

TIP 2.11

Protéger les comptes, les accès et les données

Fiche de révision - Équipements numériques

1. Identification, authentification, autorisation

Notion	À retenir
Identification	Déclarer qui l'on est.
Authentification	Prouver son identité : mot de passe, PIN, MFA, biométrie...
Autorisation	Déterminer ce que l'utilisateur peut consulter ou modifier.

Méthode à retenir :
Identifier → Authentifier → Autoriser → Chiffrer → Contrôler → Sensibiliser

2. Moindre privilège et comptes

Principe	Bonne pratique
Compte standard	Usage quotidien de l'utilisateur.
Compte administrateur	Réservé aux opérations nécessitant des privilèges élevés.
Moindre privilège	N'accorder que les droits nécessaires au besoin réel.
Séparation des comptes	Compte utilisateur distinct du compte d'administration lorsque la politique le prévoit.

3. Vérifier les administrateurs locaux

Comparer la liste des administrateurs locaux avec la configuration attendue. Un compte inconnu ou inutile doit être vérifié avant livraison.

PowerShell : Get-LocalGroupMember -Group "Administrateurs"

4. Mots de passe

À faire	À éviter
Secret long et unique.	Réutiliser le même mot de passe partout.
Utiliser la solution de gestion approuvée.	Post-it, fichier texte, ticket ou partage du secret.
L'utilisateur saisit lui-même son secret.	Demander le mot de passe personnel pour dépanner.

5. MFA

Facteur	Exemple
Ce que je sais	Mot de passe, PIN.
Ce que je possède	Téléphone, clé de sécurité, carte.
Ce que je suis	Empreinte ou reconnaissance faciale.

Demande MFA inattendue : ne pas valider. Refuser la demande et la signaler selon la procédure de l'organisation.

6. Verrouillage de session

Windows + L verrouille immédiatement la session. Un verrouillage automatique peut aussi être imposé par stratégie ; il ne doit pas être désactivé pour convenance personnelle.

7. Permissions et groupes

Bonne pratique	Pourquoi
Attribuer les droits nécessaires uniquement.	Réduit les risques d'accès ou de modification non justifiés.
Utiliser des groupes plutôt que des droits directs.	Facilite l'administration, les changements et les audits.
Ne pas donner Contrôle total par défaut.	Le niveau d'accès doit correspondre au besoin réel.

8. Chiffrement et BitLocker

Le chiffrement protège les données si le support est perdu, volé ou retiré de la machine. Un mot de passe Windows seul ne suffit pas à protéger les données d'un disque extrait du poste.

Élément	À retenir
Get-BitLockerVolume	Vérifie l'état du chiffrement et de la protection.
Clé de récupération	Secret sensible à stocker uniquement dans l'emplacement prévu par l'organisation.
Avant intervention	Vérifier que les moyens de récupération nécessaires sont disponibles.

9. Supports amovibles et confidentialité

Sujet	Bonne pratique
Clé USB personnelle	Ne pas l'utiliser pour des données professionnelles si la politique l'interdit.
Données personnelles	Accéder uniquement aux informations nécessaires à l'intervention.
Captures d'écran	Vérifier et masquer les informations inutiles avant partage.
Secrets techniques	Ne pas stocker mots de passe, tokens, clés API ou clés de récupération dans les tickets.

10. Checklist avant livraison

Contrôle	État attendu
Compte	Standard pour l'usage quotidien si prévu.
Administrateurs	Liste contrôlée, aucun compte inconnu.
MFA	Activé sur les services où il est requis.
Session	Verrouillage manuel et automatique conformes.
Permissions	Accès nécessaires, aucun privilège excessif.
BitLocker	Protection conforme et récupération maîtrisée.
Supports	Usage conforme à la politique.
Confidentialité	Aucun secret ou donnée sensible exposé inutilement.

11. À retenir

Protéger les accès consiste à limiter, authentifier et chiffrer.
Appliquer le moindre privilège, protéger les secrets, utiliser le MFA lorsque prévu, contrôler les permissions, sécuriser BitLocker et sensibiliser l'utilisateur au verrouillage et à la confidentialité.