- enable meeting chat
- report on meeting details/attendees.[12]

Again, it is recommended that you investigate the options available in the default policy and set to the least restrictive option that still maintains your governance objectives. Other more restrictive policies can be created and assigned as necessary.

APP PERMISSION POLICIES

Teams also allows for external applications, often referred to as "apps", that can provide additional functionality when added to the team workspace via a tab. These apps are managed from the Microsoft Teams admin centre where they can be enabled or blocked, and policies implemented.

At a global level, Teams breaks applications into three groups: Microsoft apps (includes partners), third-party apps and custom apps. For each of these groups you can make the determination to allow all applications; allow specific applications and block all others; block specific apps and allow all others; or block all apps. If security and data privacy are a concern, allowing specific apps (like all Microsoft authored apps) and blocking all others is the safest measure until appropriate assessments can be made. The flexibility here means you can launch teams with access to the power of the rest of the Microsoft Office suite without concern for the use of unauthorised apps.

You can use app permission policies to control what apps are available to Microsoft Teams. Policies can be utilised to allow or block all or specific apps published by Microsoft, third parties and your organisation. When an app is blocked, users subject to the policy are unable to install the app from the Teams app store. *Note: You must be a global admin or Teams service admin to manage these policies and use the global default policy or create and assign custom policies.*

MICROSOFT APP COMPLIANCE PROGRAM
The Microsoft 365 App Compliance Program provides a structure by which external applications can be deemed as trusted; it is currently voluntary. The three tiers build on each other and are currently Publisher Verification, Publisher Attestation and Microsoft 365 Certification. Verification ensures that the application developer has had their identity properly verified through Microsoft and are using standard methods for authenticating users and accessing data through the API. Attestation is a standard format for providing organisations with the appropriate information regarding data handling and compliance, however, "Microsoft does not validate the information provided. The developer solely affirms the veracity, accuracy, and integrity of the attestation documentation and corresponding app performance data". The final level, Microsoft 365 Certification, leverages third-party auditors to assess security and compliance standards while ensuring compatibility.

NOTE: Teams Voice Policies – Phone Systems and PSTN Connectivity are outside the scope of this paper.

KEY TAKEAWAYS

Microsoft terms a group of settings configurations as a "policy. "Any organisation should review these policies (or settings configurations) for all general governance considerations.

Law firms specifically should consider the implications of client matter, external access, sharing and use cases for any of the types of teams defined for the firm. Various policies may be defined for different types of teams, especially when considering organisation business-focused teams vs. matter-centric teams.

Firm employees automatically get the organisation-wide and/or global policies unless you create and assign a custom policy.

When evaluating App integration, firms should consider which level of trust is appropriate for their risk tolerance and establish policies around the acceptable use of external apps in Teams.

INTEGRATION CONSIDERATIONS

IG professionals should also consider what integration is necessary, and what integration is practical, between Teams and other tools. The use of other tools may impact the app permissions policies in that policies might need to be modified as new apps are considered for deployment.

DMS INTEGRATION

The most common integration point for many firms is their document management system (DMS) as that is often the repository of record for all documents and communications. Teams does not currently have native integration with any external DMS, relying on third party solution integration features to provide synchronisation between Teams and the DMS. As of the date of this publication, no major legal DMS provider supports native integration with Teams. While it is possible, and practical, to create an active tab in a team that contains a web-based interface to the DMS, this is not a true integration. This method can, however, allow team members to access documents from their DMS from within the Teams interface.

ETHICAL WALLS

Another common integration point for many firms to consider is Ethical Walls. While Microsoft 365 has a native feature called Information Barriers, it is limited compared to the features available in the ethical wall applications used by most firms. [13] Firms should consider how they might be able to integrate their existing ethical wall obligations into the Teams environment. This may require custom development or team owner administrative oversight of membership.

ACCEPTABLE USE

Teams can include a variety of content. By default, members can post documents, pictures, links, Gifs, videos and almost anything else you can imagine. Not everything they can post is acceptable in a professional setting. Teams gives you some control of what can be posted (see Messaging Policies, above), but you will likely want to issue guidance on what is appropriate for both internal-only teams and teams that have external guests.

NEW COMMUNICATION CHALLENGES
Communications within the collaboration platform present new challenges for governance because of the multitude of options. Distinguishing between matter level chats, document specific discussions, private chats, etc. becomes an early education process, informed by the level of the communication. A document level communication can properly be a knowledge additive to the document specifically and should, for example, be subject to the same storage, retention and disposition policy as the document itself. More general matter level communications may be viewed as transitory and subject to disposition like Slack type chats. These are best determined in conjunction with the practice in the first instance and then communicated to all users to avoid heartache.

ONGOING MANAGEMENT

As with most applications, individual teams require ongoing management. For example, team owners should be responsible for preserving content associated with users who have left the firm before their accounts are disabled in Azure Active Directory (AAD). Once an AAD integrated account is disabled, the content becomes associated with a System ID (SID) as opposed to a user account, so there isn't a way to positively identify the author of content.

Teams provides a variety of reports that allow administrators to understand the usage of Teams as a product, as well as for individual teams. This can be a necessary activity as the number of teams proliferate and it becomes advantageous to retire teams that are not actively used. Additional discussions on native reporting within Microsoft 365 is found in greater detail below.

There are also a wide variety of Microsoft 365 tools that help address security and privacy concerns. For example, there are built in tools that allow an easy implementation of data loss prevention specifically for Microsoft Teams, although you may need additional licensing.[14]

Finally, there are many different features in the Microsoft Compliance Centre that can be used to manage Teams content, allowing you to enact data classification, take actions based on the sensitivity of data and conduct a variety of audit functions.[15]

KEY TAKEAWAYS

A "sustain and maintain" plan should be established for the ongoing maintenance of any governance strategy, policies, configurations and business process affiliated with Teams. Microsoft updates 365 functionality and components regularly and often.

Any organisation needs an ongoing strategy to keep up with changes, adjust the implementation accordingly and sustain good governance of the environment.

RETENTION MANAGEMENT AND TEAMS

There are a variety of ways to apply the firm's retention policy to Teams content. You can apply retention and disposition policies to Teams within Microsoft 365 starting at the tenant level (most broad), through the Security & Compliance console and finally at the application level (most narrow). Because Teams data ends up in a variety of Microsoft 365 repositories, we recommend looking carefully at Microsoft's native retention and disposition capabilities with the goal of enacting your firm's retention policies using those tools where possible.

The retention assigned to team content should be determined based on the team type and should align with the retention policy and application methodology used for other firm data, whether it is a department team, a project team or a client-matter specific team. As an example, a team created for departments, administrative organisational units or for firm-wide use may be more permanent in nature and the information being created and managed (Channel Conversations and Files) may be retained longer term unless a retention policy is applied to the information. Retention can be applied to the team files and conversations when such a team is created and can be an ongoing (rolling) process (e.g. files or channel messages deleted 5 years after last modified date).

In contrast to the more permanent operational or departmental team, the lifecycle of project or matter-centric team will likely be limited in duration and any retention policy should be applied to the team content starting at a specific event such as the end of the project or close of the matter. At this event, the retention policy would be applied to the team's content by adding the team to the appropriate file and channel retention policies in the Compliance Centre. The appropriate policy can be applied at team creation, and it is recommended that the retention policy be considered in the development of the templates that are used to create a team. It is important to ensure that all content that may be considered part of the official file be moved to the appropriate repository prior to any retention policy execution on the content.

WHERE IS THE DATA?

Understanding where Microsoft stores Teams data is useful to inform the consequences of which method gets you to your retention and disposition goal. The chart below explains where some Teams data is stored.

FEATURE	STORAGE LOCATION
Chats / Exchange	User Mailbox
Conversations / Exchange	Group Mailbox
Channel	SharePoint

APPLYING RETENTION

While retention policies and the associated configuration for different aspects of the Teams environment may seem complex, it allows organisation to make granular decisions about how they intend to use different types of communications.

RETENTION POLICY OPTIONS (COMPLIANCE CENTRE)

Teams retention policies are created and applied through the Compliance Centre.[16] Retention policies can be applied to team files, chat and channel conversations through the compliance console. Three types of polices are available: retain, delete or retain and then delete. These policies can be triggered based on criteria such Creation Date or last Modified Date. (Note: Event-based retention is an available option within Microsoft 365 but as of the time of this writing is not appropriate for Teams related content such as files, chats or channel conversations. In addition, all features of Compliance Centre may not be available, depending on your Microsoft 365 licensing level).

Once a retention policy is created it can be applied to Teams content in one of three areas: Private Chats, Channel Conversations and Teams Channel file content. Retention policies can be applied to each of these areas separately. Due to the way that Microsoft 365 manages Private Chat and Channel Conversations, a policy must be created and applied to these items separately from any policy that may be applied to other Teams related content.[17] The requirement for separate policies increases the overhead and complexity of managing policies within the Microsoft 365 environment and should be a key IG consideration when planning the firm's Teams retention strategy.

PRIVATE CHATS

A Teams private chat can be one-to-one or one-to-many and are often viewed like traditional instant messaging. Firms may decide that Teams chat is a temporary communication mechanism that doesn't need to be retained and can have a retention period other than the retention period designated for the Team overall. Consider aligning the retention period of the chat message with the intended use of chat. For example, group chats are automatically created during Teams meetings and should only be kept if they are expected to have business use.

Another primary consideration with private chat retention is how retention is applied. Chat retention policies are applied to individual employees through the Compliance Centre. Decisions must be made on how the retention policy is applied (e.g. is there more than one chat retention policy or multiple policies based on requirement?)

CHANNEL MESSAGES

Channel messages differ from private chats as they are typically more project-related conversations. The type of team often determines the retention of its channel conversations. As an example, the lifecycle of operation teams can last many years and decades. Channel conversations should be deleted once their purpose is outdated and no longer needed. Alternatively, matter and/or project teams have set dates upon which they are considered "closed." Often conversations occurring at the start of the team are still relevant and should be kept until the matter or project is closed.

Firms may treat channel conversations like chats (see above) or like email threads that could be related to topical content of the team. In this instance, if the conversations are treated like email/email threads a decision may be made to apply a single overriding policy to all of the channel content across the firm or to have multiple policies based on type of team (see team-level retention below). (Note: channel retention is applied to teams, not individuals)

TEAMS FILES

The volume of file content stored in a team's underlying SharePoint library can become overwhelming quickly in active teams. Files should be deleted after a defined period to free up space, increase findability of relevant content and reduce eDiscovery and security risks.

Much like channel conversations, files should be removed depending on the type of team: as an example, the lifecycle of operation teams can last many years and decades. Files should be regularly removed after a defined time that considers anticipated business need, whereas a matter and project teams have a set date upon which they are considered "closed." Often content added to the team at the start of the team is still relevant and should be kept until the matter or project is closed.

RETENTION TRIGGERS

Since there are no trigger events available within a team, it is important to note the need to manually add a group to the retention policy created at the end of a matter or end of activity.

GROUP EXPIRATION POLICY
There's an additional concept of expiration with Microsoft 365. This policy detects activity within a group and will send a notification to a group owner if it's no longer active within a predetermined amount of time. When groups expire, it is "soft-deleted" and can be recovered for up to 30 days. This includes data from all its associated services (SharePoint, OneDrive, Planner, etc.). Owners will automatically be sent an email before the expiration date that will allow them to renew the group for another interval. You can set the expiration period for the group (e.g., 180 days – default is one year). The group expiration policy requires an Azure AD Premium license within the tenant (but does not require that license to be assigned). It is important to consider the natural progression of some types of matters (ie. IP) that may go dormant for extended periods. Firms may want to exclude those teams from an expiration policy.

KEY TAKEAWAYS

Retention policies may apply to many different types of content in a team: files stored in the team's SharePoint site, conversations in the Team's channel posts and chat conversations.

Organisations need to evaluate the retention requirements, business need and the maintenance impact of retention in the different areas of a team.

Implementing retention for any content (posts, chat, or files) within a team can be done in several ways. Consider evaluating retention approaches and comparing to the types of teams defined for the organisation. Can retention be streamlined in any way (such as all teams receive the same retention policy for chat)?

Law firms should evaluate each of the 3 areas of content within a team (posts, chats and files) and then consider the implications of retention given the nature of the content. Consider – is chat around a client matter different from business chat (or "water cooler" chat) that might happen on a more internal, organisation-focused team? Consider different retention policies and how those may be enacted and maintained for different areas of the firm, including any high-security, external-facing, guest-allowed or other specific use cases.

DISPOSITION MANAGEMENT

Teams fall out of use. Matters close, projects end and some teams are simply abandoned.

ARCHIVING A TEAM

When a team is no longer active, but it isn't ready to be deleted, the team can be archived. The Teams administrator can select to archive the team from the admin console. When a team is archived all activity for that team ceases. However, members can still be added and all the files and chats activities can still be viewed.[19] The team owner or an administrator can unarchive the team anytime. SharePoint and Wiki associated with the team are still active unless specifically edited to read only.

DELETING A TEAM

When a team is no longer needed it can also be deleted by the team owner or an administrator. Unlike archiving a team, deleting a team removes the underlying group framework. The team mailbox and calendar are deleted from Exchange. The corresponding SharePoint site and all its files are also deleted, and any OneNote notebook, Planner plan, Power BI workspace or Stream group affiliated with the team is deleted. Team owners and IT admins can recover deleted teams for up to 30 days.[20]

When a team is deleted, any content that is subject to a retention policy remains for the period specified (see Retention Policies above). As with all content in Microsoft 365, a legal hold takes precedence over any deletion activity, whether manual or by policy.

Because deleting a team removes the underlying group structure and related content, you must ensure that documents and related channel conversations are moved to the legal DMS for final storage (see Integrations above). Because not all content in a team is subject to retention policies, it is important to develop procedures for preserving content that is not subject to retention policies. Additional processes must be developed to handle non-traditional content such as OneNote notebooks, Forms survey structures and Planner project details.[21]

KEY TAKEAWAYS

Understand the difference between archival and deletion of a team.

A firm's legal hold process should be reviewed against the functionality of Teams and SharePoint; how will legal holds be activated and managed in Teams? How will this process be integrated into the existing litigation hold process?

A Teams disposition process should be defined by reviewing the firm's current retention and disposition processes and/or requirements, then evaluating the types of teams, content, and usage involved.

EXTERNAL ACCESS AND GUESTS

As your firm considers the various governance aspects involved in implementing Teams for internal users, further consideration needs to be given to whether, and then how, to grant access to external users. There are two ways to communicate and collaborate with people outside your organisation with Teams:

- **External access (federation)** – allows you to find and collaborate with users in other domains. External access is a way for Teams users from an external domain to find, call, chat and set up meetings with you in Teams.
- **Guest access** – adds individuals to your teams, as guests, using their email address. You can collaborate with guests as you would with any other user in your organisation

It is imperative that the rights available to external users are well understood by all parties. Once access has been granted, the ability to invite external domain users is quite open, making implementation of related policies and guidelines an imperative. Firms should also train internal users on the risks involved in inviting external users to Teams features.

EXTERNAL ACCESS

By default, external access is enabled in Teams. External access means that your organisation can communicate with all external domains and that external users in other domains can find, call, chat and set up meetings with you. External users have no access to your organisation's teams or team resources. If you add blocked domains, all other domains are allowed; and if you add allowed domains, all other domains are blocked. The exception to this rule is if anonymous participants are allowed in meetings.

EXTERNAL ACCESS OPTIONS

There are three scenarios for setting up external access in the Teams admin centre:

- Open federation: This is the default setting in Teams. It lets people in your organisation find, call, chat and set up meetings with people external to your organisation in any domain. In this scenario, your users can communicate with all external domains that are running Teams or Skype for Business AND are using open federation OR have added your domain to their allow list.
- Allow specific domains: By adding domains to an Allow list you limit external access to only the allowed domains. Once you set up a list of allowed domains all other domains are blocked.
- Block specific domains: By adding domains to a Block list you can communicate with all external domains except the ones you've blocked. Once you set up a list of blocked domains all other domains are allowed.

GUEST ACCESS

Use guest access to add an external user to a team. Once added as a guest they can chat, call, meet and collaborate on the teams' files. A guest user can be given nearly all the same capabilities as a native team member. *NOTE: Microsoft provides a detailed table comparing the capabilities of a guest and a Team member.*[22]

There are multiple levels of authorisation features that can be leveraged to manage guests (tenant admin, application portal and Teams application). Each has configuration options and settings that can be implemented to achieve the firm's desired user experience and meet the firm's security and governance policies. For instance, you can limit access to allow for only chat and restrict document sharing. It is important to understand the levels available and is critical to work with your IT team to support your necessary configuration needs.

KEY TAKEAWAYS

The method of allowing users access either as external users or guests depends on the specifics of the individual access needs. Some questions to consider:

- Do you have users in different domains who need to collaborate?
- Do you want the people in your organisation to use Teams to contact people in specific businesses outside of your organisation?
- Do you want anyone else in the world who uses Teams to be able to find and contact you, using your email address?

CONTENT SEARCH, LEGAL HOLDS AND EDISCOVERY

Microsoft Teams content can be searched and collected during eDiscovery investigations.

CONTENT SEARCH

Content Search is used to quickly find email, documents and instant messaging conversations in Teams (and Microsoft 365 Groups).

The key to searching is to first identify the various content locations in which to search (e.g., the underlying Group supporting the team, the team Chat or Channel conversations) and to configure a keyword query. The search tool allows for exporting content results, further searching and deleting email messages, and reporting on results. Leveraging PowerShell commands and scripts allows for advanced search tasks. MS 365 has provided various scripts online.

LEGAL HOLDS

When a reasonable expectation of litigation exists, organisations are required to preserve electronically stored information (ESI) including Teams chat messages that are relevant to the case. Organisations may need to preserve all messages related to a specific topic or for certain individuals.

Within Microsoft Teams an entire team or select users can be put on hold. Doing that makes sure that all messages exchanged in those teams (including private channels) or messages exchanged by those individuals are discoverable by the organisation's compliance manager or Teams Admins.[23] *NOTE: Placing a user on hold does not automatically place a group on hold or vice-versa.*

After the legal hold has been set you can use Microsoft 365's native eDiscovery features to identify and collect relevant content that has been preserved.

EDISCOVERY

Microsoft Teams content can be searched and used during eDiscovery investigations. As described in the above section "Where is the data?", in general, private chats and channel messages are stored in the individual's or Team's group mailbox, respectively. Chat related files or files uploaded or shared to a channel are discoverable in the corresponding SharePoint Online and OneDrive for Business locations. However, not all Teams content is discoverable. Microsoft provides a table detailing the content types that you can search for using Microsoft eDiscovery tools.[24]

EDISCOVERY OPTIONS

- **Core eDiscovery** - Core eDiscovery in Microsoft 365 provides a basic eDiscovery tool that organisations can use to search and export content, as well as place an eDiscovery hold on content locations in Microsoft 365 and Office 365 content repositories. Nothing is needed to deploy Core eDiscovery but there are some prerequisite tasks that an IT admin and eDiscovery manager must complete before your organisation can start using Core eDiscovery to search, export and preserve content.
- **Advanced eDiscovery** - Advanced eDiscovery provides an end-to-end workflow to preserve, collect, review, analyse and export content that is responsive to your organisation's internal and external investigations. It allows legal teams to manage the entire legal hold notification workflow to communicate with involved custodians. Advanced eDiscovery's built-in workflow aligns with the eDiscovery process outlined by the Electronic Discovery Reference Model (EDRM).

KEY TAKEAWAYS

Core eDiscovery is available with E3 licensing while Advanced eDiscovery requires E5 licensing.

eDiscovery tools can be very powerful so it's important to understand the features and limitations of each. Some firms may find that the built-in tools can act as a replacement for current discovery and hold tools, while others may need to continue to need the features in a dedicated eDiscovery application.

eDiscovery of messages and files in private channels works differently than in standard channels.

Doing deep dives is a must if you want to fully understand how the tools work and how they can work specifically for your firm.

PRIVACY / REGULATORY

Often when technologists discuss the issue of privacy as relates to Teams, the discussion refers to whether a team instance is Public or Private. For IG professionals, security and compliance standards like HIPAA and GDPR mandate data governance measures such as enterprise-wide labeling, oversight and tracking of content, as well as appropriate handling of data that has expired or changed classification. It's challenging to impose this level of control on the dispersed ecosystem of chat messages and data files circulating through Teams and can require identification of specific requirements per team.

Regulatory-specific concerns about the data can require a deeper level of classification than simply client and matter. While client and matter based classification provides the ability to define templates, apply security and wall-based restrictions and execute on discovery and legal holds, it does not permit further classification regarding the content of the data. Consideration should be given to ways that regulatory-based classification can be applied to content and at what level that classification should be applied (team, channel, etc.).

Data residency can also be a concern if your firm must abide by the data protection and compliance regulations of each individual region and multi-geo services currently exist for Exchange Online and OneDrive but are in preview or under development for SharePoint Online and Teams. Also, of consideration is the nature of the Teams content. Messages and images are ingested into Exchange, files are stored in SharePoint and chat messages are stored in OneDrive, meaning that one team may have content in multiple repositories.

METRICS AND REPORTING

Given the remarkable speed with which firms adopted Teams, the ability to report metrics around activity and usage provides valuable insight into user adoption. Native Microsoft 365 reporting provides the ability to monitor user activities like number of users in Microsoft 365, number of active users in teams/channels, active channels, messages, privacy settings of a team and guests in a team, to name a few. Auditing on, and reporting of, user behavior and activity informs who is using Teams and for what purposes. Further, reporting can be used by firms to inform policy creation.

From a compliance perspective, firms will find it necessary to understand where sensitive data exists throughout the ecosystem to comply with regulatory and data privacy concerns. Using tagging and classification, in addition to reporting, it's possible to see not only where the data exists but with whom it's being shared internally and externally. Additionally, there are third party tools that can help with this type of monitoring.

See Appendix A for a list of native reports.

LAW FIRM SPECIFIC CONSIDERATIONS

Largely, we have addressed Teams governance considerations that apply to all types of Teams implementations. Law firms, by the nature of their business, have considerations that go beyond those of a general implementation.

CLIENT COLLABORATION

Collaboration spaces, like Teams, are an excellent opportunity to develop an integral working relationship with clients while providing essential legal services. The free flow of ideas and communication directly with the client provides endless possibilities to grow and expand the relationship. One of the first decisions a law firm needs to make when setting up Teams is whether the sites will be accessible to external users. If the answer is yes, the challenge is to do this in a manner that continues to uphold the fiduciary responsibilities and jurisdictional regulations that guide the attorney-client relationship.

Firms should consider what guidelines should be provided to attorneys when using Teams with clients. Attorneys should strategise on how they will maintain attorney/client privilege, as well as attorney work product within a team shared with clients and other third-party collaborators. Knowing when communication is legal advice versus business advice may be key to maintaining these basic tenets of the attorney-client relationship.

Attorneys will need to be careful not to be swept up in the casual flow of a team or private chat. There may be cause for concern as 'chats' may be too akin to text messages for people to consider the consequences of this free flow of communication. Information conveyed utilising these conversation strings should be just as carefully considered as any other legal communication. Back in the day, email was considered too informal for legal discussions but over time this attitude has changed; hopefully this learning curve will be faster for chats and channels.

DOCUMENT PROVENANCE

Another important discussion around the use of Teams with a client is if the client or another third-party is hosting the team site. Firms need to examine policy guidance to establish when (or if) it is acceptable to collaborate with the client on legal work when the team collaboration site is hosted by the client. Any documents authored or edited on a client/third-party site should be downloaded to the law firm's proper client electronic repository to maintain an appropriate file of the representation. The documents hosted on these SharePoint sites will maintain the multiple versions and metadata. The SharePoint sites maintain a record of who said what and when, so it may be better to develop a practice of uploading drafts for review with the client and downloading the edits occasionally while collaborating with others. Additionally, any chats related to the document that are held on a client/third-party site are subject to the retention terms of the third-party. Attorneys that need to retain the chat data must ensure they quickly move it to their own systems of record.

ETHICAL WALLS

Provisioning an internal team in a law firm is complicated by the various security arrangements that are required. In addition to client authentication security requirements, law firms also need to consider how they implement the security required for ethical walls or confidentiality screens. Considering how the firm secures information by client or matter may need to be reviewed even before the first teams are established. Are you able to affect the same level of confidentiality and security while still enabling a site to be a useful collaboration environment? One of the fundamental considerations is to determine who can create a team and who may be able to add people to a team. What instructions will they be provided? How will the firm audit who has rights to a site to maintain the various security requirements?

MATTER MOBILITY

Probably one of the most difficult issues that needs to be addressed with collaboration sites such as Teams is matter mobility. If internal firm teams contain client matter information, then the client may have a right to the data. While the exact content of the client file may vary across jurisdictions, firms still need to grapple with this issue. How will the firm review the different pieces of information to determine what should and should not be transferred to another firm or to the client? What format will be used if the client or new firm do not use Teams? How will they produce the material that is attorney work product? These are all important questions that need to be considered as the Firm goes about the process of setting up the Team sites, even if they only maintain them internally.

CONCLUSION

Teams provides a very powerful collaborative space for people inside and outside your firm, allowing for chat to drive conversations, secure sharing and coauthoring of documents. Every firm is different; there's no one-size-fits-all approach. When deciding how to implement Teams, think about the work your firm does and the types of conversations your teams need to have. Keep in mind that the Microsoft 365 ecosystem is constantly changing and plan to have a strong change management plan in place, as well as good communication and training plans for your users.

APPENDIX A – NATIVE REPORTS

- Data Classification/PII Data – GDPR, HIPAA, California SB-1386, MA 201 CRM 17, PHI-US
- Sensitive Files in O365 being shared externally
- Team Name Changes – We have a Team naming convention that helps me easily identify c/m# Teams v. Admin Teams, this report shows me if an end user alters a Team name
- Team Site Channel Created – Useful to monitor if a c/m# channel is set up in an Admin Team
- Team Chat File Sharing
- Azure User Inactivity >60 Days
- Team Site Inactivity >90 Days
- How many users communicate through channel and chat messages?
- Teams usage report (active users, active users in teams/channels, active channels, messages, privacy settings of a team, guests in a team)
- Team user activity report (1:1 calls a user participate in, messages a user posted in a team chat, messages a user posted in a private chat, last activity date of user)
- Teams device usage report (Windows users, Mac users, iOS users, Android phone users)
- Teams live even usage report (Total views, start time, even status, organiser, presenter, producer, Recording setting, Production type)
- Teams PSTN blocked users report (Display name, phone number, reason, action type, action date and time)
- How many members are Team owners adding?
- Users signed in
- Apps installed
- Adoption/Engagement – usage metrics

APPENDIX B – MEMBER-OWNER COMPARISON [26]

Task	Owner	Member
Create team	Yes*	No
Leave team	Yes	Yes
Edit team name/description	Yes	No
Delete team	Yes	No
Add standard channel	Yes	Yes*
Edit standard channel name/ description	Yes	Yes*
Add private channel	Yes	Yes*
Edit private channel name/ description	No	N/A *
Delete private channel	Yes	No
Add members	Yes	No
Request to add members	N/A	Yes*
Add apps	Yes	Yes*

Can be restricted

ENDNOTES

[1] Teams has over 115 million daily users as of October 2020, up from 75 million users 6 months prior

[2] https://docs.microsoft.com/en-us/microsoftteams/limits-specifications-teams

[3] https://docs.microsoft.com/en-us/microsoftteams/private-channels

[4] Microsoft 365 groups naming policy | Microsoft Docs

[5] https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide

[6] https://support.microsoft.com/en-us/office/team-owner-member-and-guest-capabilities-in-teams-d03fdf5b-1a6e-48e4-8e07-b13e1350ec7b

[7] Assign team owners and members in Microsoft Teams - Microsoft Teams | Microsoft Docs

[8] https://docs.microsoft.com/en-us/microsoftteams/guest-access

[9] https://docs.microsoft.com/en-us/microsoftteams/guest-experience

[10] Assign team owners and members in Microsoft Teams - Microsoft Teams | Microsoft Docs

[11] https://docs.microsoft.com/en-us/microsoftteams/messaging-policies-in-teams

[12] https://docs.microsoft.com/en-us/microsoftteams/meeting-policies-in-teams

[13] https://docs.microsoft.com/en-us/microsoftteams/information-barriers-in-teams

[14] https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide

[15] https://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide

[16] https://docs.microsoft.com/en-us/microsoftteams/retention-policies

[17] Create and configure retention policies to automatically retain or delete content - Microsoft 365 Compliance | Microsoft Docs

[18] Retention policies in Microsoft Teams - Microsoft Teams | Microsoft Docs

[19] https://docs.microsoft.com/en-us/microsoftteams/archive-or-delete-a-team

[20] https://docs.microsoft.com/en-us/microsoftteams/archive-or-delete-a-team

[21] https://docs.microsoft.com/en-us/microsoft-365/solutions/end-life-cycle-groups-teams-sites-yammer

[22] https://docs.microsoft.com/en-us/microsoftteams/guest-experience

[23] https://docs.microsoft.com/en-us/microsoftteams/legal-hold

[24] https://docs.microsoft.com/en-us/microsoftteams/ediscovery-investigation

[25] Microsoft 365 Multi-Geo - Microsoft 365 Enterprise | Microsoft Docs

[26] Assign team owners and members in Microsoft Teams - Microsoft Teams | Microsoft Docs

IRON MOUNTAIN®

08445 60 70 80 | IRONMOUNTAIN.CO.UK

R.O.I. 1800 732 673 | N.I. 08445 60 70 80 | IRONMOUNTAIN.IE

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.

UKILGL-RPT-062121A