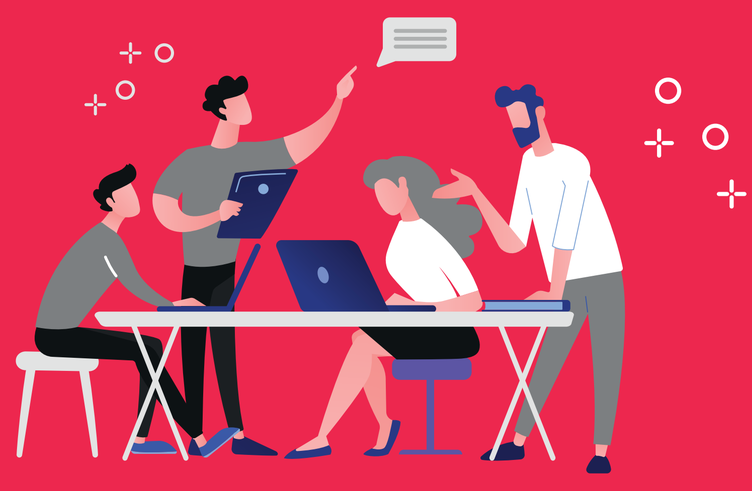
Microsoft Teams

7 Best Practices to improve Data Protection

IDECSI
Enterprise Security



About Teams chat

1

Share information in the right collaboration space: Teams or Chat

Chat conversations are used for informal communication. Team are recommended for sharing sensitive information or group collaboration.

Please note that a chat cannot be deleted and any member of a conversation can add employees into it.

2

Update access rights on shared documents from OneDrive

Shared documents in a chat are stored in OneDrive. A regular check helps to have control over access rights of previously shared documents.

About Teams group

3

Create a private team

To manage correctly team members and information. Only owners can add or remove members.

4

Add two owners for a team

To ensure that there is always an owner present to moderate information and team members.

5

Limit access to confidential data with private channels

To refine audience within a team: make sure that only authorised persons can reach out conversations, documents and applications. Access to information will therefore be under control.

6

Regularly check access to your teams, including guests

A review of access and external guests can be initiated by the owner, for example at the end of each step.

Tips: an icon is visible in Teams indicating if there are any externals members

7

Delete permanently sensitive documents

To make it completely inaccessible, it also has to be deleted from the recycle bin of the associated SharePoint site.