



The A-Z of Governance for Microsoft Teams

By Jasper Oosterveld MVP

Contents

Three-step model	3
Welcome to Microsoft Teams	4
Chat.....	4
Meet.....	4
Call.....	5
Collaboration.....	5
Automate	5
Business value	6
Customer worries.....	7
Teams explosion	7
Duplication	7
Purpose unclear.....	7
Findability	7
Complexity	7
Data leak	8
The importance of a governance strategy.....	9
Connecting IT & Business	9
Contribute to a successful adoption	9
Integration of procedures, law & regulations	9
Manage Microsoft 365 Groups	10
Step 1: Workshop	11
Scope.....	11

Vision & goals.....	12
Steering committee	12
Roles & responsibilities.....	12
Processes & procedures	12
New features & updates.....	12
Microsoft Teams Workload.....	13
Collaboration templates	13
Naming convention	14
External access.....	16
Expiration policy.....	18
Options & activity check.....	18
Backup & restore	20
Privacy	21
Sensitivity labels.....	21
DLP	26
Retention	29
Creation process	30
Team Settings.....	31
Step 2: Finalise strategy.....	32
Step 3: Implementation.....	32

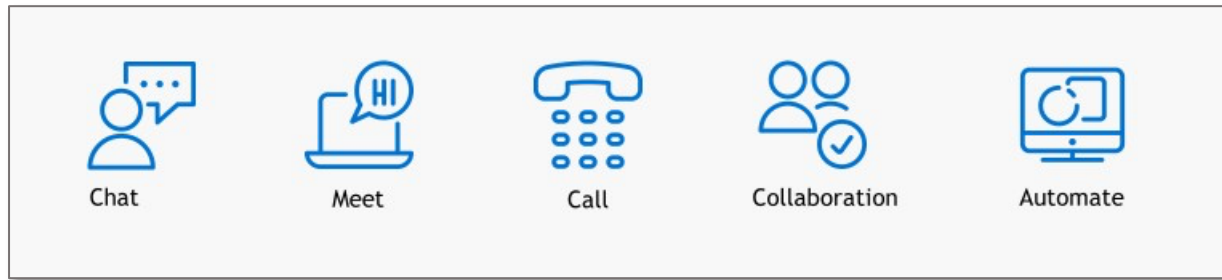
Three-step model

To create your own Microsoft Teams governance strategy, I advise applying the threestep model to deliver a governance strategy for your Microsoft Teams roll out successfully. The following steps are applicable:

- Governance workshop
- Governance strategy
- Governance implementation

Before we dive into the steps, I want to take a step back and talk a bit more about Microsoft Teams.

Welcome to Microsoft Teams



Microsoft Teams is the hub for collaboration & communication. Microsoft Teams is built on the following pillars:

Chat

Chat, compared to e-mail, provides an informal way of communication thanks to the availability of emoji's, stickers and giphy. Organisations use chat to stimulate an informal culture between colleagues and the leadership.

The adoption of chat quickly reduces the number of e-mails, you normally receive from your colleagues or partners. Who does not prefer fewer e-mails?

Meet

Online meetings are more efficient with Microsoft Teams. Presenters easily share their screen or PowerPoint presentation, attendees make notes on a digital whiteboard by using Microsoft Whiteboard, and recordings are available for people who missed the meeting.

Do you want to reach all your employees in a large and centrally organised meeting? Live meetings provide a structured meeting style with a presenter and producer. Attendees have a Q&A feature to their disposal to ask questions.

Call

Microsoft Teams is the follow-up of Skype for Business. Providing organisations with the option to set up your phone system.

Collaboration

Collaboration with your colleagues and external partners has never been easier.

Microsoft Teams provides a central location for all your communication and content, saving you valuable time finding the correct people and content.

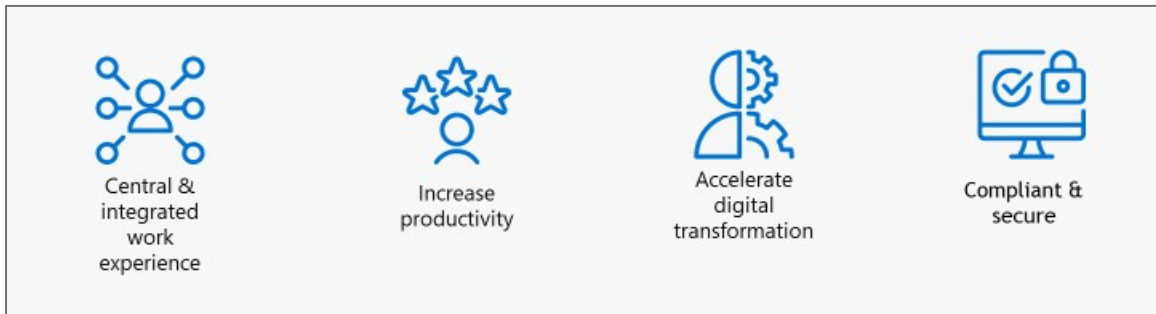
Through the connection with SharePoint Online, Microsoft Teams allows for an effective collaboration process by using the co-authoring feature in Office, enabling multiple people to work at the same time in the same Office document.

Automate

Microsoft Teams provides an integration with Power Apps & Power Automate to digitalise your business processes. At InSpark we digitalised our lunch declaration process. A bot checks who works at the office and asks the employees who participated in the company lunch. A positive confirmation sends a signal to an external financial system, automatically withdrawing your salary funds.

Business value

Microsoft Teams, with a successful governance & adoption strategy, can provide a business with value across several different areas:



Central & integrated work experience: Microsoft Teams provides an integration with Microsoft (for example: SharePoint, Yammer, OneDrive) and external services, reducing the need and time for employees to switch between multiple applications.

Increase productivity: By reducing switching between multiple applications, the concentration and focus increases, resulting in overall increased productivity.

Accelerate digital transformation: Most organisations are in the process of shifting towards the cloud, accelerating their digital transformation process. Luckily for them, Microsoft Teams is a cloud-only application.

Compliance & secure: Your data is safely stored in the Microsoft data centers. That said, you have a responsibility to provide a compliant & secure experience once the data is on your corporate and personal devices. Microsoft 365 contains multiple services to guarantee compliance & a secure experience.

Customer worries

The following worries have all been voiced whilst considering using Microsoft Teams; however, all can be mitigated by setting good Governance policies.

Teams explosion

By opening up Microsoft Teams for the whole organisation, dozens to hundreds of teams may be created. This may result in increased management requirements by the IT department and difficulty to find the correct team for the employees.

Duplication

Unfortunately, Microsoft Teams does not give you a warning when you create a team with the name of an existing team. This results in a duplicate team.

Purpose unclear

Teams without a clear name increase the difficulty in managing the teams for IT and picking the correct team that employees need to join.

Findability

In the Microsoft Teams application, the team overview menu is not user-friendly or intuitive, making it difficult to find relevant teams. This can result in the creation of duplicate teams and frustration with employees.

Complexity

The team creation menu contains many options and IT jargon. This makes it complex for less technically savvy employees to use.

Data leak

Although Microsoft Teams support compliance features, to prevent a data leak, these are not available by default. Enabling guest access results in an increased chance of a data leak.

Ignoring the list of worries would definitely be the easy way out. However, I would not recommend this approach because this would result in a failed adoption and increased IT maintenance. These need to be faced head-on and mitigated as much as possible as otherwise, they could hurt the rollout and usage of Microsoft Teams indefinitely.

The importance of a governance strategy

Defining and implementing a successful governance strategy for Microsoft Teams is important because of the following reasons:

Connecting IT & Business

A successful rollout and usage of Microsoft Teams depends on the collaboration between IT and the business. They need to be aware of each other requirements and responsibilities. This leads to more understanding, reduced miscommunication, and overall, less frustration down the line.

Contribute to a successful adoption

During the definition of the governance topics, (more about this later) decisions are being made impacting how employees are going to use Microsoft Teams. For example: Inviting guests into a team. The responsibilities for the employees taking up the roles of owner need to be communicated, or included in formal training. This should be part of your adoption strategy. Governance and adoption are crucial for a successful rollout of your Microsoft Teams implementation. Click [here](#) to learn more about adoption and Microsoft Teams.

Integration of procedures, law & regulations

All organisations have internal procedures (for example: working with 3rd party apps) that need to be matched against the feature set, and options turned on by default, of Microsoft Teams. No matter the industry, each organisation needs to comply with law & regulation (for example, GDPR). Microsoft Teams needs additional configuration (for example classification of content) to comply with the required procedures, law & regulations.

Manage Microsoft 365 Groups

The foundation of Microsoft Teams is based on Microsoft 365 Groups. Once a team is created, a lot happens in your Microsoft 365 environment:

- Shared inbox & calendar in Exchange Online
- Team site in SharePoint Online
- Plan in Planner
- Group in Microsoft Stream
- Group in Azure Active Directory

This impacts both IT and the business. Your administrators need to be aware of this situation for maintenance purposes. Your employees need to learn how to work with these multiple services.

Click [here](#) to learn more about Microsoft 365 Groups and Microsoft Teams.

Step 1: Workshop

The first step for setting up a successful governance strategy is a workshop with representatives from IT and the business. IT should be represented by the manager and at least one administrator. The business should be represented by an information manager, communication employee, compliance & risk employee, and HR. The representatives need to have the authority to make and enforce decisions in the organisation. Otherwise, your governance efforts are doomed to fail.

The following topics should be discussed during the workshop:

- Scope
- Vision & goals
- Steering committee
- Roles & responsibilities
- Microsoft Teams workload & settings
- Processes & procedures
- New features & updates

We are diving into depth regarding the Microsoft Teams workload & settings later in this ebook. The following paragraphs contain brief information about the other topics.

Scope

The scope of the governance workshop. For example: Collaboration with Microsoft Teams.

Vision & goals

The vision & goals of the organisation behind the rollout and usage of Microsoft Teams in the organisation. These are used in the communication and training sessions with the organisation. This is a mandatory part of your adoption strategy.

Steering committee

The content of the governance strategy needs to be monitored and adjusted by a group of people. This is the steering committee.

Roles & responsibilities

The roles & responsibilities related to Microsoft Teams need to be defined and assigned to people or departments. For example: Office 365 Global Administrator and Microsoft Teams administrator.

Processes & procedures

The internal processes & procedures in relationship to the usage of Microsoft Teams within your organisation. For example: The employment process. How will new employees receive a license and access to use Microsoft Teams?

New features & updates

Microsoft Teams is continuously updated by Microsoft. Your organisation needs to anticipate these changes and communicate these to employees. This can be done by monitoring the [Microsoft 365 Roadmap](#), [Office 365 message center](#), and the [public preview](#).

Microsoft Teams Workload

The topics for defining the governance strategy of the Microsoft Teams workload are divided into the following topics:

- Collaboration templates
- Naming convention
- External access
- Expiration policy
- Privacy
- Back-up & restore
- Compliance
- Creation process

The following paragraphs contain more information.

Collaboration templates

Microsoft Teams supports collaboration between a group of people. Organisations collaborate in different manners. For example:

- Departments
- Projects
- Cross-departments

The first step is defining the collaboration templates. I advise to start small and keep it simple. Start with two collaboration templates and once these are successfully deployed and adopted, start again with additional templates.

Naming convention

Per collaboration template we can define a naming convention. For example: Each time a team is created for a project the following naming convention is applied in Microsoft Teams: PRO – Name of the project. Applying a naming convention for the URL of the SharePoint team site is possible but can only be set with a provisioning solution.

The following options, for applying a naming convention, are available:

1. **Prefix-suffix naming policy:** A policy available in Azure Active Directory. You can define prefixes or suffixes that are then added automatically to enforce a naming convention on your teams. For example, in the group name "GRP_JAPAN_My Group_Engineering", GRP_JAPAN_ is the prefix, and _Engineering is the suffix.¹
2. **Connect to a provisioning solution:** By using a provision solution, to create teams, you automatically enforce a naming convention.
3. **Leave it up to the employees:** During the creation process, the employees need to apply the naming convention defined for Microsoft Teams.
4. **None:** There is no naming convention set for teams.

Advantages:

- **Improving the** findability of a team in Microsoft Teams: The current team overview menu makes it difficult to find teams. By applying a naming convention, finding teams becomes easier for employees.

¹ Source: [Enforce group naming policy in Azure Active Directory | Microsoft Docs](#)

Challenges:

- **Prefix-suffix naming policy:** The Azure AD policy requires an up-to-date Azure Active Directory. This policy does not work with multiple collaboration templates because the policy is not flexible to apply a different name per template so its corresponds with the template.
- **Employees will forget:** Most employees are not going to remember to set a naming convention while creating a team.

My advice

I advise using a naming convention when necessary. For example: I worked with a local district that shared their Office 365 tenant with other districts and organisations. By applying a naming convention, they can immediately see where a team belongs. Improving the findability for employees and the administration process for IT.

External access

External access allows organisation to collaborate with external people in Microsoft Teams. These are people with an external e-mail address.

The following options are available:

- **Allow for all teams:** All teams can invite an external person.
- **Allow for a selection of teams:** Only a selection of teams can invite an external person.
- **Disable for all teams:** No teams can invite an external person.
- **Decide with a sensitivity label:** By selecting a sensitivity label, the team can or cannot invite an external person.

External access is configured in multiple locations. Click [here](#) for more information.

Advantages:

- **Reduce shadow IT:** These days, collaboration with external people is the norm. By disabling external access in Microsoft Teams, your employees are going to use other, and most likely, external services. This results in shadow-it. By enabling external access, you reduce the risk of shadow IT within your organisation.
- **Efficient collaboration:** Collaboration with external people in Microsoft Teams is more efficient compared to sending e-mails with attachments. Microsoft Teams is made for collaboration. Internally and externally.

Challenges:

- **Compliance is crucial:** Once an external person has access to a team, and its content, they can download all the content. This could result in a data leak. This can be prevented by using compliance features such as data classification with sensitivity labels or Data Loss Prevention (DLP).
- **Increased responsibility for the owners:** The owner of a team is responsible for inviting the correct external people. This gives them an increased responsibility compared to the alternative whereby IT only invites and adds external people to teams.

My advice

Normally, of course, this differs depending on certain requirements, I advise turning on external access for all teams. This approach does require a strong control and review process. This can be done with the following activities:

- **Apply a period review:** Azure contains a feature called Azure Access Reviews. This requires owners to review the membership of their team. Click [here](#) to learn more. By using the Microsoft Graph, you can build your own review solution.
- **Apply social control:** Once a guest is added to a team, this becomes visible to the other employees. They will attend the owner about the presence of an external person.
- **Educate the team owners:** Only the owners of a team can invite an external person. This reduces the amount of people being able to invite external people. By teaching the owners about their responsibility, you reduce the risk of unwanted external access.
- **Start with compliance:** An external person needs access to a team. Once he or she has access they can download all the content. This could result in a data leak.

This can be prevented by using compliance features such as data classification with sensitivity labels or Data Loss Prevention (DLP).

Expiration policy

After a while, your Office 365 tenant contains inactive teams. Azure Active Directory contains a feature to delete inactive teams by setting an expiration policy. The expiration policy is based on a number of days. For example: 180. The owners of a team receive an e-mail notification and a message in the team 30, 15 and one day before expiration, asking them to keep or delete the team. Once the team is deleted, the team and all related content, is moved to a recycle bin. Only the Office 365 administrator can restore the team within 30 days. After this period, the team cannot be restored anymore. Click [here](#) for more information.

Options & activity check

The following options are available:

- **All teams:** All the teams are bound to an expiration policy.
- **Selection of teams:** Only a selection of teams is bound to an expiration policy.
- **None:** No expiration policy is enabled.

Active teams will not receive a notification to renew or delete the team. The activity is based upon the following user activities:

- **SharePoint:** View, edit, download, move, share, or upload files.
- **Outlook:** Join group, read/write group message from group space, Like a message (in Outlook Web Access).
- **Teams:** Visit a Teams channel.

Click [here](#) to learn more.

Advantages:

- **Keep your Office 365 tenant clean:** By removing inactive teams your Office 365 tenant stays “clean” and does not contain any inactive teams.
- **Reduce manual maintenance for IT:** By giving team owners the responsibility and action for cleaning up inactive teams, IT can spend time on other activities.

Challenges:

- **Rely on Microsoft back-up & restore:** Once a team is removed by an owner and the 30 days have passed, the team and all its content are gone forever. Without an additional back-up solution, you are bound to the Microsoft back-up & restore settings.
- **Increased responsibility for the owners:** The owner of a team is responsible for renewing or deleting a team. This gives them an increased responsibility compared to the alternative whereby IT only deletes an inactive team.
- **Retention policies need to be clear:** A team that is being marked for deletion by an owner can contain content that needs to be retained for a longer period. This is where the retention policies need to be clear, so data is not deleted that should have been preserved.

My advice

I advise to turn on the expiration policy for one year and start looking at your retention policies. You do not want any teams to be deleted containing data that should have been retained.

Backup & restore

Employees have more control over the deletion of the team and content. Microsoft supports organisations by having back-up and restore in place.

The following back-up & restore options, in relationship to Microsoft Teams, are available:

- Teams are stored for 30 days in a recycle bin. Click [here](#) for more information.
- Channels are stored for 30 days in a recycle bin. The recycle bin is available in the team's settings menu.
- Content is stored for 90 days in a recycle bin. Click [here](#) for more information.
- Video's and recordings are stored for 30 days in a recycle bin. Click [here](#) for more information. Microsoft is in the process of moving the storage or recordings to SharePoint & OneDrive instead of Microsoft Stream. This would extend the number of days to 90 instead of 30.

My advice

I would advise to review the Microsoft back-up & restore options and match these against your internal agreements and regulations. Are the Microsoft options sufficient? Perfect. If they are not, then it's time to look to 3rd party vendors. There are multiple vendors, for example AvePoint, offering back-up solutions. You should also start with defining your retention policies.

Privacy

Microsoft Teams offer privacy settings to control the access and visibility of the team and its content.

The following privacy options are available:

- **Private:** Only owners can invite new members.
- **Public:** All employees can join the team and the content is visible for all internal employees.
- **Org-wide:** All employees are automatically added to the team.

Click [here](#) for more information.

My advice

My preference is open by default to stimulate knowledge sharing and finding relevant content and people. That said, there are situations where this is not possible. For example: HR Team or Board of Directors. Owners can change the privacy settings of a team. **Be aware:** This is not possible when the privacy is set with a sensitivity label. More about this in the next paragraph.

Sensitivity labels

Sensitivity labels are used to classify and protect content. To prevent unwanted access to content. The labels are extended to being applied to Microsoft 365 Groups (Microsoft Teams & SharePoint Online).

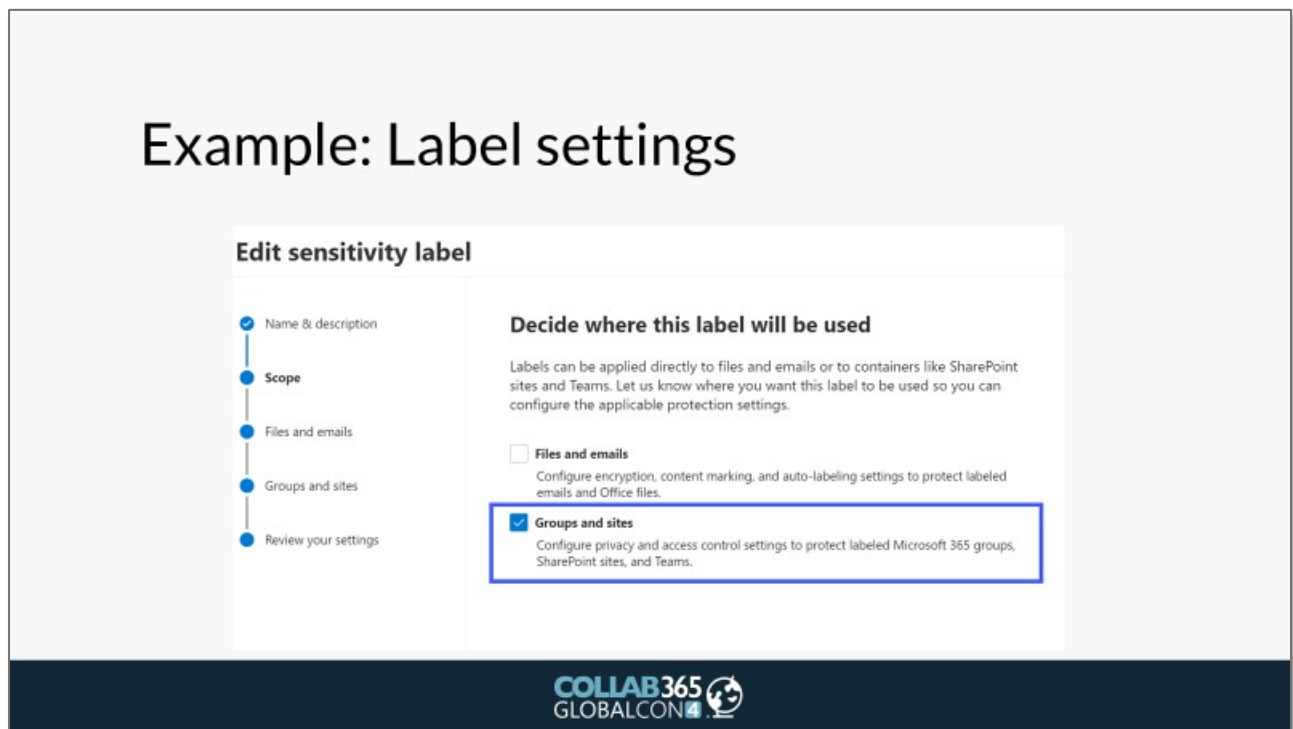
The following options are available once a label is connected to a team in Microsoft Teams:

- **Privacy:** Automatically set the privacy, that cannot be changed once applied, to public or private.
- **Guest access:** Allow or block guest access.
- **External sharing:** Set the external sharing links to anyone, new & existing, existing guests or none.
- **Unmanaged:** Define the access to the content in the SharePoint Team Site for unmanaged devices: full access, web-only or none.

The label attached to the team does not classify or protect the content. You need to set separate labels. Click [here](#) for more information.

Examples

The following screenshots show an example of the settings:



Example: Label settings

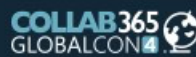
Edit sensitivity label

- ✓ Name & description
- ✓ Scope
- ✓ Files and emails
- Groups and sites**
- Review your settings

Define protection settings for groups and sites

Configure privacy and access control settings to protect labeled Microsoft 365 groups, SharePoint sites, and Teams.

- ✓ **Protection settings for groups**
Configure privacy and external user access settings to protect Microsoft 365 groups and Teams.
- ✓ **Protection settings for sites**
Determine the level of access users have to SharePoint sites from unmanaged devices.



Example: Label settings

Edit sensitivity label

- ✓ Name & description
- ✓ Scope
- ✓ Files and emails
- Groups and sites**
- Protection settings for groups
- Protection settings for sites
- Review your settings

Define protection settings for groups

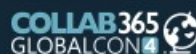
Select the settings you want to take effect when this label is applied to an Microsoft 365 group or SharePoint site. Note that the settings aren't applied to files, so they don't impact downloaded copies of files. [Learn more about site and group protection](#)

Privacy of Microsoft 365 group-connected team sites

- ☐ Public - anyone in the organization can access the site
- ☒ Private - only members can access the site
- ☐ None - let user choose who can access the site

External users access

- ✓ ☒ Let Microsoft 365 group owners add people outside the organization to the group



Example: Label & Teams


What kind of team will this be? ×


Sensitivity [Learn more](#)

Project ▼

Teams with this sensitivity must be private.

Privacy

**Private**
People need permission to join

**Public**
Anyone in your org can join ⓘ

COLLAB365
GLOBALCON4 

Example: Guest access

Start typing a name, distribution list, or mail enabled security group to add to your team.

Add

We didn't find any matches.

Close

COLLAB365
GLOBALCON4 

Example: Unmanaged Device



COLLAB365
GLOBALCON 4

My advice

The sensitivity labels cannot be used with the Microsoft Graph, making it difficult to combine in an automatic process with a provisioning solution. That said, the labels are perfect for a self-service team creation by the employees. I would strongly advise you to start with a separate project defining your content classification need.

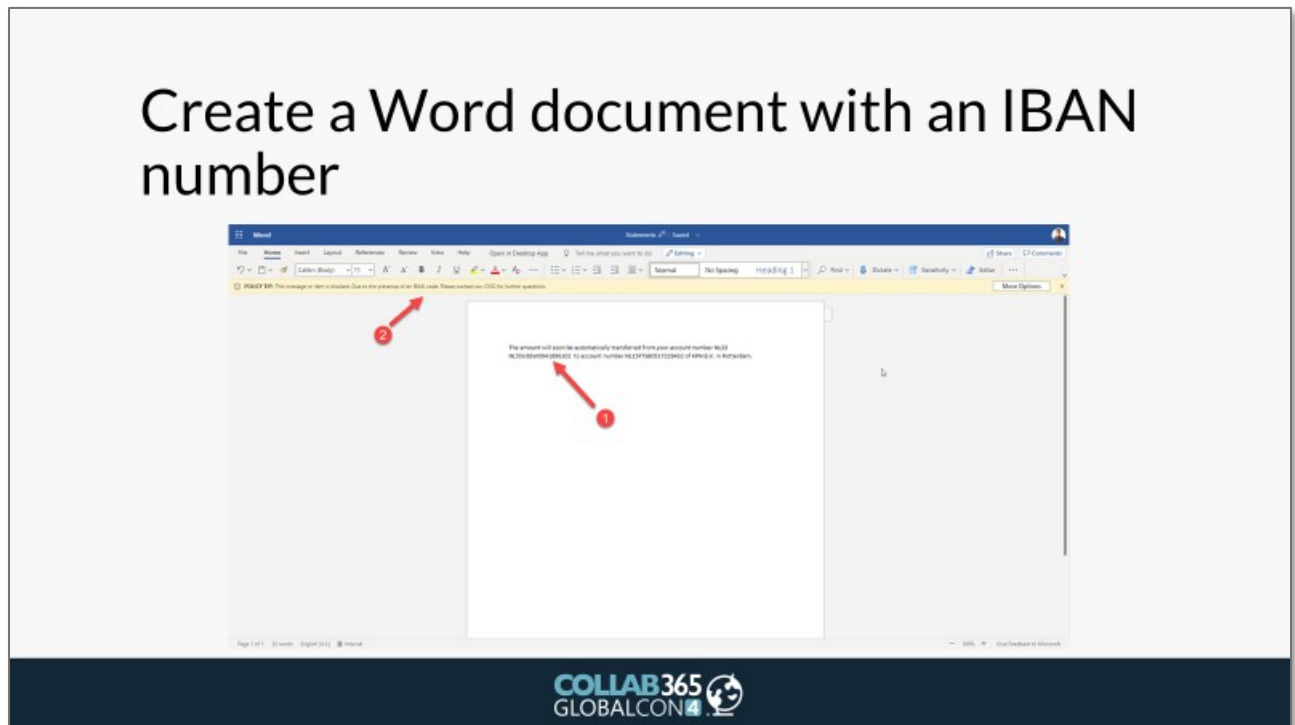
DLP

DLP (data loss prevention) prevents the sharing of sensitive information with colleagues and / or external people.

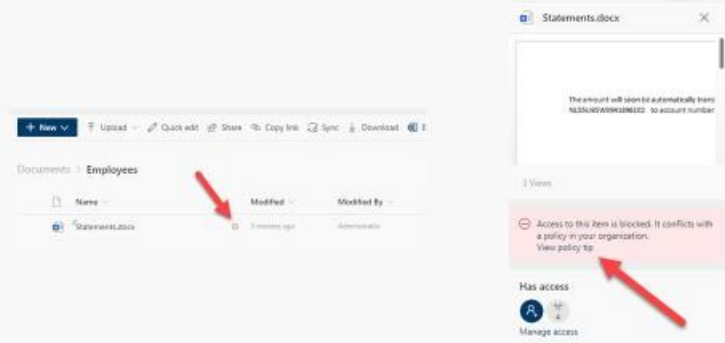
The definition of sensitive information is defined in a DLP policy. This could be a social security or credit card number. The DLP policy can be applied to chat in Microsoft Teams (you need an Office 365 E5 license) or content stored in the SharePoint Team Site (Office 365 E3). Click [here](#) for more information.

Examples

The following screenshots show an example of the employee experience when a DLP policy is triggered:



Notifications in SharePoint



Policy tip for 'Statements.docx'

This message or item is blocked. Due to the presence of an IBAN code. Please contact our CISO for further questions. Access to this item is blocked for everyone except its owner, last modifier, and the site owner.

Issues

Item contains the following sensitive information: International Banking Account Number (IBAN)

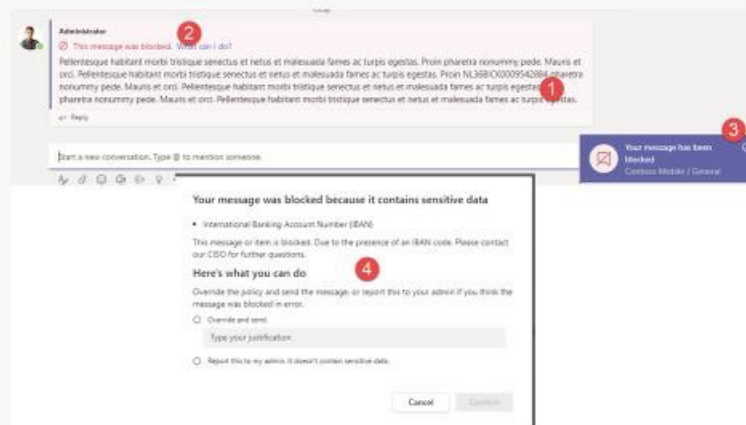
Last scanned: 11 minutes ago

[Report an issue](#) to let your admin know that this item doesn't conflict with your organization's policies.

[Override](#) the policy if you have business justification. All policy overrides are recorded.



Notifications in Teams



My advice

Before you implement a DLP policy you need to match the use of Microsoft Teams with your internal procedures and regulations. The next step is testing the DLP policy, you need to be confident the policy works as expected. Follow up: Let your employees know why DLP is being implemented and what the impact is. This increases the adoption rate of DLP. All these steps should be included in a separate project.

Retention

Retention is aimed at preserving content from being modified and / or deleted indefinitely. Click [here](#) for more information.

The following options are currently available:

- Retain content or chat for an X number of days, weeks, or years.
- Retain content or chat and delete after an X number of days, weeks, or years.
- Delete content or chat after an X number of days, weeks, or years.

During the moment of writing Microsoft does not support retention for chat in private channels. Click [here](#) for more information.

My advice

Before you implement a retention policy, you need to match the use of Microsoft Teams with your internal procedures and regulations. The next step is testing the retention policy; you need to be confident the policy works as expected. Follow up: Let your employees know why retention is being implemented and what the impact is. This increases the adoption rate of retention. All these steps should be included in a separate project.

Creation process

Did you define all the above requirements for collaboration template? Now, it is time to define the creation process of your collaboration templates in Microsoft Teams.

The following options are available:

- Allow all your employees to create a team in Microsoft Teams via the Microsoft Teams applications.
- Allow a selection of employees to create a team in Microsoft Teams via the Microsoft Teams applications.
- Provide a controlled creation process with a provisioning solution for all or a selection of employees.

What determines the use of self-service or a provisioning solution?

- Do you require multiple collaboration templates?
- Do your collaboration templates require a unique naming convention?
- Do your collaboration templates require strict external access policies?
- Do your collaboration templates require different expiration policies?

Did you answer yes? You are most likely bound to a provisioning solution. This is not a problem at all, as there is no wrong or right answer. You can start with a provisioning solution and move on to a self-service scenario in a later stage.

Team Settings

The Microsoft Teams Administrator center contains a lot of settings. These settings need to be reviewed and any adjustments need to be written down in the governance strategy document.

The following settings need to be reviewed:

- **Teams policies:** Enabling or disabling private channels. Click [here](#) for more information.
- **Update policies:** Enabling new features for a selection of employees. Click [here](#) for more information.
- **Meeting policies:** Review the default meeting options. Click [here](#) for more information.
- **Meeting settings:** Review the default meeting settings. Click [here](#) for more information.
- **Messaging policies:** Review the default messaging options. Click [here](#) for more information.
- **Teams apps:** Review the app policy & settings. Click [here](#) for more information.
- **Guest access:** Review the default guest options. Click [here](#) for more information.
- **Teams settings:** Review the remaining default settings. Click [here](#) for more information.

Step 2: Finalise strategy

After the workshop, the team needs to get an agreement on all the topics. These are added in a centralised content (for example: Word document or SharePoint Site). The final findings are presented, and the governance strategy is finalised. Ready to be implemented in the final step.

Step 3: Implementation

Once you defined and finalised your governance strategy, it is time to start the implementation. Depending on your decisions, these are divided between the following:

- **Microsoft Teams settings:** These vary from multiple policies or external access settings.
- **Governance solution:** A provisioning, governance, or back-up solution.

You successfully finished the three-step model? Great news! You made a first good step in successfully rolling out and using Microsoft Teams in your organisation. That said, you cannot sit back! You need to be sure your governance strategy is being followed and continuously reviewed and updated. Time to start with your steering committee!