

Règles de sécurité des comptes

Modèle modifiable pour les salariés et l'informatique. Convenez de la protection, de la récupération et de la fermeture des comptes. Adaptez-le à vos systèmes, responsabilités et règles internes avant diffusion.

Organisation / périmètre : _____

Responsable / validation / prochaine revue : _____

Utiliser des comptes individuels

Ne partagez pas les comptes personnels. Limitez les droits à la tâche. Séparez les comptes d'administration des usages quotidiens.

Gérer les mots de passe en sécurité

Pour chaque service, utilisez un mot de passe long et différent, généré et stocké dans le gestionnaire autorisé. Protégez le mot de passe principal et les moyens de récupération.

Configurer une MFA adaptée

Activez une authentification multifacteur forte avec l'informatique. Lorsque c'est possible, privilégiez des solutions résistantes à l'hameçonnage : clés d'accès FIDO2 ou clés de sécurité correctement configurées, avec code PIN ou biométrie.

Vérifier les demandes de connexion

N'approuvez que les demandes déclenchées par vous et correspondant à votre connexion. Refusez et signalez les demandes inattendues. Ne donnez à aucun appelant votre mot de passe, code à usage unique ou code de récupération.

Préparer la récupération à l'avance

Convenez d'un facteur de secours et d'une procédure de récupération autorisée. Protégez les codes selon les règles internes, pas uniquement derrière le compte bloqué. Ne saisissez jamais de code dans ce modèle.

Signaler les changements et anomalies

Signalez rapidement les appareils perdus, connexions suspectes et droits devenus inutiles. En cas de compromission possible, l'informatique coordonne aussi la revue des sessions, facteurs et accès applicatifs.

Contacts internes

Gestionnaire de mots de passe autorisé / guide : _____

Contact informatique / secours en cas de blocage : _____

Emplacement des consignes de récupération sans codes : _____

Liste de contrôle pour récupérer un compte

Utilisez la procédure convenue uniquement pour vos propres comptes ou ceux que vous êtes explicitement habilité à administrer. Associez l'équipe informatique responsable ; ce modèle n'autorise pas la prise de contrôle d'un compte.

Service concerné / dossier interne / heure : _____

Contact joignable / identité vérifiée par : _____

Identifier la situation

Appareil perdu, facteur défaillant ou connexion suspecte ? En cas de compromission possible, utilisez immédiatement le canal interne de gestion d'incident ; changer le mot de passe peut ne pas suffire.

Utiliser un contact connu

Contactez l'informatique au numéro enregistré ou via le portail connu. N'utilisez pas d'annonces de recherche non vérifiées, de numéros de rappel inconnus ni de liens inattendus.

Laisser l'informatique vérifier l'identité

Suivez la procédure d'identification convenue avec l'informatique. L'urgence ne remplace pas la vérification. Ne communiquez pas de code MFA à un appelant.

Utiliser une solution de secours autorisée

Utilisez un facteur de secours ou la récupération sécurisée autorisée. Faites révoquer les facteurs perdus et enregistrer les nouveaux dans des conditions contrôlées.

Examiner les autres accès en cas de soupçon

L'informatique contrôle notamment les sessions actives, jetons, autorisations applicatives, moyens de récupération et règles de messagerie. Bloquez ou révoquez les accès concernés selon les besoins.

Consigner la réalisation

Testez les contacts et la connexion, actualisez le secours et documentez les actions dans le dossier interne. N'y copiez aucun secret.

Actions / responsable / date de réalisation : _____

Résultat du test de connexion / prochaine revue : _____

Accorder modifier et révoquer les accès

Pour les arrivées, changements de poste et départs. Les RH, le responsable métier et l'informatique conviennent des validations, dates de mise en œuvre et revues. Ajoutez des lignes pour les autres services.

Personne ou référence interne / fonction : _____

Motif / date d'effet / validation : _____

Service ou compte	Accès et action nécessaires	Réalisation et preuve
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

À l'arrivée ou au changement de poste

Vérifiez l'identité et la validation, accordez uniquement les accès nécessaires et préparez la MFA et la récupération. Retirez explicitement les anciens droits après un changement de rôle. Notez l'expiration et la prochaine revue ; validez séparément les privilèges d'administration.

Au départ

À l'heure approuvée, désactivez les comptes et accès distants, révoquez sessions et jetons et vérifiez les facteurs MFA. Incluez les services hors connexion centralisée. Contrôlez appareils, clés et secrets partagés ; renouvelez ces derniers si nécessaire. Transférez données et responsabilités selon les règles internes. Traitez séparément conservation et suppression.

Réalisation vérifiée par / date / points ouverts : _____

Utilisation et sources

Modèles originaux de Paragamix GmbH. Utilisation interne, adaptation et partage avec les clients gratuits. Un lien vers la source est apprécié, sans être obligatoire. Ni audit d'accès complet ni attestation de conformité. N'inscrivez jamais de mots de passe, jetons ou codes de récupération.

[NCSC sur les identités et accès](#) | [MFA](#) | [Gestionnaires de mots de passe \(anglais\)](#)

[Version actuelle et cas pratiques](#)