FICHES MÉMO – BONNES PRATIQUES EN CYBERSÉCURITÉ

Contexte d'utilisation
Document interne destiné à la sensibilisation des collaborateurs et à l'harmonisation des pratiques de sécurité du système d'information.
Dernière mise à jour : 2025

FICHE 1 – ATTRIBUTION D'UN ACCÈS VPN

Objectif de sécurité
Garantir un accès distant sécurisé au réseau de l'entreprise tout en respectant la traçabilité et le principe du moindre privilège.

Bonnes pratiques
- Vérifier l'identité et le besoin métier avant toute attribution.
- Appliquer le principe du moindre privilège (accès limités aux ressources nécessaires).
- Définir une date d'expiration pour les accès temporaires.
- Imposer l'authentification multifacteur (MFA).
- Documenter chaque attribution dans un registre d'accès.
- Réaliser une revue périodique des accès (au minimum trimestrielle).

Erreurs fréquentes à éviter
- Donner un accès VPN complet sans restriction.
- Conserver des accès après changement de poste ou départ.
- Partager des identifiants VPN.
- Ne pas désactiver les accès en fin de mission.

Niveau de risque : Élevé

FICHE 2 – PARTAGE DE DONNÉES SENSIBLES

Objectif de sécurité
Prévenir les fuites de données et garantir la conformité réglementaire (RGPD).

Bonnes pratiques
- Classifier les données avant tout partage.
- Utiliser uniquement des outils validés par l'entreprise.
- Chiffrer les fichiers lors de partages externes.
- Limiter les droits d'accès (lecture seule si possible).
- Définir une durée de validité pour les liens de partage.
- Vérifier les adresses e-mail des destinataires.

Erreurs fréquentes à éviter
- Envoyer des données sensibles par e-mail non chiffré.
- Utiliser des services cloud personnels.
- Créer des liens publics sans contrôle.

Niveau de risque : Élevé

FICHE 3 – CRÉATION ET SUPPRESSION DE COMPTES UTILISATEURS

Objectif de sécurité
Maîtriser le cycle de vie des comptes pour éviter tout accès non autorisé.

Bonnes pratiques
- Appliquer un processus de validation formel.
- Respecter une convention de nommage standard.
- Attribuer uniquement les droits nécessaires.
- Activer les comptes uniquement à l'arrivée effective.
- Désactiver immédiatement les comptes lors d'un départ.
- Révoquer l'ensemble des accès associés (VPN, cloud, applications).

Erreurs fréquentes à éviter
- Utiliser des comptes génériques partagés.
- Laisser actifs des comptes inutilisés.
- Attribuer des droits administrateurs par défaut.

Niveau de risque : Élevé

FICHE 4 – ACCÈS AUX RESSOURCES CLOUD

Objectif de sécurité
Garantir un accès sécurisé et maîtrisé aux services cloud de l'entreprise.

Bonnes pratiques
- Imposer la MFA sur tous les comptes cloud.
- Centraliser les accès via SSO.
- Activer les journaux d'audit et la supervision.
- Mettre en place des politiques d'accès conditionnel.
- Chiffrer les données au repos et en transit.
- Sensibiliser les utilisateurs au phishing.

Erreurs fréquentes à éviter
- Utiliser des comptes personnels.
- Désactiver la MFA.
- Accorder des permissions excessives.

Niveau de risque : Élevé

FICHE 5 – TÉLÉTRAVAIL

Objectif de sécurité
Maintenir un niveau de sécurité équivalent à celui du travail sur site.

Bonnes pratiques
- Utiliser uniquement du matériel professionnel.
- Accéder aux ressources internes via VPN.
- Sécuriser le Wi-Fi personnel.
- Verrouiller automatiquement les sessions.
- Maintenir les systèmes à jour.

Erreurs fréquentes à éviter
- Utiliser du matériel personnel non sécurisé.
- Se connecter à des réseaux publics sans VPN.
- Stocker des données professionnelles sur des supports personnels.

Niveau de risque : Moyen

FICHE 6 – UTILISATION DE SUPPORTS AMOVIBLES

Objectif de sécurité
Limiter les risques d'infection et de fuite de données.

Bonnes pratiques
- Utiliser uniquement des supports validés par l'entreprise.
- Chiffrer systématiquement les données sensibles.
- Scanner les supports avant utilisation.
- Désactiver l'exécution automatique.
- Détruire les supports en fin de vie.

Erreurs fréquentes à éviter
- Utiliser des clés USB inconnues.
- Copier des données sensibles sans chiffrement.
- Laisser des supports sans surveillance.

Niveau de risque : Élevé

FICHE 7 – ACCÈS ADMINISTRATEUR / PRIVILÈGES ÉLEVÉS

Objectif de sécurité
Réduire les risques liés aux comptes à privilèges.

Bonnes pratiques
- Séparer comptes utilisateurs et administrateurs.
- Limiter le nombre de comptes à privilèges.
- Imposer la MFA.
- Journaliser et auditer toutes les actions.
- Révoquer les droits après intervention.

Erreurs fréquentes à éviter
- Travailler quotidiennement avec un compte admin.
- Partager des comptes administrateurs.
- Conserver des droits inutiles.

Niveau de risque : Élevé

FICHE 8 – CONNEXION À DISTANCE (RDP / SSH)

Objectif de sécurité
Empêcher les intrusions et prises de contrôle à distance.

Bonnes pratiques
- Ne jamais exposer RDP/SSH directement sur Internet.
- Utiliser un VPN ou un bastion.
- Privilégier l'authentification par clé.
- Restreindre les accès par IP.
- Surveiller et bloquer les tentatives suspectes.

Erreurs fréquentes à éviter
- Laisser des ports ouverts publiquement.
- Utiliser des mots de passe faibles.
- Négliger les mises à jour de sécurité.

Niveau de risque : Élevé

FICHE 9 – GESTION DES MOTS DE PASSE ET MFA

Objectif de sécurité
Renforcer l'authentification des utilisateurs.

Bonnes pratiques
- Utiliser un gestionnaire de mots de passe professionnel.
- Créer des mots de passe longs et uniques.
- Activer la MFA dès que possible.
- Changer immédiatement les mots de passe compromis.

Erreurs fréquentes à éviter
- Réutiliser les mots de passe.
- Stocker les mots de passe en clair.
- Partager ses identifiants.

Niveau de risque : Élevé

FICHE 10 – ENVOI DE DONNÉES PAR EMAIL

Objectif de sécurité
Prévenir les fuites d'informations par messagerie électronique.

Bonnes pratiques
- Vérifier les destinataires avant envoi.
- Chiffrer les emails contenant des données sensibles.
- Privilégier les liens sécurisés aux pièces jointes.
- Ne jamais envoyer de mots de passe par email.

Erreurs fréquentes à éviter
- Envoyer des données sensibles en clair.
- Utiliser une messagerie personnelle.
- Cliquer sur des liens ou pièces jointes suspectes.

Niveau de risque : Moyen

Notes d'utilisation
Ces fiches doivent être relues annuellement, adaptées au contexte de l'entreprise et complétées par des actions de sensibilisation régulières.