External Sharing and Guest User Access in Microsoft 365 and Teams

A guide for developing and enforcing the right policy for your organization

AvePoint®

Table of Contents

Introduction

Microsoft Teams has become the central productivity hub for organizations today. Its value in enabling business continuity and collaboration can be seen in a nearly 500 percent increase in daily active users since the start of the COVID-19 pandemic.

It only makes sense that this surge in usage is also reflected by a strong demand to collaborate with individuals outside of the organization. Microsoft Teams brings chat, video and file sharing together in a way email simply can't match.

We have great news. Microsoft Teams can be securely configured to enable outsiders to participate as guest members of a Teams workspace and to enjoy many of the same functions that insiders use. Teams can also be set up to support telephony and chat capabilities across organizational boundaries, providing a new and enhanced telephone service for modern times.

And various other services in Microsoft 365 that are part of Teams — such as SharePoint and OneDrive — can also be configured to support secure and controlled sharing with outsiders.

If it sounds like there are many options for configuring secure and controlled sharing for Microsoft Teams, you'd be right. Microsoft 365 is a set of (sometimes loosely) interconnected services that provide lots of flexibility. This is perfect for productive collaboration, but it also creates complexity.

Microsoft's challenge is to address the different, overlapping, and frequently conflicting needs of the hundreds of millions of people and the organizations they work for. This means it's almost certain you can get Microsoft Teams and Microsoft 365 to work for your organization, but you'll have to configure it to do so — and probably add some third-party tools to the mix too.

We are going to assume you are open to the idea of collaborating with outside users in Microsoft 365 (formerly Office 365). After all, you have taken the time to download and read this e-book.

But it's safe to say that somewhere in your organization — and we're trying hard not to glance over at the security and compliance team when we say this — the proposal to enable external sharing and guest user access will run into resistance.

So, before we show you which toggles to flip, we are going to share some of the common objections and how to overcome them. Drafting coherent and organizationally appropriate policies can accelerate this process; we'll explain how to develop those as well.

We will then go step by step through the complex and layered approach of configuring Microsoft 365 and Microsoft Teams in alignment with your policies.

Outsider Access Vocabulary

Before we continue, it’s worth getting some clarity on the terminology used to describe the ability of outsiders to gain secured access to Microsoft Teams and SharePoint Online.

There are three very similar terms that refer to the same concept, but each has a different scope and focus:

Guest Access

Guest Access to provides outsiders with access to the content inside a Microsoft Teams workspace — such as the channels, discussions, and shared files stored in SharePoint Online. This is controlled at the individual user level; setting it up correctly is the focus of this e-book.

External Access

External Access for enabling outsiders to use one-to-one chat capabilities to interact with your insiders via Microsoft Teams. External access is controlled at the domain level, not the individual user level, and is not the focus of this e-book.

External Sharing

External Sharing that gives outsiders access to the content inside a SharePoint site. Multiple controls can be configured at different levels for external organizations (e.g., by domain name) and by user. Since External Sharing can be set up independently of Guest Access to provide backdoor access to the documents and files stored in a Teams workspace, it is also a focus in this e-book.

In this e-book, we use the general term “access by outsiders” to refer to the idea of providing secure access to people that don’t work for your organization directly. When using any of the above terms specifically, we will put it in italics for clarity.

Overcoming Objections

Let’s take our proposal for sharing with outsiders to Megan Smith, the chief risk and compliance officer, at Contoso.

Focused only on the benefits, you might start a conversation like this:

> “Wouldn’t it be great if we were able to collaborate in Microsoft Teams with the vendors, contractors, and other people outside of our organization that we work with on a regular basis? It would make sharing documents easier and enable co-authoring, which would make us much more productive.”

In response, however, Megan could share several concerns.

> “Once we open the gates, there is no putting the horse back in the barn. Once guest users are in our environment, how are we going to ensure they don’t access sensitive data? How will we kick them out when they are no longer needed?

> “Our users have only just become accustomed to Teams; asking them to be perfect in how they apply permissions at the workspace and document levels is asking a lot of someone who is thinking about the task at hand first and security second. It’s just too easy to overshare.

> “There is too much risk here and even if some users may be resorting to shadow IT, we don’t want to take on the liability of having that level of risk in our sanctioned environment.”

Megan is not wrong. Without the right policies and controls, your information security is only as strong as your weakest link.

Try reframing your approach. Focus instead on convincing Megan that the risk of disabling external sharing and guest user access is far greater than enabling it.

> “The reality is modern organizations don’t do everything alone; they rely on networks of outsiders to perform and execute various work tasks. Sharing with outsiders isn’t a new idea, even though the mechanisms for doing so are changing.”

Consider these talking points to support your position:

> “Using email to send documents to anyone has been a mainstay of business for decades, even though security controls are significantly lacking. Once an attachment is sent, there is no control over who is accessing that data”

> “By enabling external sharing and guest user access, we can migrate collaboration to Microsoft Teams to leverage best practice approaches and additional functionality so we can mitigate the risk and loss of control via email.”

> “We will be able to verify identities using multifactor authentication to know exactly which workspace our guests can access and what specific data they access. We’ll also be able to monitor and enforce our policies and revoke access at any time.”

By now, Megan might ask how exactly this will all be done. Her team has security audits that will need to be passed. The chief information officer might ask how much it will cost and who will oversee the initiative.

After reading this e-book, you will be able to give them both an answer.

Policy Considerations

Before configuring Microsoft 365 to enable access to outsiders, several basic policy decision points must be addressed first.

While there are many ways to develop and tailor the appropriate policies for your organization’s unique needs at a granular level, here are a few of the most important top-line considerations.

Who should be allowed to be invited as a guest?

Determine if the agility, regulatory and sensitivity levels of your work environment are more appropriate for a policy that is everyone except or a policy that is no one except those from specific organizations or domains.

Once that determination has been made, coordinate with business stakeholders to either build a list of common collaborators (such as vendors) to whitelist or to identify organizations that may need to be blacklisted (such as competitors).

In general, highly regulated and sensitive environments will want to deploy a no one except policy while most organizations will want to deploy an everyone except policy while layering on more protections for specific workspaces and files downstream.

Note: The allow/deny list is NOT infinite. The entire policy can consist of only 25,000 characters. This means if you are a large organization and want to granularly specify hundreds of allowed domains, you will likely run into this limitation.

Cheat Sheet: ***Who should be allowed to be invited as a guest?***

A. Everyone except _____________.

B. No one except _____________.

Should guests be allowed to see the organizational directory?

In most cases, it would be inappropriate for guests to be able to look up or contact anyone within the organization. The best practice is to limit access to only those who are members of the same Team as the guest.

Cheat Sheet: ***Should guests be allowed to see the organizational directory?***

A. Yes

B. Limit to members of the same Team only

Who should be allowed to admit new guests to the Microsoft Teams environment?

When a user would like to have a guest added, there needs to be a process for admitting them into the environment. There are two people who can add an external user to a Team using Microsoft 365 native functionality: an IT admin or the Owner of the Team.

Microsoft 365 will never let a member of a Team invite a net new external guest. Depending on the selected settings, however, members could add and share with guests who are already in Active Directory but not members of that specific Team.

The challenge with having only IT admins add new guest users creates a bottleneck. They're also not as close to the business needs, so managing the lifecycle of a guest — when they need to be onboarded and offboarded — can be a challenge.

On the other hand, not every organization is comfortable with enabling any Team Owner to admit new guests which then presents two options:

1. Enable Team Owners to invite guests and then lock down specific Teams where sensitive work is being done. This requires coding through Powershell or configuring sensitivity labels so they can be applied to Groups and workspaces. Both options can be tedious to maintain at scale and could require upgraded licenses, depending on the application.
2. Deploy a third-party solution such as AvePoint's Cloud Governance to enable an approval process for admitting guests. Because Cloud Governance can guide users to correctly categorize the purpose during the creation process, specific types of Teams can be permitted or prohibited from allowing guests.

***Cheat Sheet:** Who should be allowed to admit guests to Microsoft Teams?*

A. Microsoft 365 administrators only

B. Any Microsoft Team Owner

C. Any Microsoft Team Owner except for the Owners...

- ...of these specific Teams
- ...of Teams with a certain sensitivity level
- ...of Teams within this department
- ...of Teams designated for internal collaboration

***Cheat Sheet:** Do you want requests for external guests to have an approval process?*

A. Yes

B. No

What type of guests should be able to access files in SharePoint and OneDrive?

This is a separate concern from the considerations around guests in Microsoft Teams — and, as we will see later, it is a separate process. First, determine what *external sharing* settings make sense for your organization in SharePoint and OneDrive.

Some organizations make the choice to lock down Microsoft Teams and only allow external sharing via SharePoint. There are valid use cases for this choice, but for the purposes of this e-book we are assuming the goal is to enable collaboration in Microsoft Teams.

Conversely, it is possible to enable guests in your Microsoft Teams without giving them access to the Group-related resources such as SharePoint or OneNote. Since this defeats much of the intention and value of collaborating in Microsoft Teams, we are not aware of many organizations that select this option.

Most organizations will want to mirror those allow/deny settings in SharePoint. Maintaining this sync can be a tedious process filled with gaps without third-party tools.

The real choice comes down to whether you want to enable external sharing with existing guests only in the directory or also with new guests that verify via a one-time passcode.

You can also choose to external sharing set globally or create different external sharing permissions for individual SharePoint sites. Unlike Microsoft Teams, this does not require the use of Powershell. Similar to Microsoft Teams, it does require considerable manual work on behalf of admins to maintain or it requires deploying sensitivity labels to a workspace. Both of those options can be very difficult to deploy and maintain securely at scale.

Solutions such as AvePoint Cloud Governance can dramatically increase your security while decreasing the amount of time spent on these tedious site-by-site governance tasks and preventing configuration drift.

Our recommendation for those planning to only leverage native functionality: Only enable external sharing with existing guests, if possible, for your organization. Otherwise, you will be making a complex task more complex.

Cheat Sheet:* What type of guests should be able to access files in SharePoint and OneDrive?

A. Guests that are already in the directory

B. New and existing guests

C. I want to have different file sharing settings for certain types of sites

**You could also choose option "D. Anyone with a link." Don't choose option D.*

How will guests be offboarded?

Just like in real life, lingering guests can ruin the party. The reason for their invitation could no longer be relevant or the Team they were a part of was disbanded. But without an admin actively taking the step to remove them from Azure AD, those guests still have access to your environment.

Take a moment to survey your administration team. Ask them how many have proactively removed a guest from Azure AD in the last year because they no longer needed access. It will not be a high number — admins and end users are busy and coordinating on guest access isn't at the top of their list.

At this point, all it takes is for someone in your organization to accidentally invite the wrong "Bob Smith" to a Team with sensitive information and voila: You have a data breach.

The challenge is that while Microsoft 365 offers an automated way for Team Owners to request guests be added to the environment, it doesn't offer an automated way for anyone within the business to request they be removed from Active Directory.

Here's the catch: An AAD P2 license provides Azure AD Access Review functionality, but that will only prompt Group owners to review and remove guests *from their Groups* on a periodic basis — NOT the directory. Veteran admins know this means a flood of IT tickets in the best-case scenario (and a cluttered and unsecured Active Directory at worst).

***Cheat Sheet:* How will guests be offboarded?**

A. This is not a big concern for my organization.

B. We'll create a process where admins manually and routinely track guests to determine whether their access level is still needed.

C. We will investigate a third-party tool for automating the process.

How will you determine who has access to sensitive information in your environment?

Let's say you have a security incident or an audit on the horizon. You will be asked if a specific guest or any outsider had access to sensitive information. A common assumption is you can review the workspaces (Teams, Groups, Sites) of which the person was a member to determine this information.

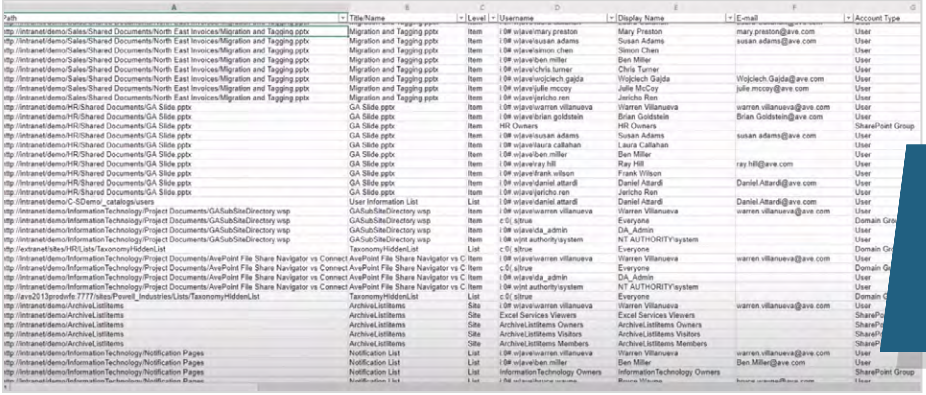
As covered in our [Mitigating Collaboration Risk Workbook](), this is only part of the story.

Guests can be granted permission to specific files and documents s completely independent of their workspace membership with the simple click of the "share" button by any workspace member.

This is a critical and often overlooked point, so it bears repeating: **The permissions of a Team and the permissions of the documents within them are almost entirely independent on one another.**

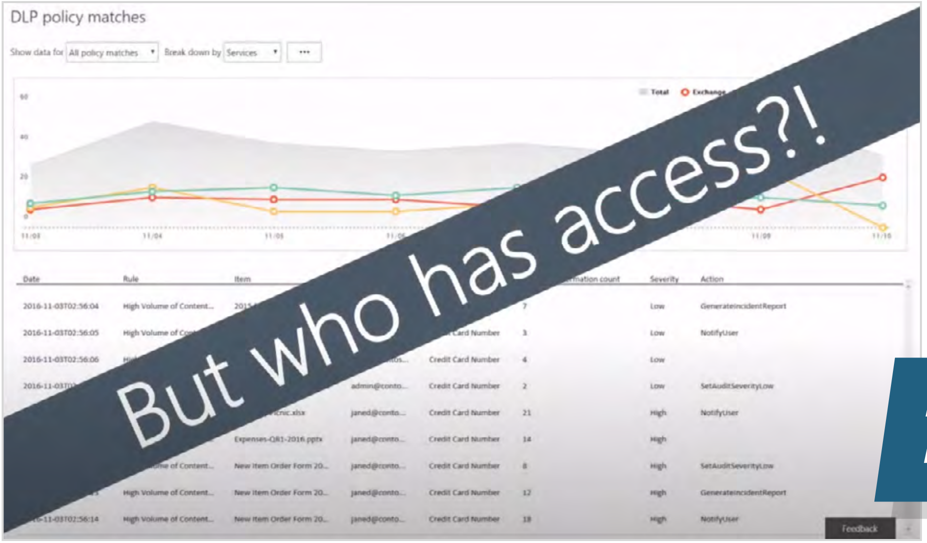
If your organization has advanced licenses, setup and deployed sensitivity levels to workspaces, the sensitivity level of the Team will not impact the ability of a document within it to be shared. But if a document has been given a higher sensitivity level than the sensitivity level of a workspace, it will simply notify the user (not the admin) with no enforcement actions taken.

For example, a guest may not be a member of the "Secret Project" Team, but if someone takes a file from that Team and selects "Anyone in Contoso with the link" setting and sends it to the guest via chat, they now have access.



Path	Title/Name	Level	Username	Display Name	E-mail	Account Type
ttp://intranet/demo/Sales/Shared Documents/North East Invoices/Migration and Tagging.pptx	Migration and Tagging.pptx	Item	i:0#.w|ave\mary.preston	Mary Preston	mary.preston@ave.com	User
ttp://intranet/demo/Sales/Shared Documents/North East Invoices/Migration and Tagging.pptx	Migration and Tagging.pptx	Item	i:0#.w|ave\susan.adams	Susan Adams	susan.adams@ave.com	User
ttp://intranet/demo/Sales/Shared Documents/North East Invoices/Migration and Tagging.pptx	Migration and Tagging.pptx	Item	i:0#.w|ave\simon.chen	Simon Chen		User
ttp://intranet/demo/Sales/Shared Documents/North East Invoices/Migration and Tagging.pptx	Migration and Tagging.pptx	Item	i:0#.w|ave\ben.miller	Ben Miller		User
ttp://intranet/demo/Sales/Shared Documents/North East Invoices/Migration and Tagging.pptx	Migration and Tagging.pptx	Item	i:0#.w|ave\chris.turner	Chris Turner		User
ttp://intranet/demo/Sales/Shared Documents/North East Invoices/Migration and Tagging.pptx	Migration and Tagging.pptx	Item	i:0#.w|ave\wojciech.gajda	Wojciech Gajda	Wojciech.Gajda@ave.com	User
ttp://intranet/demo/Sales/Shared Documents/North East Invoices/Migration and Tagging.pptx	Migration and Tagging.pptx	Item	i:0#.w|ave\julie.mccoy	Julie McCoy	julie.mccoy@ave.com	User
ttp://intranet/demo/Sales/Shared Documents/North East Invoices/Migration and Tagging.pptx	Migration and Tagging.pptx	Item	i:0#.w|ave\jericho.ren	Jericho Ren		User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\warren.villanueva	Warren Villanueva	warren.villanueva@ave.com	User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\brian.goldstein	Brian Goldstein	Brian.Goldstein@ave.com	User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	HR Owners	HR Owners		SharePoint Group
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\susan.adams	Susan Adams	susan.adams@ave.com	User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\laura.callahan	Laura Callahan		User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\ben.miller	Ben Miller		User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\ray.hill	Ray Hill	ray.hill@ave.com	User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\frank.wilson	Frank Wilson		User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\daniel.attardi	Daniel Attardi	Daniel.Attardi@ave.com	User
ttp://intranet/demo/HR/Shared Documents/GA Slide.pptx	GA Slide.pptx	Item	i:0#.w|ave\jericho.ren	Jericho Ren		User
ttp://intranet/demo/C-SDemo/_catalogs/users	User Information List	List	i:0#.w|ave\daniel.attardi	Daniel Attardi	Daniel.Attardi@ave.com	User
ttp://intranet/demo/InformationTechnology/Project Documents/GASubSiteDirectory.wsp	GASubSiteDirectory.wsp	Item	i:0#.w|ave\warren.villanueva	Warren Villanueva	warren.villanueva@ave.com	User
ttp://intranet/demo/InformationTechnology/Project Documents/GASubSiteDirectory.wsp	GASubSiteDirectory.wsp	Item	c:0(.s|true	Everyone		Domain Gro
ttp://intranet/demo/InformationTechnology/Project Documents/GASubSiteDirectory.wsp	GASubSiteDirectory.wsp	Item	i:0#.w|ave\da_admin	DA_Admin		User
ttp://intranet/demo/InformationTechnology/Project Documents/GASubSiteDirectory.wsp	GASubSiteDirectory.wsp	Item	i:0#.w|nt authority\system	NT AUTHORITY\system		User
ttp://extranet/sites/HR/Lists/TaxonomyHiddenList	TaxonomyHiddenList	List	c:0(.s|true	Everyone		Domain Gr
ttp://intranet/demo/InformationTechnology/Project Documents/AvePoint File Share Navigator vs Connect	AvePoint File Share Navigator vs C	Item	i:0#.w|ave\warren.villanueva	Warren Villanueva	warren.villanueva@ave.com	User
ttp://intranet/demo/InformationTechnology/Project Documents/AvePoint File Share Navigator vs Connect	AvePoint File Share Navigator vs C	Item	c:0(.s|true	Everyone		Domain Gr
ttp://intranet/demo/InformationTechnology/Project Documents/AvePoint File Share Navigator vs Connect	AvePoint File Share Navigator vs C	Item	i:0#.w|ave\da_admin	DA_Admin		User
ttp://intranet/demo/InformationTechnology/Project Documents/AvePoint File Share Navigator vs Connect	AvePoint File Share Navigator vs C	Item	i:0#.w|nt authority\system	NT AUTHORITY\system		User
ttp://ave2013prodwfe:7777/sites/Powell_Industries/Lists/TaxonomyHiddenList	TaxonomyHiddenList	List	c:0(.s|true	Everyone		Domain G
ttp://intranet/demo/ArchiveListItems	ArchiveListItems	Site	i:0#.w|ave\warren.villanueva	Warren Villanueva	warren.villanueva@ave.com	User
ttp://intranet/demo/ArchiveListItems	ArchiveListItems	Site	Excel Services Viewers	Excel Services Viewers		SharePo
ttp://intranet/demo/ArchiveListItems	ArchiveListItems	Site	ArchiveListItems Owners	ArchiveListItems Owners		SharePo
ttp://intranet/demo/ArchiveListItems	ArchiveListItems	Site	ArchiveListItems Visitors	ArchiveListItems Visitors		ShareP
ttp://intranet/demo/ArchiveListItems	ArchiveListItems	Site	ArchiveListItems Members	ArchiveListItems Members		ShareP
ttp://intranet/demo/InformationTechnology/Notification Pages	Notification List	List	i:0#.w|ave\warren.villanueva	Warren Villanueva	warren.villanueva@ave.com	User
ttp://intranet/demo/InformationTechnology/Notification Pages	Notification List	List	i:0#.w|ave\ben.miller	Ben Miller	Ben.Miller@ave.com	User
ttp://intranet/demo/InformationTechnology/Notification Pages	Notification List	List	InformationTechnology Owners	InformationTechnology Owners		SharePoint Group
ttp://intranet/demo/InformationTechnology/Notification Pages	Notification List	List	i:0#.w|ave\bruce.wayne	Bruce Wayne	bruce.wayne@ave.com	User

Combing through thousands of lines in a permission report is like looking for a needle in a haystack



Date	Rule	Item	[illegible]	[illegible]	...mation count	Severity	Action
2016-11-03T02:56:04	High Volume of Content...	2015[illegible]	[illegible]	[illegible]	7	Low	GenerateIncidentReport
2016-11-03T02:56:05	High Volume of Co[illegible]	[illegible]	[illegible]	...Card Number	3	Low	NotifyUser
2016-11-03T02:56:06	Hi[illegible]	[illegible]	...tos...	Credit Card Number	4	Low	
2016-11-03T0[illegible]	[illegible]	[illegible]	admin@conto...	Credit Card Number	2	Low	SetAuditSeverityLow
[illegible]	[illegible]	...icnic.xlsx	janed@conto...	Credit Card Number	21	High	NotifyUser
[illegible]	[illegible]	Expenses-QR1-2016.pptx	janed@conto...	Credit Card Number	14	High	
[illegible]	...me of Content...	New Item Order Form 20...	janed@conto...	Credit Card Number	8	High	SetAuditSeverityLow
[illegible]	High Volume of Content...	New Item Order Form 20...	janed@conto...	Credit Card Number	12	High	GenerateIncidentReport
...6-11-03T02:56:14	High Volume of Content...	New Item Order Form 20...	janed@conto...	Credit Card Number	18	High	NotifyUser

DLP reports only tell part of the story

Natively, the only way to know for sure which guests have access to which types of documents is to peruse permission reports, audit reports and DLP reports. These are not only siloed but contain thousands of lines of information.

There are third-party solutions that will highlight which documents are being shared with external guests, but only AvePoint's Policies and Insights can tell you if that data is sensitive (whether you have classified your data or not).

***Cheat Sheet:** How will you determine who has access to sensitive information in your environment?*

A. Reviewing workspace permissions will get us close enough

B. Periodic reviews using native tools and revoke improper access as we identify it

C. Third-party solutions to monitor and prevent oversharing sensitive information with guests

Scoring your cheat sheets: What's next?

□ If you mostly chose **option A**, then an open scenario is appropriate for your organization.

□ If you mostly chose **option B**, then a "some control" or "significant control" scenario is appropriate for your organization, but you may also want to investigate how third-party solutions can alleviate the time burden on your IT team and expedite user requests for external collaboration.

□ If you chose **option C** for any question, you will want to request a demo to see Cloud Governance and Policies and Insights in action.

Mark down or remember your selections. After our walkthrough of the different external sharing settings in Microsoft 365, we will show you how to configure specific settings tailored to all of the scenarios listed above.

The Layers of Guest Access & Common Challenges

As previously mentioned, configuring external sharing in Microsoft 365 is complicated with interdependent settings across six different admin interfaces. So, we will use an analogy to simplify the process — the security precautions many organizations take to access their physical environments.

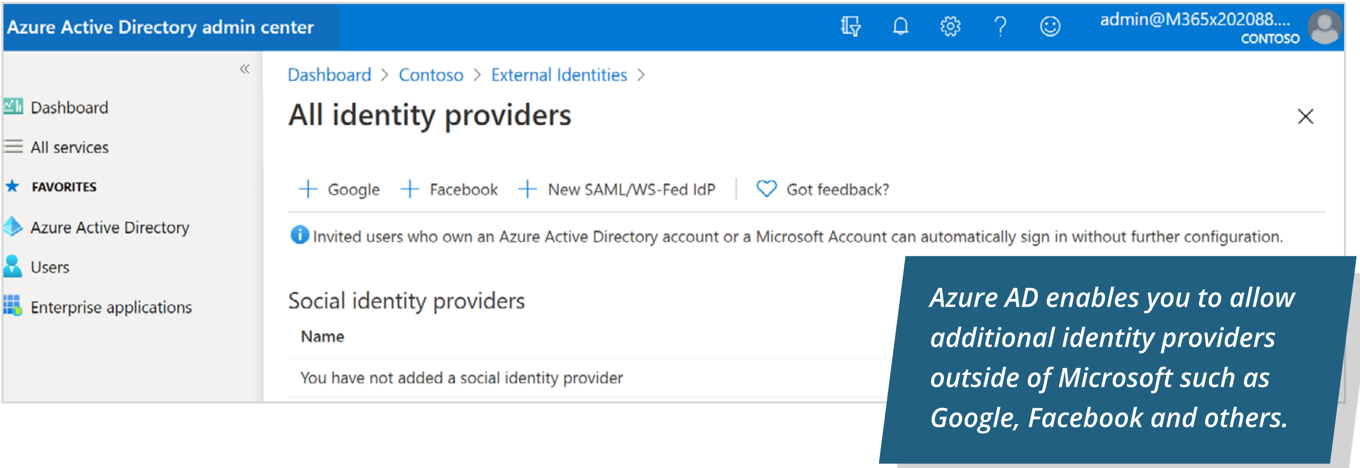
Editor Note: the analogy and layers discussed in this chapter is assuming a typical organization with an E3 license that does not include workspace sensitivity labels. We will briefly cover the label approach, along with its strengths and weaknesses, at the conclusion of the chapter.

If you invite an outsider to come to your office building for a meeting, they will go through several levels of security checks in order to gain access to the meeting room and sensitive information being shared within that room.

Azure AD: Accessing the campus

Microsoft's layered model of security settings for securing and controlling outsider access to Microsoft Teams and Microsoft 365 begins with organization-wide settings in the Azure AD Admin Center.

These global settings focus on verifying identity and setting the rules under which outsiders can be added to the directory (and by whom), along with their rights once established. An organization can have 5 guest users for every paid license.



All identity providers

Invited users who own an Azure Active Directory account or a Microsoft Account can automatically sign in without further configuration.

Social identity providers

Name
You have not added a social identity provider

Azure AD enables you to allow additional identity providers outside of Microsoft such as Google, Facebook and others.

The Microsoft 365 external sharing model is set up so that guests need to verify with their own identity provider and then you can choose to add on more stringent requirements for signing into your environment. This is a great feature, as it means that when a user leaves their home organization (perhaps from a partner to a competitor) their account is no longer active, and they no longer have the means to log in as a guest to *your* environment.

As we depicted in our cheat sheet, the key settings at the Azure AD level are to determine if guests can see your entire membership directory or just the members of Teams to which they belong.

This is also where you can select the "Admins and users in the guest inviter role can invite" toggle to determine if administrators can invite guests through the admin interface. It will need to be toggled on to allow Team Owners to invite guests through additional settings downstream. You could also choose to allow guests to invite other guests, but most organizations don't do this.

CASE STUDY

Cloud Governance Helps Cambridge Consultants Achieve 94 Percent Adoption While Avoiding Sprawl in Microsoft Teams

Cambridge has 900 employees in seven offices around the world. The company has been around for over 60 years and tackles an average of more than 400 projects each year.

Their engineers, designers, scientists, and consultants work on projects that contain sensitive information, and access to the project data is on a strict need-to-know basis.

During the adoption process of Microsoft Teams, Cambridge Consultants were looking for a governance tool to sync membership with Active Directory Security Groups and enforce consistent access across all their systems.

"For many years we have had a custom solution that allows our project managers to update Active Directory security groups with authorized project team members," explained Julie Peck, enterprise applications architect at Cambridge Consultants. "The security groups are then used by all of our applications that store project data. It was really important to us that Teams followed the same model."

To ensure strong end-user adoption, Cambridge Consultants wanted to enable users to self-create Teams while also controlling risks to sprawl, and unauthorized access to content.

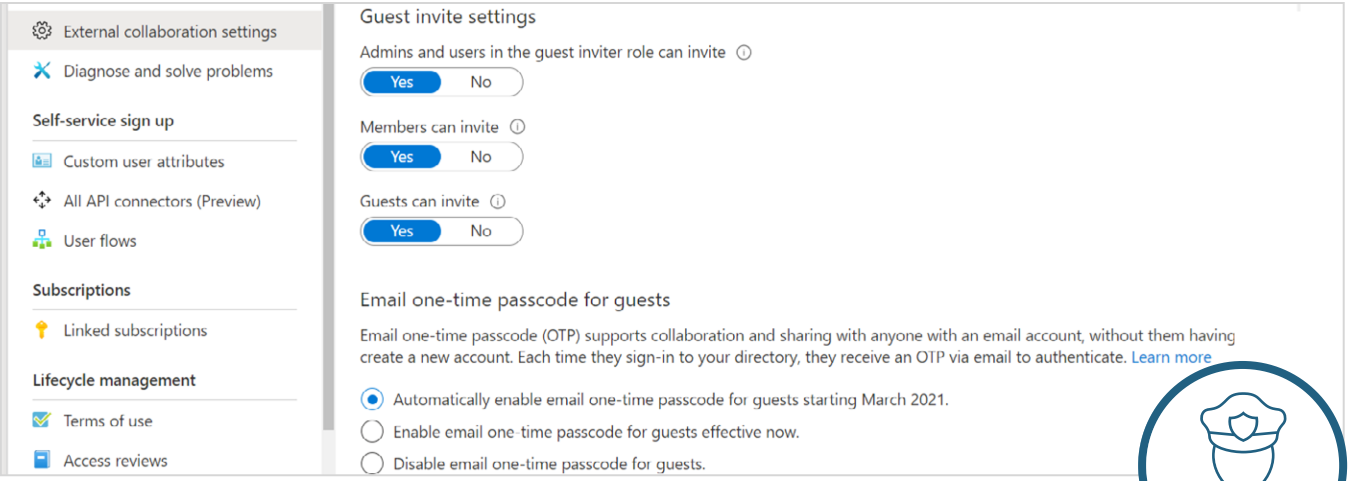
Cambridge Consultants also sought tools to monitor their employee's usage of the application, ensure Teams are compliant and the employee access was valid.

At Cambridge Consultants, all current Microsoft Team's team creation requests go through their IT Department.

The department then separates the teams requests into two different types, Project and Public.

For Public Teams, there is only one configuration. For Project Teams, they are further separated depending on if they are client-facing or internal.

For the different types of Teams, the IT Department will send a corresponding form for the user to fill out for their Team to be provisioned and configured according to the company's governance policy.



Guest invite settings

Admins and users in the guest inviter role can invite ⓘ
[✓ Yes] No

Members can invite ⓘ
[✓ Yes] No

Guests can invite ⓘ
[✓ Yes] No

Email one-time passcode for guests

Email one-time passcode (OTP) supports collaboration and sharing with anyone with an email account, without them having create a new account. Each time they sign-in to your directory, they receive an OTP via email to authenticate. Learn more

● Automatically enable email one-time passcode for guests starting March 2021.
○ Enable email one-time passcode for guests effective now.
○ Disable email one-time passcode for guests.

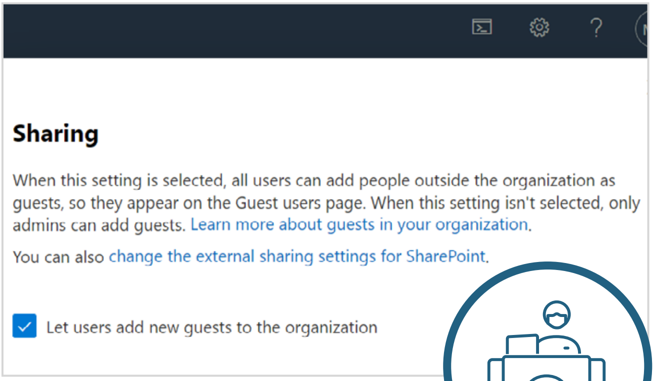
One-Time Passcode: As of March 2021, a one-time passcode option will be available to guests by default. This means if a resource like a document is shared with them and they are not currently in the directory or have a Microsoft account, they will be provided a one-time passcode for identity verification. Using our physical security analogy, organizations with larger buildings or campuses may enforce entry requirements to the entry road, car park or campus perimeter for outsiders arriving by vehicle. A security guard checks that the outsider has valid identification from a trusted authority before lifting the entrance barrier.

Some highly secured sites will only allow certain organizations into the premises while others may just have a list of blacklisted organizations that can never enter. In other words, someone cannot get access to a meeting room if they can't get inside the campus but being allowed inside the campus does not provide them with access to every meeting room.

Microsoft 365 Global Admin Center: The Building

This analogy is also helpful to remember there are several buildings on the Azure AD campus and Microsoft 365 is only one of them. And our receptionist is the Microsoft 365 Global Admin Center "Security and Privacy" tab under "Org Settings."

This step of toggling either to allow or prohibit Microsoft 365 users (actually just Team Owners) to invite guests will seem redundant here but remember: Azure AD serves many masters and each building will have its own protocols.



Sharing

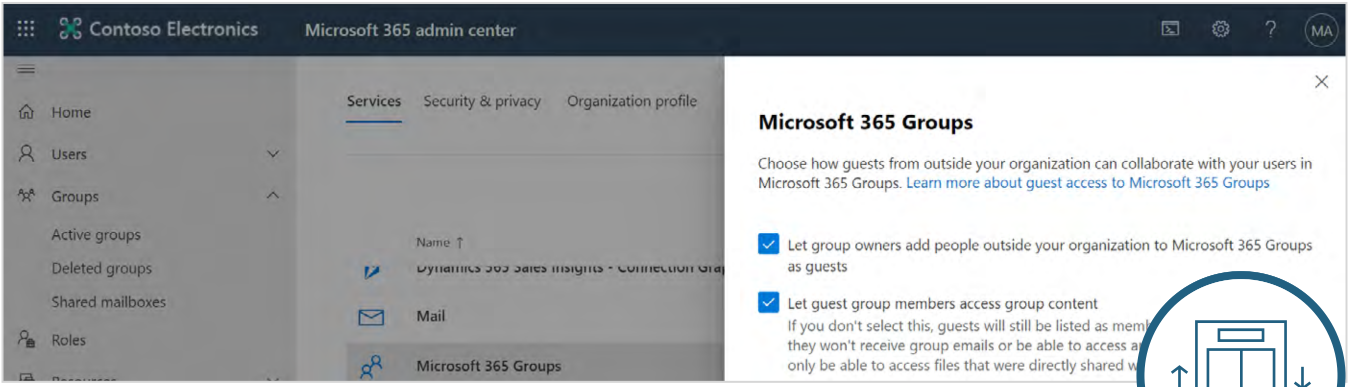
When this setting is selected, all users can add people outside the organization as guests, so they appear on the Guest users page. When this setting isn't selected, only admins can add guests. Learn more about guests in your organization.

You can also change the external sharing settings for SharePoint.

☑ Let users add new guests to the organization

Microsoft 365 Global Admin Center Group Settings: The Floor

Now we're still in the Microsoft 365 Global Admin Center but we will move to the "Services" tab and the global Microsoft 365 Groups settings. Here, we can select once again if Owners can invite guests, this time specifically to Microsoft 365 Groups and if those guests can access Group content once they are a member.



Microsoft 365 Groups

Choose how guests from outside your organization can collaborate with your users in Microsoft 365 Groups. Learn more about guest access to Microsoft 365 Groups

☑ Let group owners add people outside your organization to Microsoft 365 Groups as guests

☑ Let guest group members access group content

If you don't select this, guests will still be listed as mem they won't receive group emails or be able to access a only be able to access files that were directly shared w

There is also a setting to determine if guests can access Group resources — essentially, the files and folders in SharePoint Online. This is a tricky area of setting overlap with settings in the SharePoint Online Admin Center. If you have enabled guests to access Group resources here but have disabled access in SharePoint Online, then guests will get an error trying to access Group files, notebooks and other resources. This is a flood of IT tickets you will want to avoid.

The analogy here is having the elevator give the guest access to a certain floor. Just like you couldn't enable guests to access a floor without letting them in the building, you can't enable Group guest access without enabling global Microsoft 365 guest access.

Microsoft Teams Admin Center and Microsoft 365 Global Admin Center SharePoint Settings: The Meeting Rooms

Once the global settings are established, the subsequent ones deal with increasingly lower-level settings that apply to ever smaller groups of insiders, outsiders and resources (e.g., SharePoint sites, Teams workspaces, etc.).

CASE STUDY

Swinburne University Uses Cloud Governance To Rapidly Extend Microsoft Teams To Students During COVID-19

Swinburne needed a way to set up different policies within Teams for its two distinct user bases: students and staff. Argame also wanted stronger lifecycle management policies than what was provided natively within Microsoft Teams.

“Someone creates a Team and if they left the organization that team and data is sitting there and no one knows what happened,” said Argame. “We started to look at that and wondering at the same time how can we automate the creation of the Team and also have it limited to certain people who can create Teams.”

In addition, Argame was seeking a solution to balance the need for external sharing with prudent security controls.

“Guest access wasn’t available because we didn’t want everyone to create Teams and have guests enabled to invite random people in those Teams,” said Argame.

After an attempt to create a provisioning script in-house, Argame discovered and started to evaluate AvePoint Cloud Governance.

Cloud Governance’s ability to automatically set different policies for different sets of users based off their attributes in Active Directory allowed Argame to quickly roll out Teams for the student body while setting different permissions for staff.

“Students can only be added to a Team by an academic and all provisioning requests from staff are routed to the service desk,” said Argame. “If we didn’t have Cloud Governance, it would have taken a while to roll out Teams to students properly.”

Cloud Governance’s functionality to automate provisioning requests and capture additional metadata around each Team has greatly scaled the service desk as well.

“Before cleaning up the Teams being created and not used took a lot of time. We had to figure out and contact the Owners and then if the Owners aren’t around anymore figure out who is going to be the next one,” said Argame. “Now, I don’t have to worry about any of that.

For Swinburne’s staff users, they have seen tremendous value now that external sharing has been abled thanks to Cloud Governance.

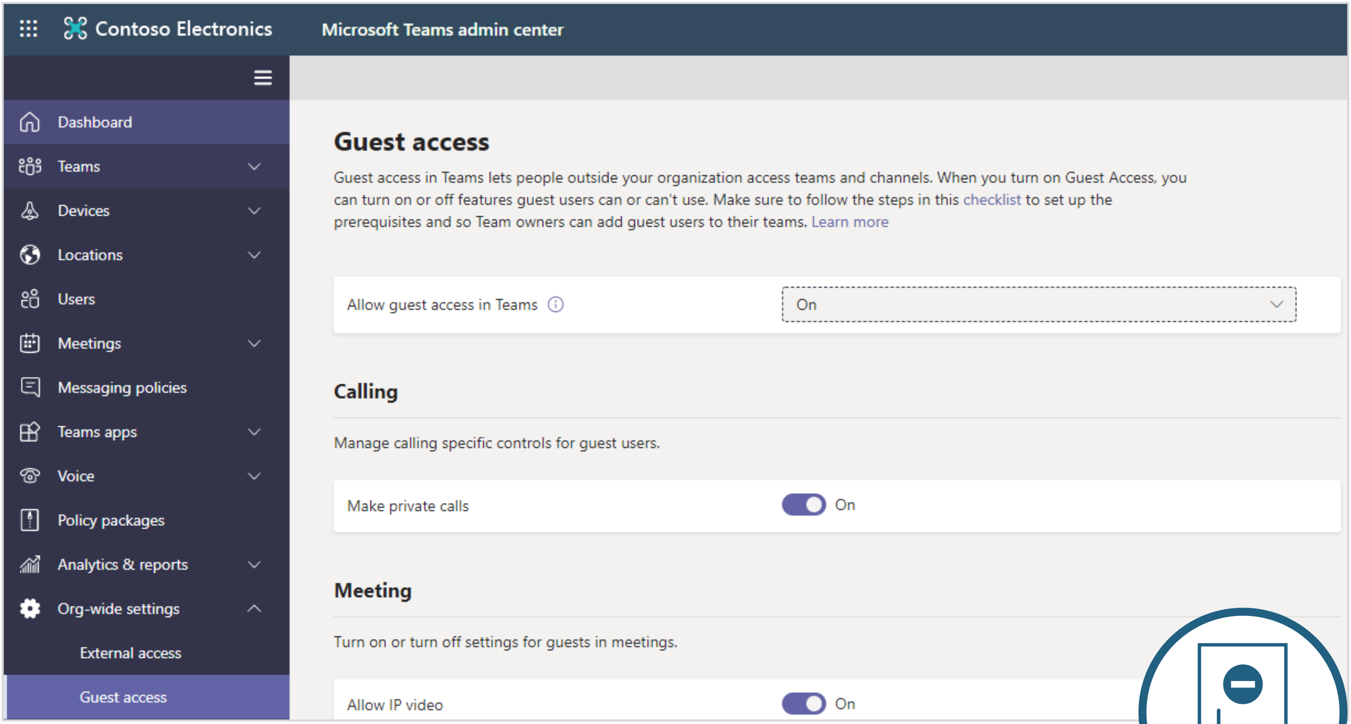
In the **Microsoft Teams Admin Center**, we will skip over the setting labelled “external access,” which deals with federated access via Skype For Business and instead choose “guest access” under “Org settings.”

If access via Microsoft 365 Group settings is access to the floor, this would be access to specific meeting rooms. At this point, guest access in Teams can either be off or on. If guest access is allowed, there are several other settings that control what guests can or can’t do in Microsoft Teams.

If you want guests in some Microsoft Teams, you need to enable them in all Microsoft Teams. If you are using some Teams that are specifically to house sensitive information or discussions, you can lock them down individually using PowerShell. This will prohibit Team Owners from being able to add guests to that specific Team (although admins are still permitted to do so).

As you can imagine, this can get quite cumbersome and difficult to manage at scale. This is one of the challenges solved by AvePoint’s Cloud Governance and a key use case. It dramatically simplifies the process with a central location for managing sharing with outsiders, but that is only a fraction of its value.

Cloud Governance can categorize a Team during the provisioning process by issuing a tailored



Guest access

Guest access in Teams lets people outside your organization access teams and channels. When you turn on Guest Access, you can turn on or off features guest users can or can't use. Make sure to follow the steps in this checklist to set up the prerequisites and so Team owners can add guest users to their teams. Learn more

Allow guest access in Teams: On

Calling

Manage calling specific controls for guest users.

Make private calls: On

Meeting

Turn on or turn off settings for guests in meetings.

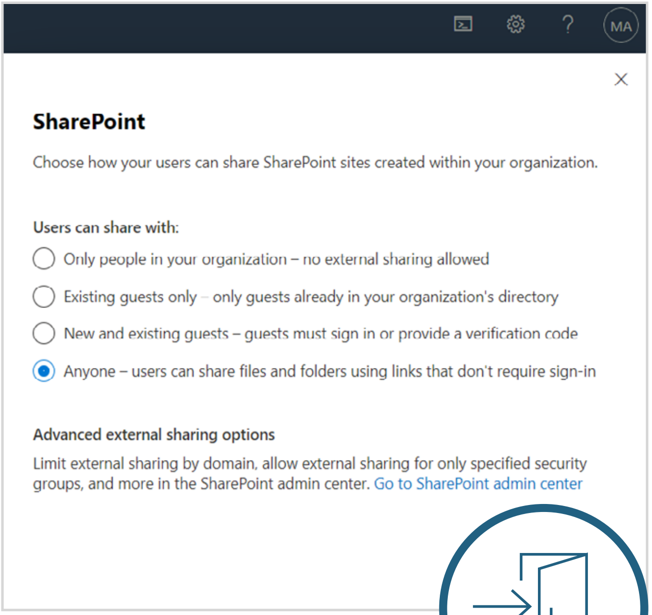
Allow IP video: On

questionnaire to the workspace requestor. Once it is created, the Team now has the ability to add guests based on purpose, sensitivity level, department or many other customizable settings in alignment with your chosen governance policies (and subject to approval if you'd like). Team Owners will be asked to periodically recertify the membership of the Team, and if any guests within them are still appropriate and needed.

These automated processes allow organizations to scale guest access to Teams in a secure way. After all, the answer to, "should guests be allowed in a Team?" is almost never "yes" or "no," but rather "it depends."

Once we move back to **Microsoft Global 365 Admin Center and the SharePoint settings**, our analogy with physical security begins to break down. The ability for guests to access SharePoint sites and content is governed in parallel to the Azure Active Directory and the Microsoft 365 Admin Center Global Group settings we set earlier. (We told you this would be complicated!)

We are going to stretch here to try and save our physical security analogy — this would be



SharePoint

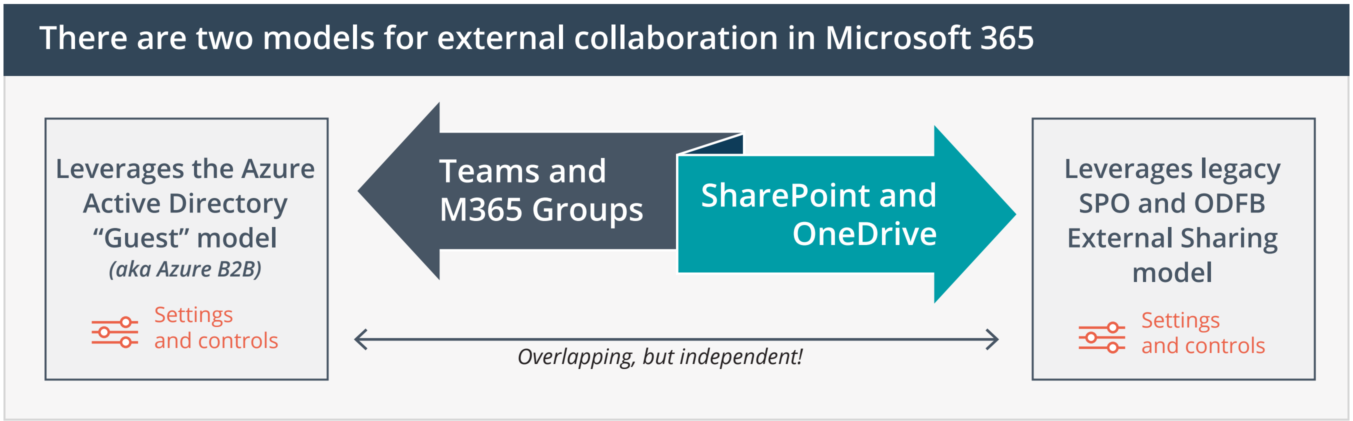
Choose how your users can share SharePoint sites created within your organization.

Users can share with:

○ Only people in your organization – no external sharing allowed
○ Existing guests only – only guests already in your organization's directory
○ New and existing guests – guests must sign in or provide a verification code
● Anyone – users can share files and folders using links that don't require sign-in

Advanced external sharing options

Limit external sharing by domain, allow external sharing for only specified security groups, and more in the SharePoint admin center. Go to SharePoint admin center



There are two models for external collaboration in Microsoft 365

Leverages the Azure Active Directory “Guest” model *(aka Azure B2B)*

Settings and controls

Teams and M365 Groups

SharePoint and OneDrive

Overlapping, but independent!

Leverages legacy SPO and ODFB External Sharing model

Settings and controls

the equivalent of guests going through a separate entrance to the building with its own security protocols, some of which conflict with the main entrance we just talked about. They still have access to the discussion and files, but they didn't have to be cleared by the guard at the gate, the receptionist in the lobby or have the right keycard to access the correct floor or meeting room.

Put another way, depending on the settings you choose, this can be a siloed access path for guests that needs to be managed and governed.

In this space, there are four options for sharing in SharePoint:

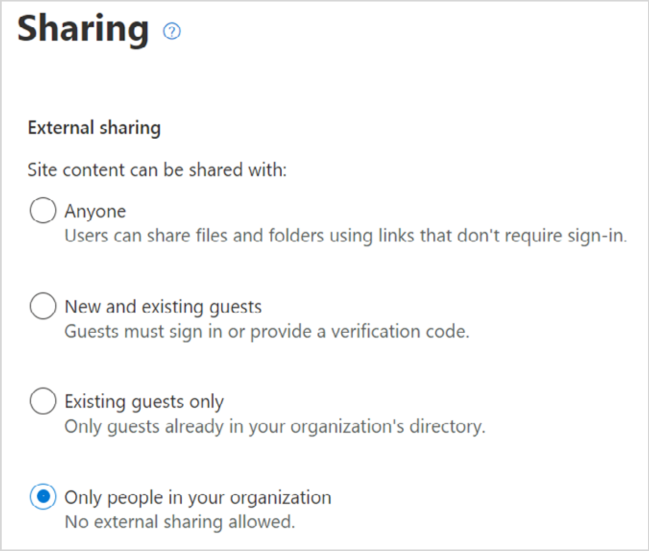
- Only people in your organization, no external sharing allowed
- Existing guests only
- New and existing guests; all must sign in or provide a verification code
- Anyone — users can share files and folders using links that don't require sign in

You can prohibit external sharing in SharePoint but allow it in Microsoft 365 Groups, but that will lead to user frustration as guests get error codes when trying to access SharePoint content.

Our strong recommendation here is to select “Existing guests only.” This setting will force (and again, were stretching our analogy) guests in that offsite meeting room to still be cleared by the guard at the gate, the receptionist, etc.

By contrast, choosing the “new and existing guests” setting opens up a siloed process that will need to be managed, and the “anyone” setting will be too permissive for most organizations.

SharePoint makes it a bit easier to designate specific SharePoint sites that do not allow Owners to invite guests — no Powershell required. To lock down a specific SharePoint site, visit the SharePoint Admin Center > Sites > Active Sites. Select the site you would like to



Sharing

External sharing

Site content can be shared with:

○ Anyone
Users can share files and folders using links that don't require sign-in.

○ New and existing guests
Guests must sign in or provide a verification code.

○ Existing guests only
Only guests already in your organization's directory.

● Only people in your organization
No external sharing allowed.

lock down and select the “Only people in your organization” setting.

Note: Sites can be more restrictive but cannot be less restrictive than your global settings. This is exactly like Microsoft Teams, in which you must open up all the meeting rooms before deciding which to place under lock and key.

Unlike Microsoft Teams, however, SharePoint doesn’t require Powershell to manage the guest settings of each site and each site can have its own allow/deny list.

It also uses a completely different external identity model from Active Directory guests. So external sharing invitations issued from SharePoint Online directly will not create a guest account in the directory. This is good because they won’t be able to access other workspaces but it makes managing guest users difficult as administrators now have to hunt for them site by site.

The level of control SharePoint allows is awesome. However, it is very difficult and time consuming to manage at scale (not to mention prone to human error and oversight).

This is another use case where automating the process via AvePoint’s Cloud Governance can improve the integrity of the guest access process while saving administrators a considerable amount of time.

CASE STUDY

Case Study: City of Port St. Lucie Improves Guest Access Oversight

The City of Port St. Lucie rolled out Microsoft Teams for the first time as part of their quick efforts to support remote work and keep collaboration among city employees running efficiently. However, managing the service threatened to overwhelm the lean IT department.

“Cloud Governance allowed me to scale so I could keep up without having to hire someone,” said Melton. “The provisioning request goes through the questionnaire and I’ll use Cloud Governance’s Teams app, MyHub, to facilitate the request. A process that took me 30 minutes per Team now takes me 5.”

All workspaces that were created prior to implementing AvePoint were able to be imported into the city’s management and governance process moving forward. Cloud Governance also improved how the city managed its guest users and external sharing in Microsoft Teams.

“Guest users are only supposed to be in our tenant for a short time–typically the length of a project,” said Melton. “We saw many guests users sitting in our AD without a reason, so we set up Cloud Governance to automatically sort through and expire them so they aren’t hanging in our AD forever.”

After finding so much success with AvePoint solutions, Melton started leveraging Policies and Insights (PI) as soon as it became available in July 2020. PI provides the ability to monitor risk and access on sensitive documents by proactively monitoring and remediating policy violations. It also provides actionable security dashboards to highlight and track exposure (anonymous links, external user access) over time.

“When we ran a scan with Policies and Insights for the first time, we came up with thousands of document links that were shared incorrectly,” said Melton. “We went through them and hit a button and it basically fixed the links and instantly mitigated that risk.

PI’s simple, three step process (identify, prioritize, prevent) visualizes reports for IT, security, and business units by consolidating disparate reports that contain thousands of unprioritized line items in the Microsoft Compliance and Security Center.

The other important consideration, and potentially the most overlooked factor, when it comes to guest user access is that they remain in Azure Active Directory even if they have been removed from all Teams, SharePoint sites or Groups.

Going back to our analogy, you can have guests permanently hanging out on the floor within your building — already past the gate guard, receptionist and elevator keycard reader — whether they are actively involved in any meetings or not. This creates an increased risk of oversharing, as these "ghost users" may be able to access information or workspaces as an existing guest that they would otherwise not be able to as a net new guest.

Cloud Governance can help by governing external users just like it governs workspaces. When an end user requests to invite a guest, one or multiple guest owners (think of them as chaperones) are assigned who can vouch for the need for the guest to continue to exist or be pruned from the environment. Cloud Governance will periodically check in with these guest owners to recertify the need for this guest, making ongoing guest user management a quick and painless process for admins.

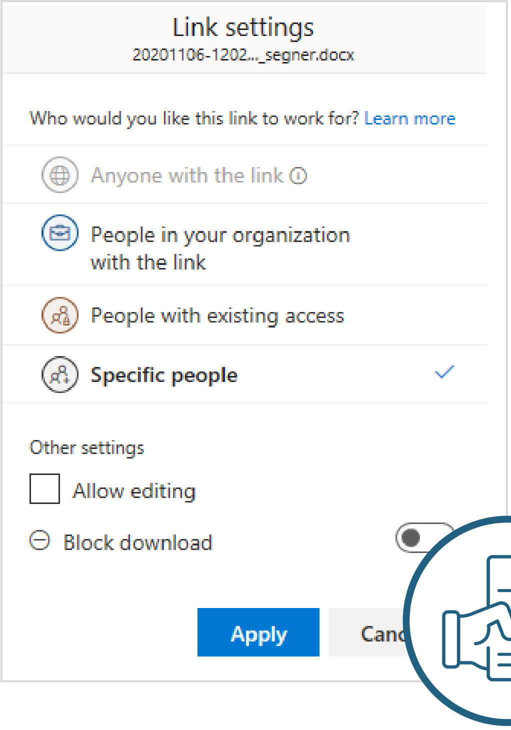
SharePoint Admin Center: The File

Up to this point, we have just covered the process of managing guest access to a Microsoft Team or SharePoint site. In other words, we are managing access to the workspace or meeting room.

However, potentially sensitive information can be shared with outsiders even if they are not a member of a workspace. For example, a user can select the share button within a file and provide that link to anyone via email or chat.

To use our analogy, this would be the equivalent of someone taking an important file out of the file cabinet after the meeting and sharing it with someone outside of our campus.

The good news is Microsoft 365 provides a process for managing this SharePoint and OneDrive external sharing capability in the SharePoint Admin Center.



Link settings
20201106-1202..._segner.docx

Who would you like this link to work for? Learn more

○ Anyone with the link ⓘ

○ People in your organization with the link

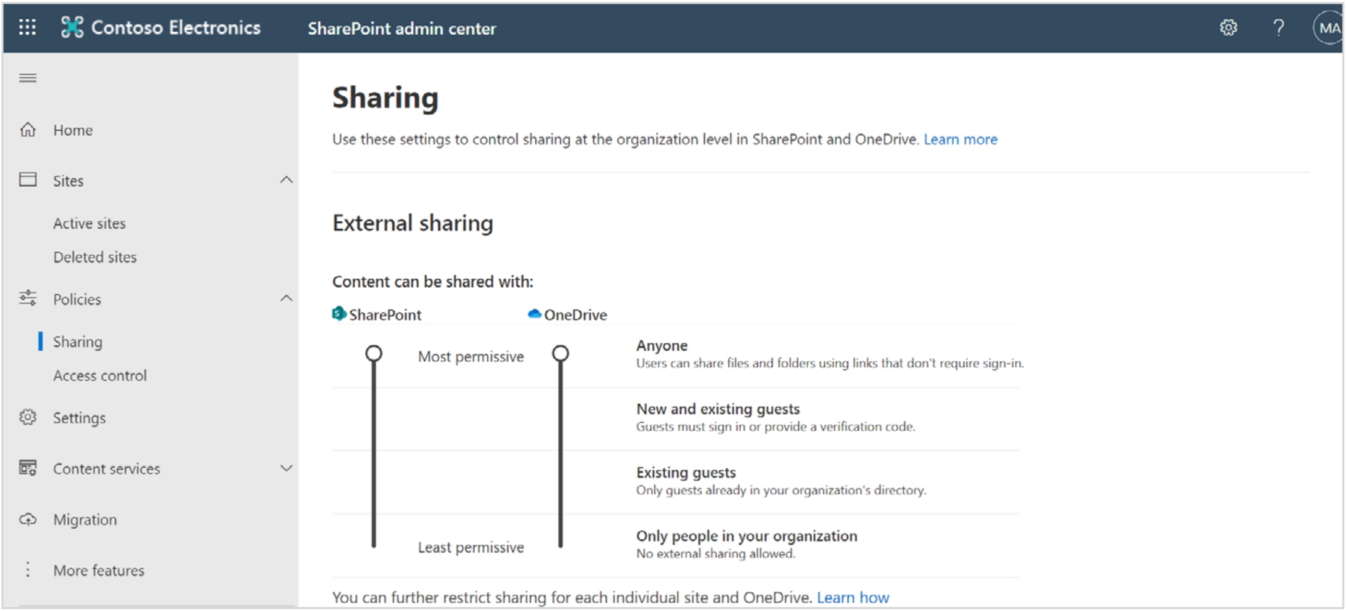
○ People with existing access

● Specific people ✓

Other settings

□ Allow editing

⊖ Block download



Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive. Learn more

External sharing

Content can be shared with:

SharePoint OneDrive

Most permissive

Least permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

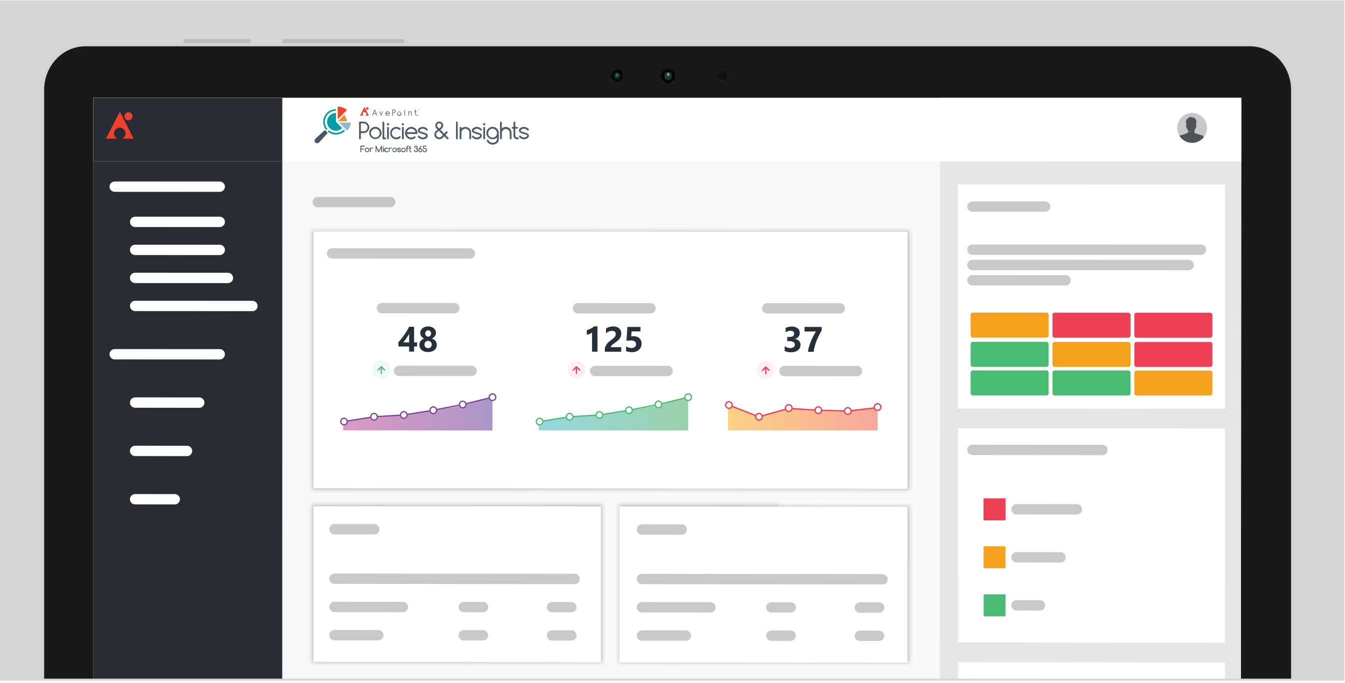
Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. Learn how

If you do nothing else, we recommend you change your settings to prohibit the share with anyone. These anonymous links create a tremendous unmanaged information management risk.

Since each file has their own permissions separate from the workspace, what is the single source of truth for what information outsiders have access to? This is where AvePoint's Policies and Insights can help. The solution identifies, prioritizes and can help mitigate these oversharing situations where sensitive information has been shared with external guests.



6 Levels of Settings for Secure Sharing with Outsiders

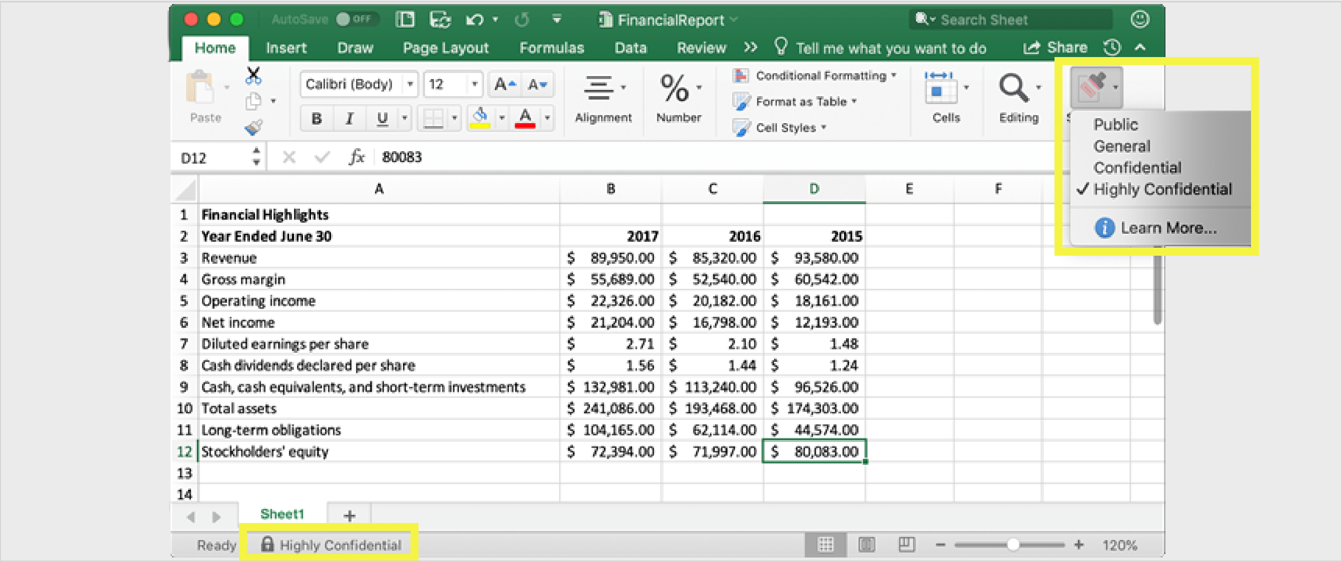
Security Layer	Where	What
"The Campus"	Azure AD Admin Center Azure Active Directory External Collaboration Settings	Three settings: 1. **Guest user access.** What access do guests have within Azure AD to directory entities, (e.g., other people's details)? 2. **Guest invite settings.** Who can invite guests to the directory — admins and users with the Guest Inviter role, directory members who are not admins and don't have the guest inviter role, or other guests? Also covers support for registering guests using an email one-time-passcode, and whether guests can complete self-service sign-up via user flows. 3. **Collaboration restrictions.** Do you wish to limit guest access by domain or not? Includes an open setting (any domain), along with blacklist and whitelist alternatives.
"The Building"	Microsoft 365 Admin Center Settings Org Settings Security & Privacy Sharing	One setting: Can insiders with user privileges in Microsoft 365 (e.g., they are not an administrator), add new guests to the organization? Two options: Yes or No
"The Floor"	Microsoft 365 Admin Center Settings Org Settings Services Microsoft 365 Groups	Two settings, both of which have two options only (Yes or No): 1. Can group owners add outsiders to Microsoft 365 Groups as guests? If set to "no," only administrators can add outsiders as guests. 2. Can guest group members access group content? If set to "no," outsiders can only access the files that were shared directly with them via links. They won't get access to the other resources that make up the different content stores in a Microsoft 365 Group.

Security Layer	Where	What
"The Meeting Room"	Teams Admin Center	**External Access** Controls whether your insiders can interact with outsiders using the voice calling and chat capabilities of Microsoft Teams. This works at the domain level, not the individual user level. Two independent settings enable (or disable): • Communicating with outsiders who use Skype for Business or Microsoft Teams • Communicating with outsiders who use the consumer version of Skype Both settings can be "On" or "Off," and both can be further refined by adding domains to a whitelist (allowing only these domains) or a blacklist (allowing all domains except for the listed ones). **Guest Access** Controls whether outsiders can access the content inside Teams workspaces, such as the channels, discussions and files. If Guest Access is set to "On," there are three subsequent groupings of settings: • Calling controls, with one setting for whether outsiders can make private calls or not. • Meeting controls, with three settings: is IP video allowed in meetings (on or off), what type of screen sharing is permitted by outsiders (disabled, single application only, or their entire screen), and whether Meet Now is allowed (on or off). • Messaging controls, with eight different settings: can guests edit their sent messages, can they delete sent messages, and can they use 1:1 chat in Teams? The final five cover usage rights and restrictions for Giphys, Memes and Stickers, and whether the use of the immersive reading experience is supported or not.

Security Layer	Where	What
"The Separate Entrance"	Microsoft 365 Admin Center Settings Org Settings Services SharePoint	One setting: For all SharePoint sites in the organization, what's the highest permitted sharing level with outsiders? There are four options: 1. Share with anyone without requiring sign-in to access files and folders shared via links. 2. Limit sharing to new and existing guests. They must be in the directory for sharing to happen, but new people can be added. 3. Limit sharing to existing guests in the directory only. Other guests must be added to the directory separately before files and folders can be shared with them. 4. No outsider access at all. Sharing is only for insiders. Note that a particular SharePoint site can have a lower sharing level than the highest permitted one, but no site can have a higher sharing level.
"The File"	SharePoint Admin Center Policies Sharing	**External Sharing** Repeats the sharing level setting for the whole organization for SharePoint, as set in the Microsoft 365 Admin Center (Row 4). Adds the ability to set a different maximum sharing level for OneDrive, but the OneDrive setting cannot be less restrictive than the SharePoint one. Some of the following options disappear when more restrictive sharing settings are selected (if files and folders can't be shared using the "Anyone" option, for instance, the expiration and permission levels for Anyone links is hidden). These advanced sharing options for outsiders are offered: • Whether or not sharing is limited by domain. If yes, limitations can be by blacklist or whitelist, and cover SharePoint content only.

Security Layer	Where	What
“The File” cont.		• Whether to restrict external sharing to insiders in specified security groups. This offers a way of controlling who has the right to initiate sharing with outsiders. • Whether guests must sign in using the same account to which a sharing invitation was sent, or if they can sign in using a different one. Requiring the same account means your directory is cleaner, and not filled with strange user accounts. • Whether guests can share items they don’t own • For people who use a verification code, after how many days must they reauthenticate? **File and Folder Links** Set the default type of link and default permission level for links, along with expiration and permission levels if Anyone links are selected. For default link type, there are three options: 1. Specific people only, as per the sharing settings set by the user 2. Only people in your organization, thereby prohibiting access by outsiders to the link 3. Anyone with the link For default permission link, there are two options: • View only • Edit (and by implication, view as well) If Anyone links are permitted, what are the expiration and permission levels that are supported for such links? **Other Settings** Three (minor) settings about the details of sharing and its implications are experienced in OneDrive and SharePoint.

Microsoft 365 includes six groups of settings for controlling the nature and degree of sharing with outsiders. High-level controls over guest accounts in Azure AD B2B and the Microsoft 365 Admin Center paint the broad picture of how sharing can or can't happen, and then workload-specific sharing settings for SharePoint and Teams address more specific options. Owners of Teams workspaces and SharePoint sites can enable more restrictions for their specific sites, but they cannot circumvent or loosen the global settings.



	A	B	C	D
1	**Financial Highlights**			
2	**Year Ended June 30**	**2017**	**2016**	**2015**
3	Revenue	$ 89,950.00	$ 85,320.00	$ 93,580.00
4	Gross margin	$ 55,689.00	$ 52,540.00	$ 60,542.00
5	Operating income	$ 22,326.00	$ 20,182.00	$ 18,161.00
6	Net income	$ 21,204.00	$ 16,798.00	$ 12,193.00
7	Diluted earnings per share	$ 2.71	$ 2.10	$ 1.48
8	Cash dividends declared per share	$ 1.56	$ 1.44	$ 1.24
9	Cash, cash equivalents, and short-term investments	$ 132,981.00	$ 113,240.00	$ 96,526.00
10	Total assets	$ 241,086.00	$ 193,468.00	$ 174,303.00
11	Long-term obligations	$ 104,165.00	$ 62,114.00	$ 44,574.00
12	Stockholders' equity	$ 72,394.00	$ 71,997.00	$ 80,083.00
13				
14				

Deploying Sensitivity Labels to Workspaces and Documents

Microsoft 365 has recently deployed a mechanism for applying sensitivity labels to workspaces and documents that can impact external sharing and guest access settings.

While this is a different path, it leads to many of the same challenges (separated permissions, workspace lifecycle management, enforcement, guest user lifecycle management, etc.) and it requires upgraded licenses at an additional cost of $6 user a month (P1) or $9 user a month (P2).

For these reasons, we advise organizations to either examine the native-only approach we outlined above or deploying a third-party tool such as Cloud Governance.

For this approach to be used for guest access and external sharing, Microsoft Information Protection settings must be pre-configured correctly. Sensitivity labels can be ordered from low to high sensitivity with associated policies that include if guest access and external sharing are enabled or prohibited. Different sensitivity labels can be available for several types of workspace requestors based on their Active Directory attributes; users can apply these labels when they provision the workspace. Separately, users can also manually label their documents or auto-labelling can be deployed with an upgraded E5 license.

Still, there are challenges to this approach:

- Users are not provided with any context on what label is appropriate for what workspace or document. There is no information provided during the provisioning process on what policy actions a label will enforce.
- Configuration drift is a serious issue. A workspace can have a label with settings applied on provisioning but there is nothing stopping a Team Owner from changing settings immediately afterward or any mechanism that will notify the business or admins that a change has been made.
- There is still no automated way of effectively offboarding guests, nor is there a source of truth for which guests have access to what data.
- When a document with a higher sensitivity label is placed in a Team with a lower sensitivity label, there is no enforcement action taken. An email is sent to the offending user to ask them to revert their action.

Configuring Your Guest Access Policy: Possible Scenarios

As we have explored above, there are many controls to explore when configuring Microsoft 365 to support secure access from outsiders. And each organization has its own requirements for outsider access. This section will outline some of the major decision points across four general-purpose scenarios for how an organization can set this up with standard licensing.

Remember the policy cheat sheet? You can map your answers back to these scenarios which will help you determine your settings.

For the tailored control scenario below, we have chosen simple configuration with four different workspace templates.

Sensitive Internal

The Sensitive Internal workspace would likely be used by departments within the organization that routinely handle sensitive information, such as the finance department.

Sensitive External

The Sensitive External workspace would likely be used in limited scenarios and heavily monitored. For example, the legal department might have a project that required some external collaboration on sensitive files with external counsel — a limited number of regular external collaborators that have been signed to an NDA.

Non-Sensitive External

The Non-Sensitive External workspace could be used for departments that do not regularly handle sensitive information (such as marketing) but have vendors like public relations agencies that serve as external collaborators. Rather than limit guests, this template restricts sensitive information.

Non-Sensitive Internal

The Non-Sensitive Internal workspace could serve as the de facto or most used workspace for everyday work and collaboration within the organization.

Four Scenarios for Sharing with Outsiders

Open Scenario	For organizations that don’t deal with sensitive or regulated content and speed of collaboration is key.
Significant Control	For organizations dealing with very sensitive content on a regular basis. External sharing only happens with guests and very few guests are admitted and only by admins.
Some Control	For organizations trying to balance the need for external sharing and information security.
Tailored Control	For organizations where a “one size fits all” tenantwide approach isn’t ideal Different types of workspace templates can be created with tailored controls and provisioned automatically based on information provided by the user. For example: • Sensitive Internal • Sensitive External • Non-Sensitive External • Non-Sensitive Internal Note: Third party solutions are also being deployed to prevent sensitive data from being uploaded to non-sensitive workspaces.

	Open Scenario	**Significant Control**	**Some Control**	**Tailored Control**
Considerations	Data loss, accidental security breach	Shadow IT; Email attachments; impedes adoption	Very time intensive for IT; error prone	Balances security and access. Requires third-party solutions like Cloud Governance. Return on investment from saved IT resources.
Who can invite guests?	Admin and Owners	Admin only	Admin and Owners	***Sensitive Internal***- No one ***Sensitive External***- Administrators only ***Non-Sensitive External***- Admin and Owners/ process owners ***Non-Sensitive Internal***- No one

	Open Scenario	Significant Control	Some Control	Tailored Control
Guest approval required?	No	Yes, manual process	Yes, request sent to IT for approval	***Sensitive Internal***- N/A ***Sensitive External***-Yes, multi-tiered approvals possible ***Non-Sensitive External***-Yes, automated ***Non-Sensitive Internal***-N/A
How is Guest off-boarding handled?	Typically loosely monitored. AD becomes cluttered quickly with lingering guests	Admins manually check with all original guest requestor on a monthly basis.	Typically loosely monitored. AD becomes cluttered quickly with lingering guests	Automated recertifications are sent to appropriate organization contacts to determine if guests need to be removed from Active Directory.
Domains (Organizations) Allowed to Be Guests	All except	None except	All except	***Sensitive Internal***- None ***Sensitive External***-None except ***Non-Sensitive External***-Any except ***Non-Sensitive Internal***-None
External Sharing in SharePoint and OneDrive	New and existing guests	Manually monitored and approved on site-by-site basis	Existing guests only	***Sensitive Internal***- No ***Sensitive External***-Existing guests only ***Non-Sensitive External***-New and existing guests ***Non-Sensitive Internal***-No

Another way to tailor your external sharing and other governance controls could be by department or business unit. For example, legal could have more restrictive settings than marketing.

Tailoring Control Across Departments

Department A	Department B	Department C
No external sharing	External Sharing In: 👥 T S	External Sharing In: S
Expires After: 6 Months	Expires After: 12 Months	Expires After: 9 Months
Team Creation: Central IT	Team Creation: Dept IT	Team Creation: Users
Member Recertification: 3 Months	Member Recertification: 6 Months	Member Recertification: 12 Months

Conclusion

We hope you have found this a useful, applicable resource. The key points worth reiterating are:

Strategy Best Practices

- Unless you have email disabled, your users are sharing externally. Use the tools Microsoft has provided to make the process of sharing information with outsiders more controlled and secure.
- Sharing with outsiders requires working through a labyrinth of settings and admin centers. It is best to start by determining your governance policies. Otherwise, it's easy to get lost.
- Creating a very open or very restricted environment for sharing with outsiders is relatively straightforward. Most organizations are going to fall somewhere in the middle where some areas need to be a bit more open and others a bit more restricted. For example, the Marketing department is likely to prefer the first scenario of fairly open sharing. The Research department, on the other hand, would prefer the middle scenario, while Legal and Finance would be better served by the high restrictions scenario. Each will have external communication use cases that will straddle the non-sensitive and sensitive spectrum. Managing those needs at scale is exceedingly difficult and solving the challenge should be the crux of your strategy.

Don't Forget!

- Microsoft 365 works by enabling all Teams or Sites to guests and then locking down select workspaces. It does not work by locking down all workspaces and opening up a select few.
- SharePoint has its own permission structure outside of Azure Active Directory.
- Guests that are no longer members of any Teams, Sites or Groups are still living in the Directory unless proactively removed by an admin.
- Access to sensitive documents can be provided via Team, Site or Group membership OR by a sharing link from the document itself.

Configuration Best Practices

- Prohibit anonymous, share with “anyone” links in SharePoint and OneDrive. This is a massive risk and it’s not worth taking.
- If possible, restrict your SharePoint settings to enable Owners to invite only “existing guests” in Active directory to prevent having to manage multiple siloed processes.

Mitigated These by AvePoint Solutions

- While there is a workflow for onboarding guests there is no corresponding workflow for off-boarding them or recertifying they are still needed within the environment.
- There is no process for business owners to approve guest requests.
- There is no easily accessible source of truth for which guests have access to what data, and associated sensitivity levels.
- The only way to allow some Team Owners to invite guests and to prohibit others with standard licensing, is with Powershell. SharePoint is a no-code but manual, time intensive process. Sensitivity labels have challenges that must be mitigated as well.

As we have seen with other digital collaboration tools and the introduction of one-time passcodes, Microsoft has communicated it is actively working to make it easier for end users to collaborate externally.

Microsoft 365 is ever-changing. The settings in this e-book will change and toggles will shift, but we can anticipate that these changes will be in the direction of making external sharing easier.

As a result, it is critical for organizations to give immediate and serious consideration to their external sharing policies. We would also recommend you consider solutions that will help you adjust without having to make compromises between your security policies and user experience. The last thing you will want to do is to build an intricate script, or internal processes that fall apart as this experience evolves.

Resources

Blog

- 25 Popular Microsoft 365 Guest Access Questions Answered
- Microsoft Teams Q&A: How to Secure External Sharing & Guest Users
- 3 Major Questions to Ask Before Enabling External Sharing in Office 365

Webinars

- Solving The M365 Guest User Puzzle
- Protecting Sensitive Data in Office 365 at the Team and Data Levels
- AvePoint's Newest Solution Protects Your O365 Data

E-books

- Tailoring Teams
- Value of Automated Governance in Office 365
- Mitigating Collaboration Risk Workbook

Product Pages

- Cloud Governance
- Policies and Insights

AvePoint®

525 Washington Blvd, Ste 1400 | Jersey City, NJ 07310
P: +1.201.793.1111 | E: sales@avepoint.com | www.avepoint.com