Governance Decisions.

The definitive guide to your Microsoft Teams governance

BRAINSTORM

**The Seven
Governance Decisions**

So, you're trying to decide what to turn off and on in Teams? Smart move. But how do you decide what your users can and can't control?

Remember that by default, *Teams has some built-in limitations* that can't be changed. That said, here are 7 key decisions you should make as a Teams admin.

1

Naming Conventions

Make your life easier and set up an _Office 365 group naming policy_. Use a prefix-suffix naming policy and/or blocked words list.
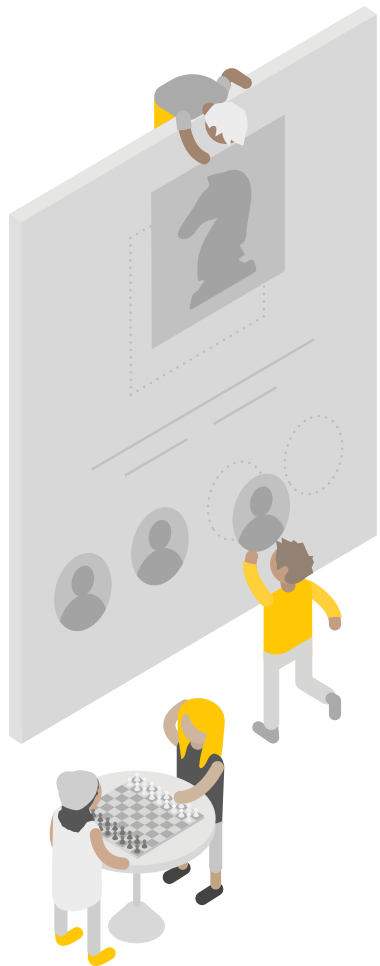
You can also _create Office 365 Group classifications_ using Azure AD PowerShell. Users will see options to classify their team when they create it (i.e. Internal, Partner, Client, etc.)

For users, naming happens automatically. Let's say you had a naming policy that looked something like this: "GRP [Group Name] [Department]"

Kelly from Marketing wants to create a social media team. She inputs the group name and the Team is created with the name "GRP Social Media Marketing."
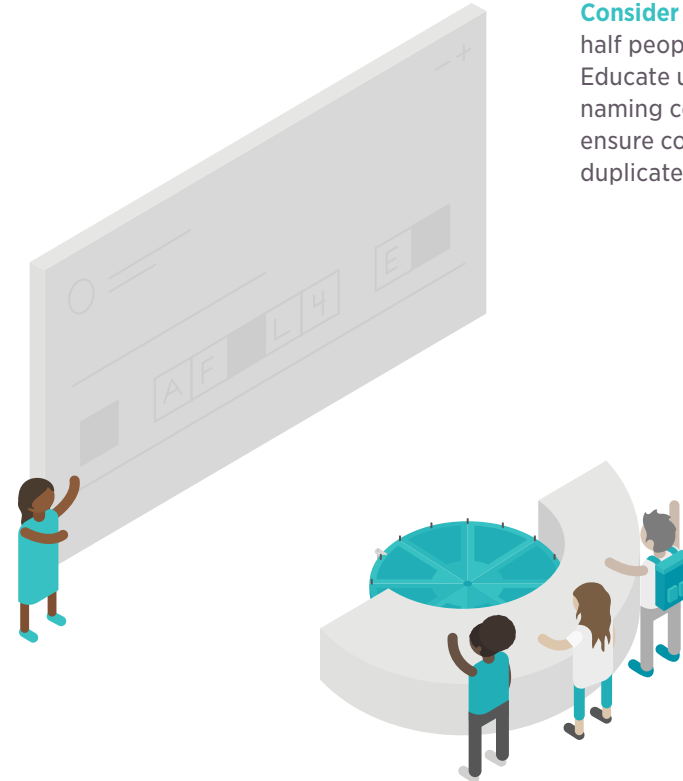
Consider this: Governance is half people, half technology. Educate users on your naming conventions to ensure correct titles without duplicate wording.

2

Team Creators

You might expect over-excited users to receive access to Teams and immediately start creating groups.

We get it: The sudden influx of users is scary, so most admins turn the Team Creation feature off. Just remember; you'll encourage better Microsoft Teams adoption by keeping the feature on… with some limitations.

Create a certification course that teaches your user best practices. Then, enable *security groups* that will automatically give access to qualified users. (Here's a *step-by-step walkthrough*.)

Consider this: Make it easy for your users to adopt Teams. Give users autonomy after they've learned best practices.

3

Expirations

Unused groups can pile up fast. Don't panic, there's a setting for that. Just manage the life cycle of Office 365 groups by *setting an expiration for any Office 365 groups* that you select.
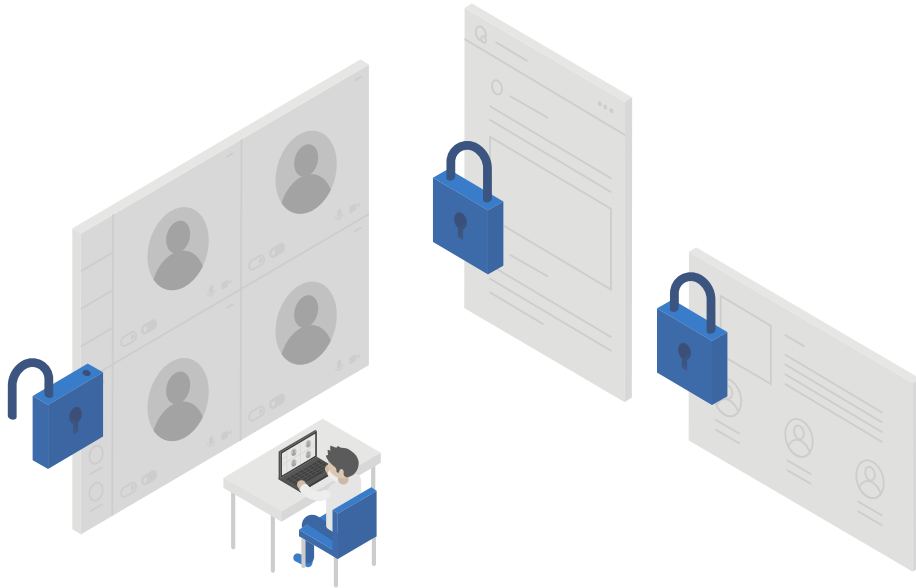
Here's how it works: owners of expired groups will be asked to renew their group. Any Office 365 group that is not renewed will be deleted. But don't worry; any deleted Office 365 group can be restored within 30 days by the group owners or the administrator.

When groups expire is up to you. You can set up a time-based expiration policy, or you can set up an *activity-based expiration policy*.
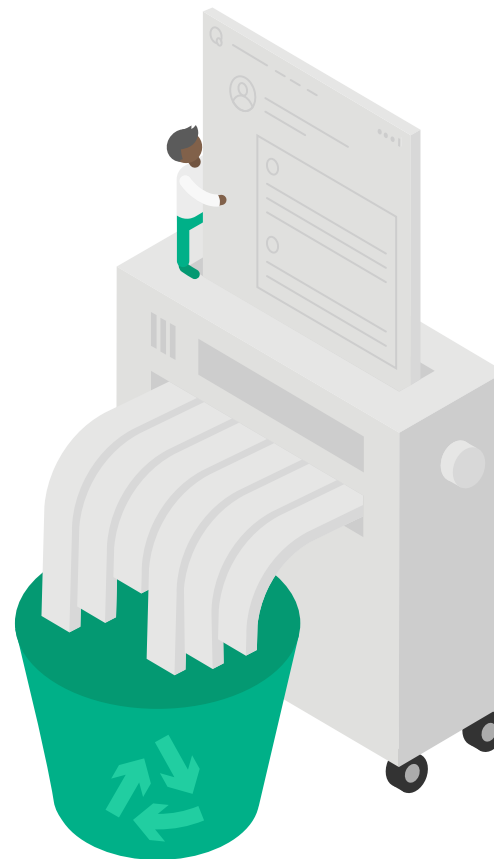
Consider this: There may be security compliance restrictions at your organization. Piggyback off those policies when setting expirations.

4

Guest Access

How does Teams let you communicate with people outside of your organization? Guest access. Yes, this setting has the biggest potential security leak, since any and all guests will have access to the files and chats posted in a team. Here's how to reduce risk while still allowing guest access.

Train your users.
They should know when a guest is present in their team, and what type of content is confidential.

Create a private channel
within a team. Don't include guests in the private channel member list.

Limit guest privileges.

Allow guest access
in Teams meetings, but not in Teams groups.

Consider this: Be patient with yourself in this process. Meanwhile, to find what works best for your organization, make sure you _understand these four areas of authorization_.

5

Policies

Keep these three policies in mind (or you might end up in an uncomfortable conversation with the company lawyer):

Retention
Teams conversations are persistent and retained forever by default. That cat gif you sent to your boss? Retained forever. For chat and channel messages, you can *configure Teams retention policies*.

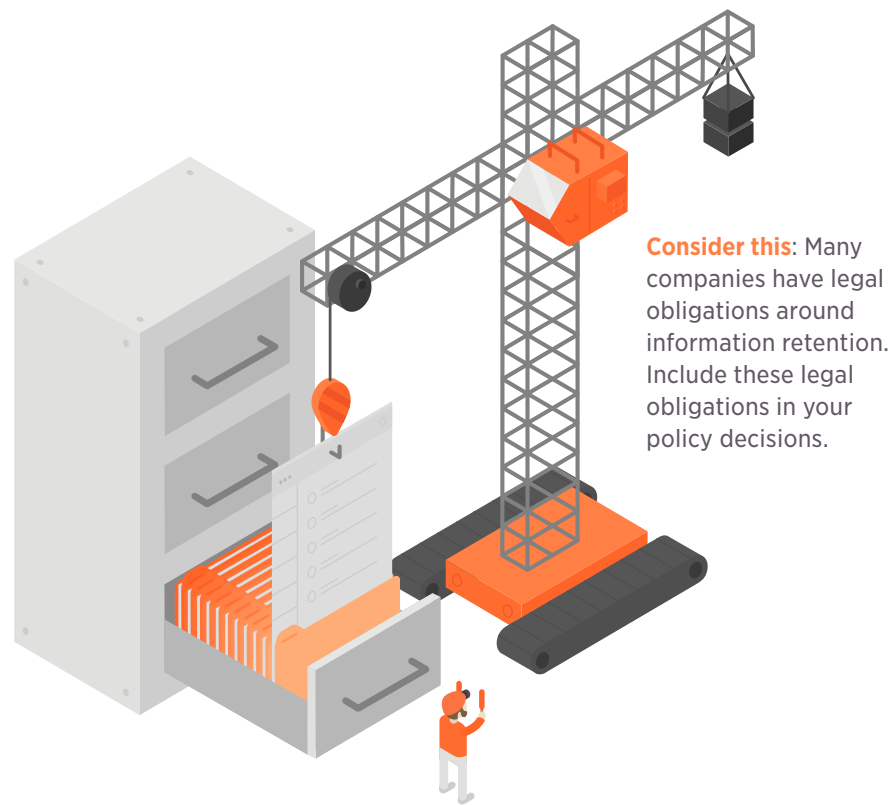Use OneDrive and SharePoint retention policies for the files stored in Teams.

eDiscovery
Avoid the scorching stare of the Legal team. Be aware of the *process of conducting an eDiscovery investigation in Teams*.

Archival
Teams can be archived as a 'soft delete.' These teams will be in a temporary storage – a sort of limbo – before a 'hard delete' occurs.

Consider this: Many companies have legal obligations around information retention. Include these legal obligations in your policy decisions.

6

Templates

Tired of doing the same set-up for each team? Templates to the rescue. It's easy to re-define properties for team creation with *Teams Templates*. Control the team name, description, public/private visibility, general team settings like @ mentions and guest access, and more.

When determining if you should use templates, ask yourself:

1. Does my organization need the same repeated resources for every team?

2. Are there groups within my organization that create teams frequently?

3. Will templates save time for my users?

Consider this: Conduct group discovery and monitoring before you create a template. This will increase the efficacy of your templates.

7

Monitoring

Monitoring shows you how users are adopting and interacting with Teams. Take advantage of usage reports to help you prioritize training and communication efforts.

Case in point: you can access Teams usage reports in the *Office 365 Admin portal*, or through the *QuickHelp Admin Portal*.

Consider this: Monitoring provides powerful insights into user behavior. Capitalize on these insights to change user behavior with technology and education.

Take it to the Next Level

Think of Teams Governance like a kite string. Your users' productivity is the kite.

So—by extension—if you give users too much slack, they'll fly out of control and crash. Give too little, and your users won't reach the heights they need to. Teams Governance is a delicate balance that's meant to help you achieve your business outcomes.

BRAINSTORM

Get your users to adopt Teams and turn your software investment into the best decision you've ever made.

Schedule a demo to get started.

Change is everything.