

MANAGING MICROSOFT TEAMS

Pat Petersen, MCT

Pat.Petersen@rsmus.com

@prpetersen



Please thank our sponsors



Who is this presenter | Let's ask Copilot



Copilot

Pat Petersen is a **Director at RSM US LLP**, a leading provider of audit, tax, and consulting services¹. He has over 20 years of experience in information technology and specializes in helping clients maximize their adoption of Microsoft 365 tools and technologies, including Teams, SharePoint, OneDrive, and Office applications².

Pat also contributes to organizing Microsoft Teams chat and channels into sections, providing valuable insights and strategies for effective use of these tools³.

Is there something specific you would like to know about his work or expertise?



1



Pat Petersen's Speaker Pro...

2



RSM's Microsoft Innovatio...

3



Security | Technologies | R...

Show more

Who is this presenter



- Minneapolis, Minnesota, USA
- MVP – M365 and Teams
- MCT – Since 2011
- Collab & Voice focused
- Own 1975 AMC Pacer



NOW ON TO THE GOOD STUFF

Agenda

- Basic Governance
 - Naming policies
 - Blocked words
 - Restricting who can create Microsoft 365 Groups
 - Usage guidelines
 - Microsoft 365 Group expiration
 - Microsoft Teams templates
- Policies
 - Teams
 - Meeting
 - Live Events
 - Messaging
 - App permission
 - App Setup
- Usage Analytics
 - Admin center
 - Productivity Score
- Voice
 - Audio Conferencing
 - Configuration Overview

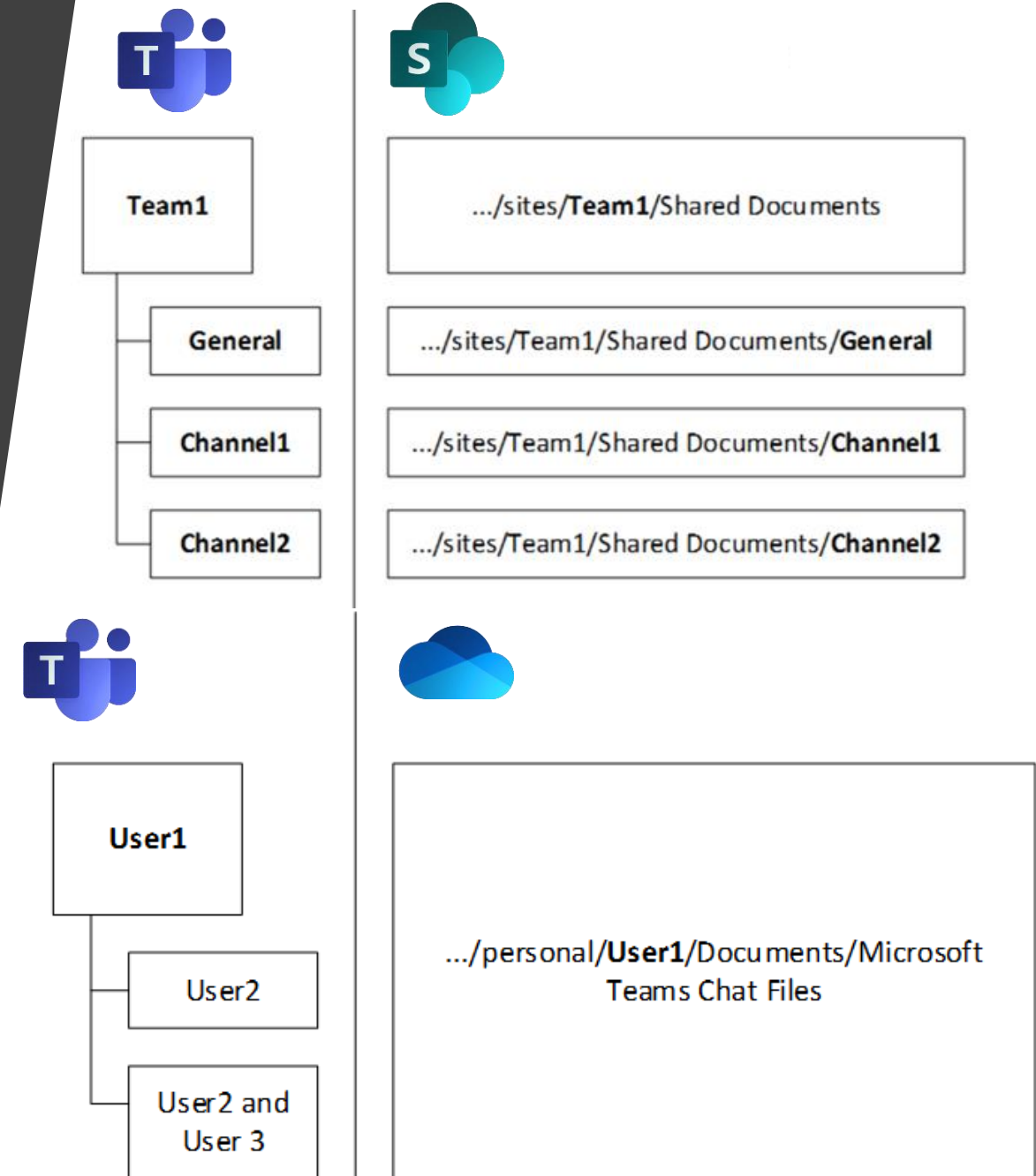
Description

- Microsoft Teams is a robust platform with many services. In this session we will focus on how an organization can manage Microsoft Teams. We will focus on roles, settings, policies, access, policy packages and using PowerShell. If you have already deployed Microsoft Teams, we will review the analytics and reports that are available as well including Voice.

USING MICROSOFT TEAMS

File Structure

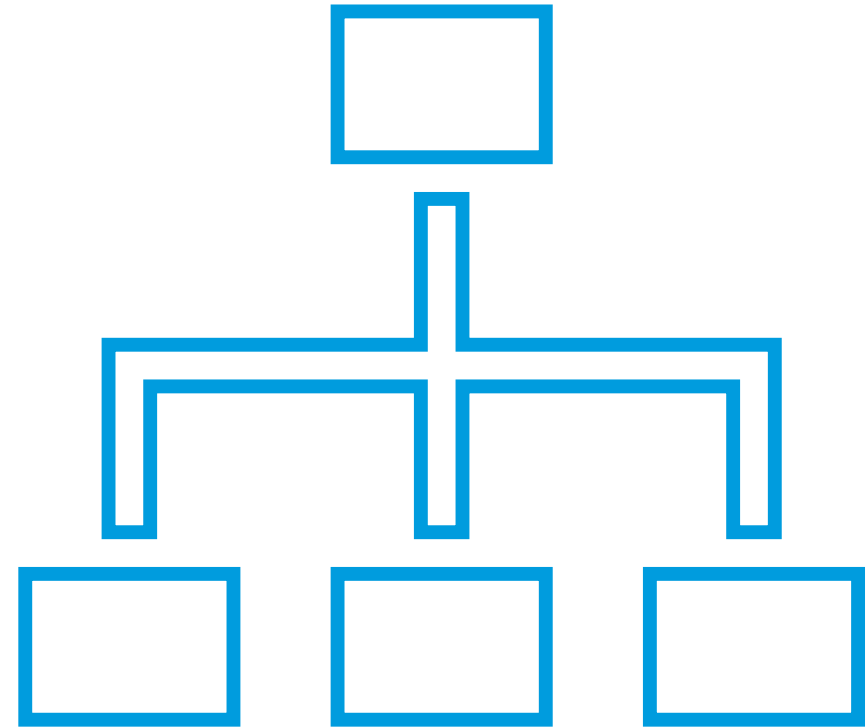
- Files in Teams/Channels
 - Modern Team site is created as part of creating Office 365 group
 - Document library has a folder for each channel
 - By default, all channels/folders inherit the permissions of the underlying O365 Group
You can change them in SharePoint and Teams will respect them
- Files in 1:1 or Group Chat
 - Files are in a folder in the sender's OneDrive called "Microsoft Teams Chat Files"
 - Each file has unique permissions of the people in the chat



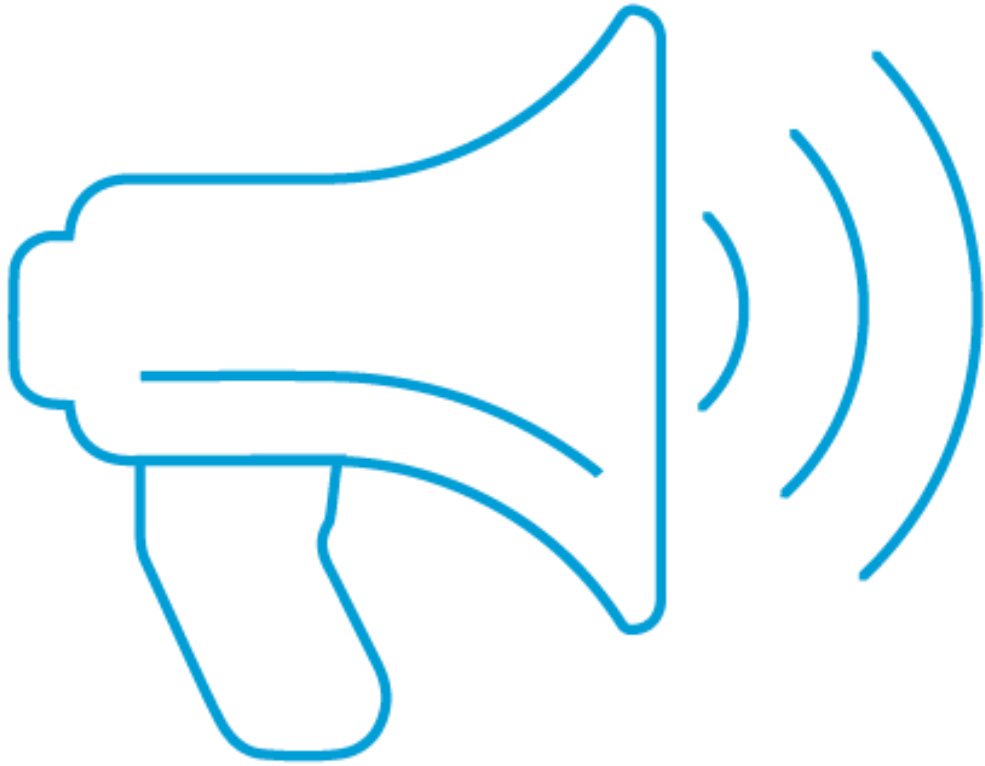
BASIC GOVERNANCE

Microsoft Teams and Microsoft 365 Groups

- Most settings in this module will be applied at the Microsoft 365 Group level
- Remember the architecture
 - Each team is part of a group
 - All group settings also impact the team



Special Notes...



- Azure AD Premium licenses are required for most features
- Always check licensing

Naming Policies

- Naming policies have been available before in distribution lists
- Benefits
 - Consistency in your tenant
 - Quickly identify the purpose of the group
 - Naming policies can depend on the information in the User Profile
Country, Department, etc!

Example Naming Policy

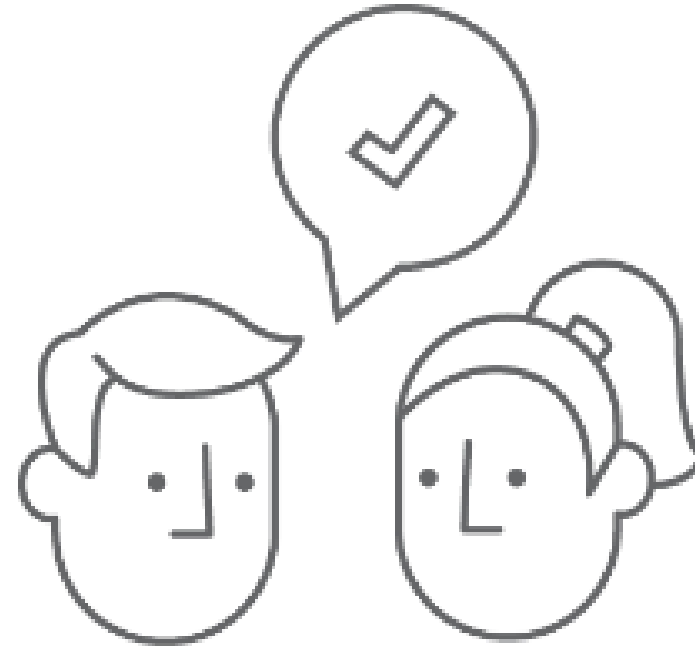
- Team [Department] [TeamName] [OfficeLocation]
- Team Marketing Project Oakdale US

Configuration Basics

- Naming Policies are done in the following format
 - Prefix(es)
 - Group name as entered by user
 - Suffix(es)
 - Both prefix and suffix are optional
 - Total length must be under 53 characters

Naming Policies Do Not Apply to Everyone

- Some administrative roles are exempted from those policies
 - Global admin
 - Partner Tier 1 Support
 - Partner Tier 2 Support
 - User account admin
 - Directory writers



Configuration

- Configuration done via the Azure Active Directory admin portal
 - <https://portal.azure.com/>
 - Azure AD > Groups > Naming Policies

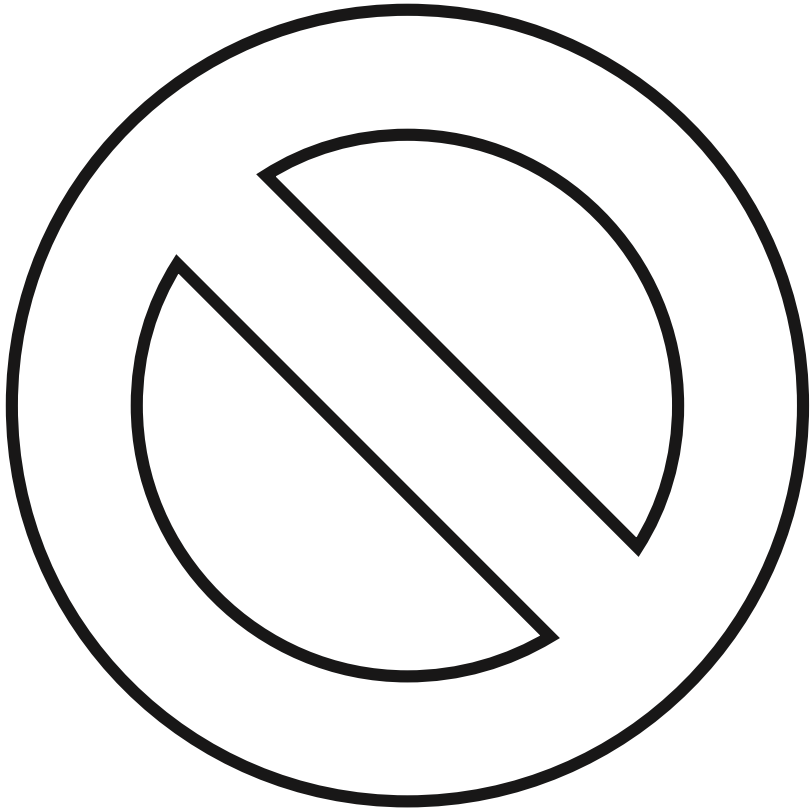
Azure Active Directory Attributes

- Supported:
 - [Department]
 - [Company]
 - [Office]
 - [StateOrProvince]
 - [CountryOrRegion]
- Extension attributes and custom attributes aren't supported
- See latest list of supported attributes
 - <https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/groups-naming-policy>

Microsoft 365 Groups Blocked Words

- Users can use any words inside the Microsoft 365 Groups they create Human Resources, IT, etc..
- Every Microsoft 365 Group creates a Mailbox that shows up in the GAL
- Users could send sensitive information to HumanResources@xyzcompany.com by thinking it's an official group

Before We Start Configuring



- Identify your list of blocked words
 - Microsoft provides an option to block common inappropriate words
 - Focus on Business / Privacy related words
 - Sub-string searches are not carried out
 - Class isn't blocked even if "ass" is a blocked word

Blocked Words Do Not Apply to Everyone

- Some Administrative roles are exempted from those policies
 - Global admin
 - Partner Tier 1 Support
 - Partner Tier 2 Support
 - User account admin
 - Directory writers

Configuration | Azure Portal

- Azure AD > Groups > Naming Policies
 - Upload a CSV file containing blocked words
 - 5,000 maximum

Blocked words

Group naming policy

Enable custom blocked words list

You can upload a list of words you wish to block to prevent Office 365 groups being given profane or reserved names and aliases. You may download the .csv file to view and/or edit the existing list of blocked words.

To view and/or edit blocked words list:

1. Download .csv file of blocked words

[Download](#)

2. Add or remove terms (5,000 word maximum)

3. Upload your .csv file

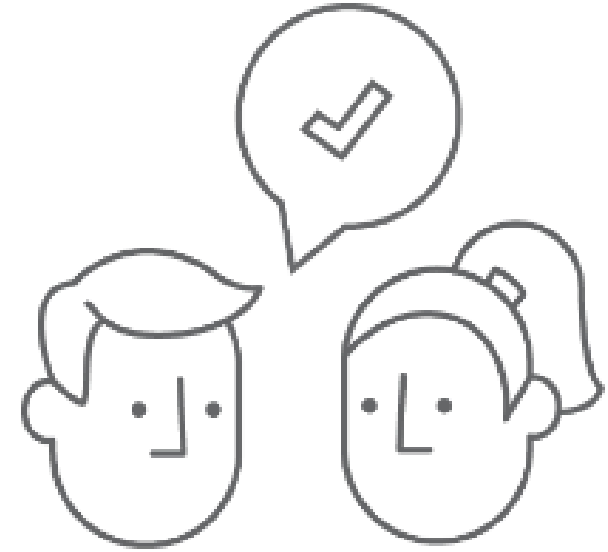
Select a file



**LET'S TAKE A LOOK AT GROUP NAMING
SETTINGS**

Restricting Group Creation

- What creates a Microsoft 365 Group?
- Modern Team Site
- Planner Plan
- Stream Group
- Microsoft Team
- You can set your tenant, to only allow a certain group of people to create Groups



LET'S TAKE A LOOK AT GROUP RESTRICTIONS

Configuration | PowerShell Only

- `$Setting = Get-AzureADDirectorySetting | `where-object {$_.displayname -eq 'Group.Unified'}`
- `$Setting["EnableGroupCreation"] = "False"`
`$Group = Get-AzureADGroup -SearchString "Office 365 Group Creators"`
- `$Setting["GroupCreationAllowedGroupId"] = $Group.ObjectId`
`Set-AzureADDirectorySetting -Id $Setting.id ``
`-DirectorySetting $Setting`

Microsoft 365 Groups Usage

- Internal Guidelines
 - Teach users what they can/cannot do with Microsoft 365 Groups
 - Reduces number of support tickets, and clean up in the future
- Guest Guidelines
 - Link to guest guidelines included as part of e-mail sent when an external user is invited to a Microsoft 365 Group
 - You can include information such as Privacy Policies, Confidentiality, and more!

Create Discard

Create a group

A group provides a space for shared conversations, files, a group calendar, and more.

Group name

Description

Tell people the purpose of your group.

Privacy

Public - Anyone in your organization can see what's

Classification ⓘ

Confidential

Language for group-related notifications

English (United States)

☐ Send all group conversations and events to members' inboxes. They can stop following this group later if they want to.

[Group usage guidelines](#)

Before...

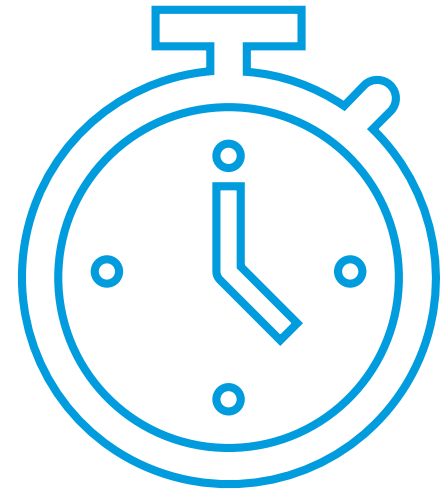
- Internal guidelines
 - URL to your internal guidelines
 - You could host it as a SharePoint page
- Guest guidelines
 - URL to your external guidelines
 - Make sure it's accessible externally

Configuration | PowerShell Only

- `$Setting = Get-AzureADDirectorySetting | `where-object {$_.displayname -eq 'Group.Unified'}`
- `$Setting["UsageGuidelinesUrl"]="https://rsmdemo.sharepoint.com/SitePages/Microsoft365GroupsPolicies.aspx"`
- `$Setting["GuestUsageGuidelinesUrl"]="https://rsmus.com/guestpolicy"`
- `Set-AzureADDirectorySetting -Id $Setting.id ` -DirectorySetting $Setting`

Microsoft 365 Group Expiration

- Automatically delete unused Microsoft 365 Groups
- Ensures you do not keep unused groups inside your tenant
- You can set after how many days a Group should expire
 - Active groups are automatically renewed
- Owners of the group are notified to renew the group before expiration
- Any group that is not renewed is deleted
- Deleted groups can be restored within 30 days



Expiration



- Only one expiration policy per tenant
- Policy can apply to
 - All Groups
 - Selected Groups

Configuration Options

- From the Azure AD Admin Portal
 - Azure AD > Groups > Expiration
Configure: Group lifetime; Backup e-mail; contact; All/Selected groups
- With PowerShell
 - Dedicated cmdlets for the Microsoft 365 Group Expiration
 - New-AzureADMSGroupLifecyclePolicy
 - Get-AzureADMSGroupLifecyclePolicy
 - Set-AzureADMSGroupLifecyclePolicy
 - New-AzureADMSGroupLifecyclePolicy `
 - GroupLifetimeInDays 99
 - ManagedGroupTypes "All"
 - AlternateNotificationEmails "help@rsmus.com"

**LET'S TAKE A LOOK AT GROUP EXPIRATION
SETTINGS**

TEAMS TEMPLATES

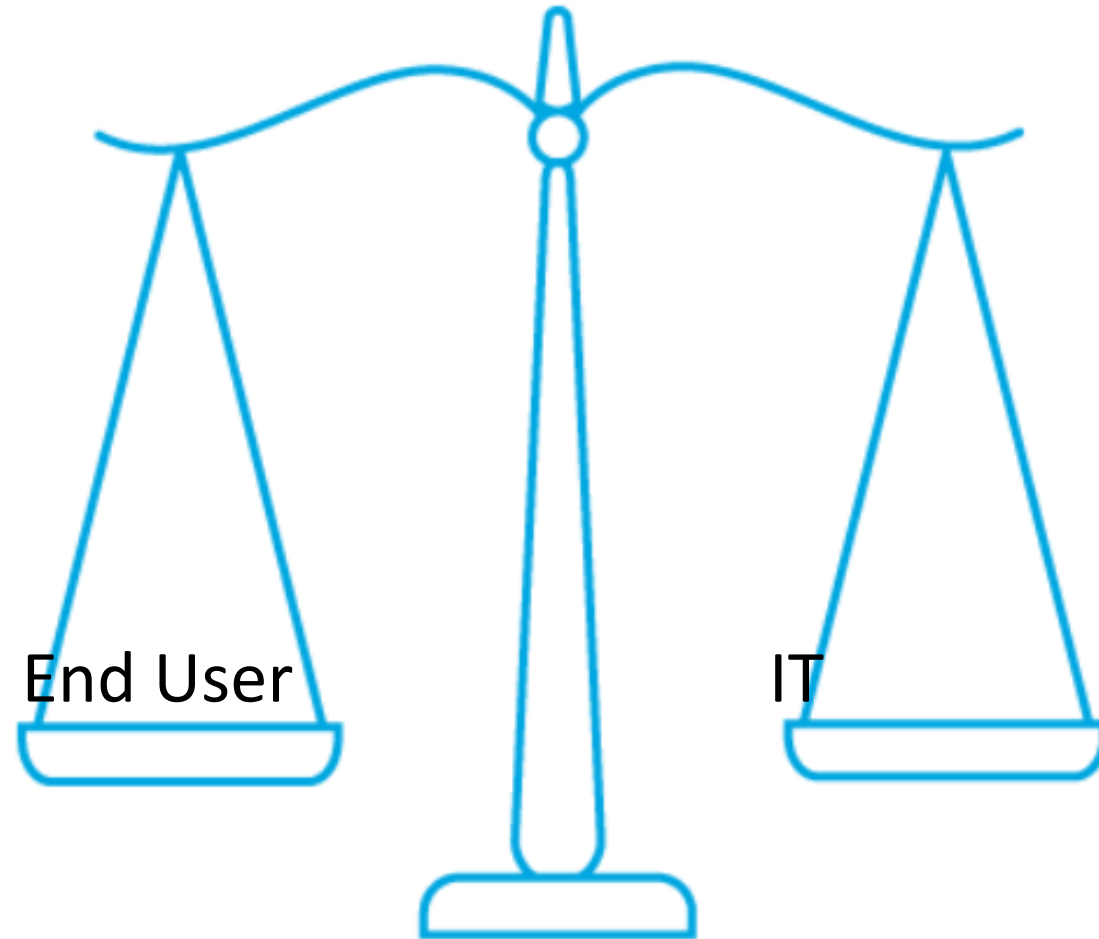
What can users do?

- Users can create a team from an existing team
- Create a team from a Template

Templating with PnP PowerShell

- You can also create SharePoint / Teams templates with PnP PowerShell
 - Open-Source initiative on GitHub
 - Not officially supported by Microsoft
 - Heavily backed by Microsoft <https://github.com/pnp/PnP-PowerShell>
 - Not a turnkey solution
 - You need to manually create
 - End-user form
 - Approvals
 - Automation
 - etc

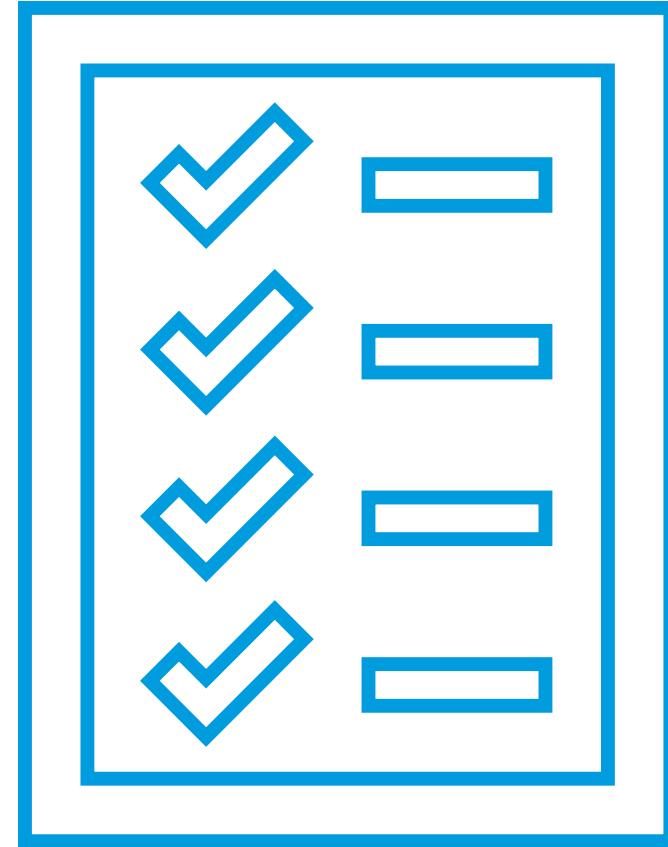
You Need to Achieve Balance



TEAMS POLICIES

Teams Policies

- Policies
 - Teams
 - Meeting
 - Live Events
 - Messaging
 - App permission
 - App Setup

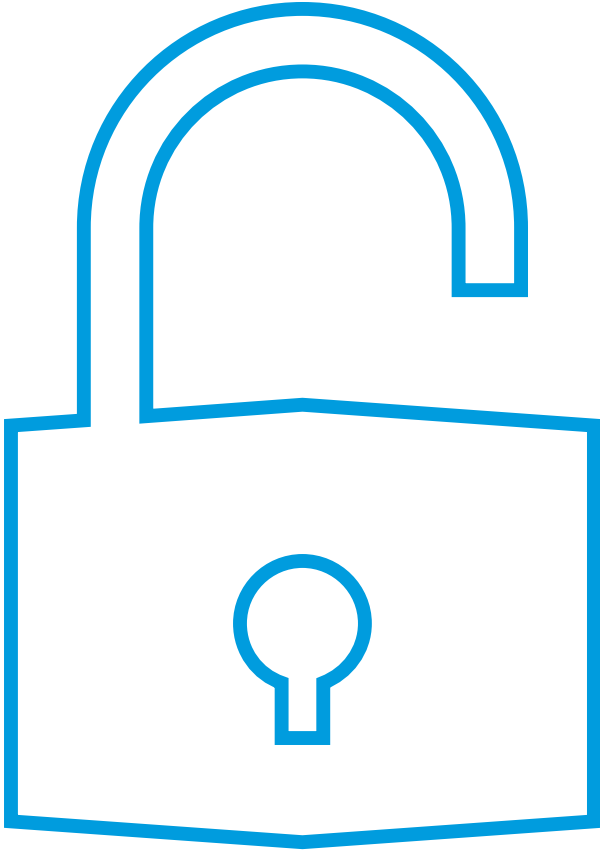


Policies Offer Flexibility

- Multiple ways of assigning policies
 - Per department
 - Per country
 - Per role
- Policies offer a flexible strategy
 - HR and Marketing can have different live events policies, but same messaging policy



How Policies Are Applied



- Default Org-wide policy for all users
- You can edit default policy
- You can create multiple custom policies
 - More permissive OR more restrictive than default
 - You can apply custom policies on a per user basis

Creating Policies

- User Interface
 - Teams Admin Center
- PowerShell
 - Skype for Business Online PowerShell cmdlets
 - Some policies can only be created via PowerShell while some are UI only

Teams Policies | Private Channels

- Create private channels in teams they are a member of, and Team owner enabled the permission

New teams policy

Name

Description

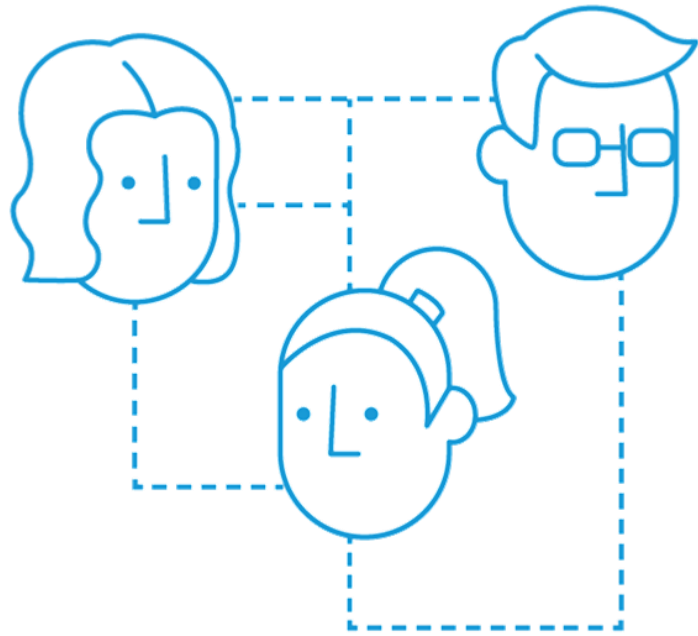
Create private channels ⓘ

☒ On

Meeting Policies & Settings

- Meeting policies
 - Control different features around meetings
 - Audio & video
 - Content Sharing
 - You can apply different policies to different profiles
- Meeting settings
 - Apply to all meetings scheduled in the tenant
 - Participants
 - E-mail invitations customization
 - Network settings

Three Ways Policies Apply to Users



- Configurations in meeting policies apply differently depending on the user role
 - Organizer / Participant
 - All meeting participants inherit the policy of the organizer
 - Per-Organizer policies
 - Per-User policies
 - Only apply to the specific user the setting is configured for Combination of per-organizer and per-user

Combination Of Per-Organizer & Per-User Policies

User	Allow Cloud Recording	Allow IP Video
Pat Petersen	True	True
Ben Anderson	False	False
Hassan Moses	True	False

- If Pat organizes a meeting, Pat and Hassan can record the meeting but not Ben
- If Ben organizes a meeting, no one can record the meeting
- If Hassan organizes a meeting, no one can share their video
- If Pat organizes a meeting, Only Pat can share their video

Meeting Policy Settings - Audio & Video

- Media bit rate (Kbs)
 - Per user policy
 - Minimum: 30 Kbps
 - Highest quality: 10 Mbps
 - Teams will adjust to low bandwidth
- Teams bandwidth requirements -
<https://docs.microsoft.com/enUS/microsoftteams/preparenetwork#bandwidth-requirements>



Meeting Policy Settings - Content Sharing

- Combination of per-organizer and per-user policy
- Screen sharing mode
 - Entire screen
 - Single application
 - Disabled

Video Filters / Background

- Controls whether users can customize their video background in a meeting
 - Per-user Policy
 - PowerShell Only
 - NoFilters : User can't customize their background
 - BlurOnly : User can blur their video background.
 - BlurandDefaultBackgrounds : User can blur their video background or choose from Microsoft provided background images
 - **AllFilters** : User can blur their video background, choose from Microsoft provided background images, or upload custom images to use as their background.

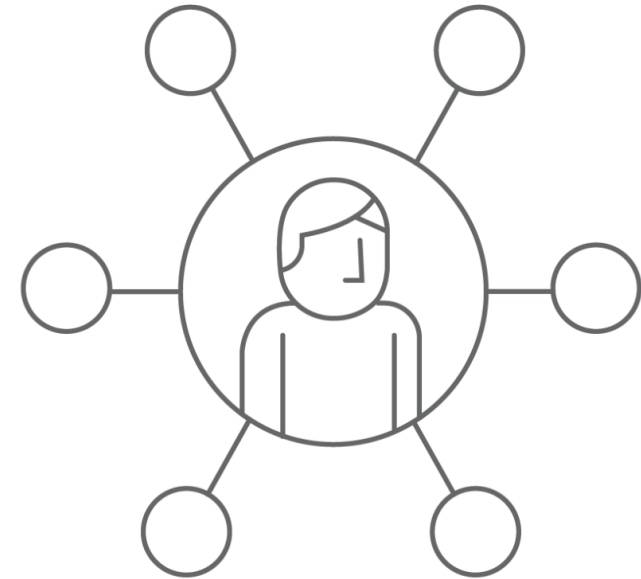
Meeting Settings

- Participants
 - Can anonymous users join a meeting
 - Email invitations
 - Logo / Legal / Help URLs
 - Footer text
 - Network
 - QoS markers
 - Port configurations



Live Events Policies & Settings

- Allow scheduling
- Allow transcription for attendees
- Who can join scheduled live events
 - Everyone
 - Everyone in the organization
 - Specific users or groups
- Live Event recording
 - Always record
 - Never record
 - Organizer can record



Messaging Policy Settings - General

- Owners can delete sent messages
- Users can delete sent messages
- Users can edit sent messages
- Read receipts
 - User Controlled
 - On for everyone
 - Off for everyone
- Users can chat

Messaging Policy Settings – “Fun” Settings

- Use Giphys in conversations
- Giphy content rating
 - No restriction
 - Moderate
 - Strict
- Use memes in conversations
- Use stickers in conversations

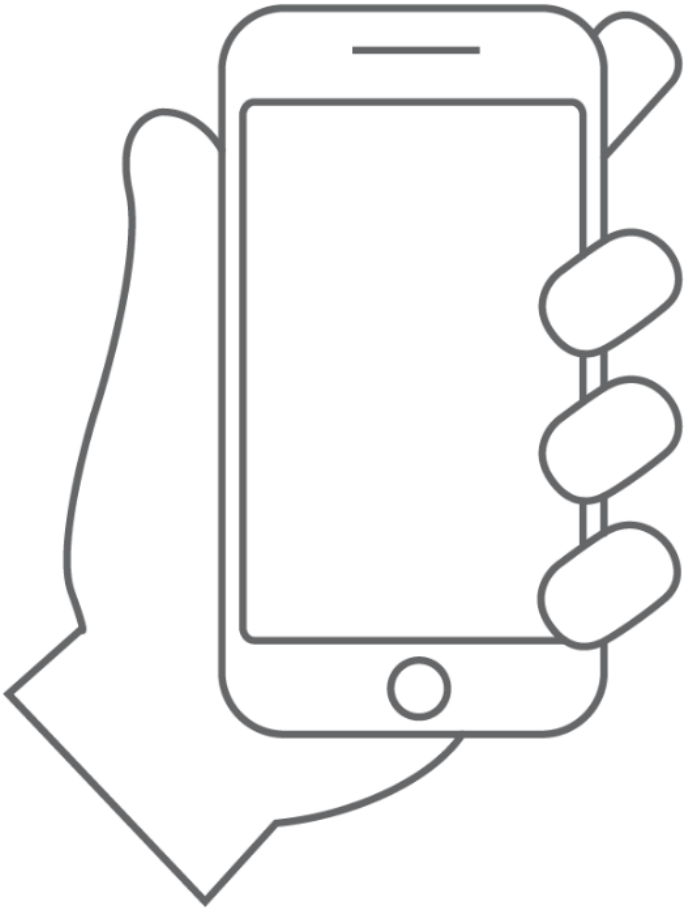
Messaging Policy Settings - Features

- Allow URL previews
- Allow users to translate messages
- Allow immersive reader for viewing messages

Messaging Policy Settings - Audio Messages

- Three possible options
 - Allowed in chats and channels
 - Allowed in chats only
 - Disable
- Audio messages are not captured in eDiscovery reporting

Messaging Policy Settings - Other



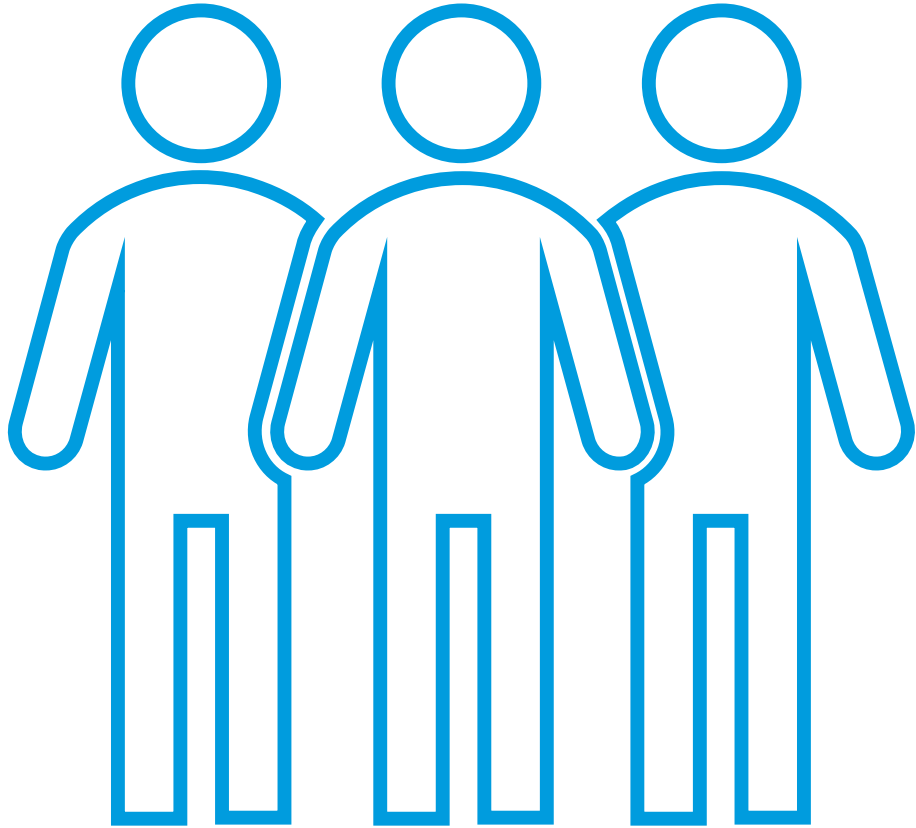
- On mobile devices, display favorite channels above recent chats
- Allow a user to remove users from a group chat
- Enable suggested replies

Assigning Policies to Users

- We can grant policies at different levels
 - User
 - Batch of Users
 - Group
- Two ways of granting policies to users
- Teams Admin Center
- PowerShell

Assigning Policies In The Admin Center

- Manually add a user to a policy
- Assign to a group



Submit session feedback

