Securing External Collaboration in Office 365

Corey Buzzell and Paul Edlund
Microsoft
Communicating like a giant network
Microsoft 365

A complete, intelligent, secure solution to empower employees

Unlock creativity  Built for teamwork  Integrated for simplicity  Intelligent security
Microsoft Teams Can Feel Like This

Why do I need so many accounts?

I want to work anytime & anywhere

Make it easier to collaborate

Let me use the tools I want

Lawyers

How do I secure this?

Is it too late? (aka taking candy from children)

How do I know when changes happen?

Can I delegate this?

Lawyers

IT Security

IT Security
Fact: Teams have diverse needs

Challenges for Users
Multiple logins and difficulty sharing and discovering information

Challenges for IT
Shadow IT leads to security and compliance risk and limits agility

Challenges for Business
Incomplete toolkit leads to disengaged employees and costly, duplicative tools
Our Approach:

- **Seamless Experiences**
  Connected experiences enable sharing and discovery across applications

- **Simplify IT**
  Centralized management with intelligent, built-in security and compliance

- **Maximize Productivity**
  Complete toolkit drives employee engagement and enables rationalization
Ideal Workflow: https://aka.ms/sharingexternally

- Determine your security posture for external access
- Discover your current state
- Create a governance plan
- Use groups for security
- Transition to Azure AD B2B
- Secure access with Entitlement Management
- Secure access with Conditional Access policies
- Secure access with Sensitivity labels
- Secure access to Microsoft Teams, OneDrive, and SharePoint
Demo

Setting up:
1) Azure AD External Collaboration Settings
2) Identity Governance
Best Practices: No anonymous links

External sharing

Content can be shared with:
- SharePoint
- OneDrive

Most permissive
Users can share files and folders using links that don’t require sign-in.

Anyone
New and existing guests
Guests must sign in or provide a verification code.
Existing guests
Only guests already in your organization’s directory.

Least permissive
Only people in your organization
No external sharing allowed.

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

More external sharing settings
- Limit external sharing by domain
- Allow only users in specific security groups to share externally

Manage security groups

- Guests must sign in using the same account to which sharing invitations are sent
- Allow guests to share items they don’t own
- People who use a verification code must reauthenticate after this many days [30]
Best Practices: Use (M365) Group-based collaboration

- Teams and/or Group-connected SharePoint sites
- One place to manage access to multiple services
- Governance: self-service, expiration, membership reviews, etc.
Best Practices: Teams/Groups are different from Client Matters

- Think about the scenarios you want to enable with Teams
- Client Matters?
- Team/Group : Client Matter = NO
- Non-matters?
- Team per client?
- Expiration
- Extract content to DMS?

https://docs.microsoft.com/en-us/microsoftteams/limits-specifications-teams
Best Practices: Reduce accidental external sharing

- Team/Group naming to clearly denote where we have external guests
- Separate Teams >> Private Channels (Corey’s opinion)
Best Practices: Self-service Team/Group provisioning

- If you have automation in middleware/orchestrator, create Teams with that as part of Matter creation.
- If you don’t already have/need automation, allow for self-service and use Sensitivity Labels to control settings of the Team/Group. We recorded an ILTA webcast you can watch again on this subject. https://aka.ms/ProtectingClientMatter
- If you don’t have/need automation, but want more control, create a custom provisioning UI that enables extra governance/metadata AND automatically provisions Teams: https://aka.ms/RequestATeam
Best Practices: Teams Connect / Shared Channels (coming soon)

- Eliminates the need for external partner to switch tenants
- More seamless collaboration
- External Identity >> Guest
- Maintains security & compliance capabilities

Questions?