Protégez vos documents sensibles en toute circonstance

Gestion des accès et authentification

• Appliquer le principe du moindre privilège : limiter l'accès aux fichiers uniquement aux personnes dont le rôle nécessite explicitement de les consulter ou de les modifier.

• Imposer l'authentification multifacteur (MFA) pour tous les accès aux plateformes de partage afin d'atténuer les risques liés au vol d'identifiants.

Sécurisation technique des données

• Chiffrer les fichiers sensibles au repos et en transit en utilisant des protocoles modernes (AES-256 et TLS 1.2 minimum).

• Utiliser des outils de Data Loss Prevention (DLP) pour identifier et bloquer automatiquement le partage de documents contenant des données sensibles vers des destinataires non autorisés.

Bonnes pratiques de partage externe

• Privilégier le partage par lien restreint (individus spécifiques) plutôt que le partage par lien public.

• Définir des durées d'expiration automatiques pour tous les liens de partage externes.

• Protéger les liens de partage par des mots de passe robustes et une vérification d'identité du destinataire.

• S'assurer que la solution utilisée permet de révoquer immédiatement l'accès à un document, même après son envoi.

Audit et culture de sécurité

• Journaliser et auditer régulièrement les accès aux fichiers pour détecter les comportements anormaux ou les exfiltrations de données.

• Former les employés à ne jamais utiliser de solutions de partage de fichiers grand public non autorisées par l'entreprise (Shadow IT).