Smartfuture
Certifications | Training | Technology solutions

Formation

Gestion des permissions et des autorisations

Formation opérationnelle pour structurer, sécuriser et administrer les droits d'accès au sein de votre environnement numérique (Microsoft 365, SharePoint, Teams, applications métiers…). L'objectif : garantir le bon accès à la bonne personne, au bon moment, tout en réduisant les risques.

Formation 100% pratique

Exercices & cas d'usage

Formateur expérimenté

2 jours
14 h

Format
Atelier pratique

Modalité
Présentiel ou en ligne

Niveau
Débutant / Intermédiaire

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

OBJECTIFS PÉDAGOGIQUES

- Comprendre les concepts clés de permissions, autorisations, rôles et groupes.
- Structurer une stratégie de gestion des droits alignée sur l'organisation.
- Configurer et contrôler les accès utilisateurs dans les principaux outils collaboratifs.
- Mettre en place des bonnes pratiques de revue, de journalisation et de retrait des droits.

PUBLIC CIBLE

- Administrateurs Microsoft 365, SharePoint, Teams, applications métiers.
- Référents digitaux et owners de sites/équipes.
- Responsables sécurité / RSSI / DSI.
- Managers amenés à valider et sponsoriser les règles d'accès.

PRÉREQUIS

- Bonne connaissance de l'environnement de travail de l'organisation (Microsoft 365 ou équivalent).
- Notions générales de sécurité de l'information.
- Aisance avec les interfaces d'administration ou de paramétrage.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Concepts fondamentaux des permissions et autorisations

Notions de base

- Différence entre authentification, autorisation et audit.
- Principes de moindre privilège et de séparation des rôles.
- Rôles, groupes, niveaux d'autorisation, héritage des permissions.

Risques liés à une mauvaise gestion des accès

- Sur-exposition de l'information (documents « Partagé avec tout le monde »).
- Accès orphelins après départ ou changement de poste.
- Impact sur la conformité et la confidentialité.

Structurer la gestion des droits dans l'organisation

Modèle de gouvernance des accès

- Définir les rôles clés : IT, responsables métiers, owners, contributeurs, lecteurs.
- Règles d'ouverture vs. fermeture des espaces (sites, équipes, canaux).
- Utilisation des groupes de sécurité et des groupes Microsoft 365.

Processus de création, modification et suppression des droits

- Demande d'accès : validation, traçabilité, durée limitée.
- Changement de poste ou mobilité interne.
- Gestion des comptes externes (invités, partenaires).

Gestion pratique des permissions dans les outils collaboratifs

Exemples dans Microsoft 365 (SharePoint, Teams, OneDrive…)

- Gérer les droits sur un site SharePoint (héritage, rupture, niveaux).
- Permissions sur les bibliothèques et dossiers sensibles.
- Accès dans Microsoft Teams : équipe, canaux standards et privés.
- Partage de fichiers OneDrive : liens, expiration, restrictions.

Bonnes pratiques d'administration quotidienne

- Modèles de sécurité par type d'équipe/projet.
- Check-list avant ouverture d'un nouvel espace collaboratif.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Revue, audit et nettoyage des droits

Contrôler et suivre les accès dans le temps

- Mettre en place des revues périodiques des droits.
- Identifier les accès anormaux ou surdimensionnés.
- Journalisation, rapports et traçabilité.

Nettoyage et remédiation

- Plan de nettoyage des droits hérités ou obsolètes.
- Mise en conformité progressive des espaces existants.

Atelier : cas pratiques de gestion des permissions

Mises en situation concrètes

- Création d'un espace projet avec règles d'accès spécifiques.
- Gestion d'un dossier sensible (RH, Finance, Direction).
- Traitement d'un audit révélant des droits excessifs.

Plan d'action pour votre organisation

- Définir les priorités : quels espaces sécuriser en premier ?
- Établir une feuille de route « permissions & autorisations » avec les parties prenantes.