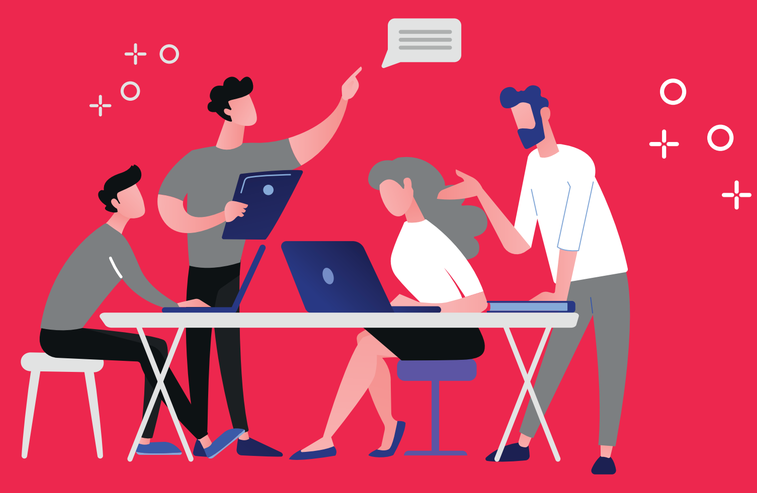
IDECSI
Enterprise Security

Microsoft Teams

7 bonnes pratiques pour améliorer la protection des données



Autour des conversations Teams

1 Partager les informations dans les bons espaces : Equipes ou Conversations

Les conversations chat vont servir pour des échanges informels.
Les équipes sont recommandées pour du partage d'informations sensibles ou de la collaboration en groupe.

Attention : Les conversations ne peuvent pas être supprimées et tous les membres d'une conversation peuvent ajouter d'autres collaborateurs.

2 Mettre à jour les droits d'accès sur les documents partagés depuis OneDrive

Les documents dans les conversations sont stockés dans votre espace OneDrive. Une revue des droits régulière permet de garder le contrôle sur les partages et les droits accordés sur vos fichiers.

Autour des équipes Teams

3 Créer des équipes privées

Pour mieux gérer les membres d'une équipe et les informations. Seuls, les propriétaires peuvent ajouter ou supprimer des membres.

4 Nommer deux propriétaires d'équipe

Pour s'assurer qu'un administrateur est toujours présent pour modérer les informations et les membres de l'équipe.

5 Limiter l'accès aux données confidentielles avec des canaux privés

Pour affiner l'audience au sein d'une équipe : seules les personnes autorisées pourront avoir accès aux publications, documents, applications, ... L'accès à l'information sera alors plus contrôlé.

6 Vérifier régulièrement les accès sur vos équipes Teams, notamment les invités

Une revue des accès et des invités externes peut être initiée par les responsables d'espace en fonction de l'avancée du projet, par exemple à chaque fin d'étape.

Astuce : une icône est visible dans l'équipe teams vous indiquant si des externes sont présents.

7 Supprimer définitivement un document sensible

Pour qu'il ne soit plus du tout accessible, il faudra le supprimer également au niveau de la corbeille du site SharePoint associé.