					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P34S					Titre du document : **Politique relative aux appareils mobiles et au BYOD**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Clauses 5.1, 5.2, 6.1, 6.2, 8	Exigences générales du SMSI et mesures de sécurité applicables aux appareils mobiles et au BYOD
ISO/IEC 27002:2022	Mesures 5.10–5.13	Mesures détaillées applicables aux appareils mobiles, au BYOD et à l'accès à distance
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Contrôles applicables aux équipements, aux supports et à la configuration
RGPD de l'UE	Article 5(1)(f)	Protection des données à caractère personnel et des terminaux mobiles
NIS2 de l'UE	Article 21(2)(d)	Protection des équipements essentiels à l'activité, y compris dans le cadre du BYOD
DORA de l'UE	Articles 9, 10	Risques liés aux TIC et continuité d'activité applicables aux terminaux mobiles
COBIT 2019	APO13, DSS01, DSS05	Gouvernance des systèmes d'information, opérations et contrôles des services de sécurité

1. Objet

1.1. La présente politique définit les exigences de sécurité obligatoires applicables à l'utilisation des appareils mobiles, y compris les smartphones, tablettes et ordinateurs portables, pour accéder aux informations, systèmes ou services de l'entreprise.

1.2. Elle encadre également l'usage du Bring Your Own Device (BYOD) afin de garantir la protection des données clients et des données métier, indépendamment du propriétaire de l'appareil.

1.3. La politique impose des mesures de protection cohérentes pour les accès mobiles, contribue à l'atteinte des objectifs de certification ISO/IEC 27001 et prévient la perte de données ou la compromission résultant de la perte, du vol ou d'un usage inapproprié des terminaux mobiles.

1.4. Elle exige la mise en œuvre de mesures de protection techniques et procédurales pour l'usage mobile dans les PME ne disposant pas d'équipes informatiques dédiées, y compris dans les environnements de télétravail et les services cloud.

2. Champ d’application

2.1. La présente politique s'applique à l'ensemble des employés, prestataires, stagiaires et fournisseurs de services qui :

2.1.1. utilisent un appareil mobile pour accéder aux données ou systèmes de l'entreprise, les traiter ou les stocker ;

2.1.2. se connectent aux services de l'entreprise, y compris la messagerie, les dossiers partagés, les applications cloud ou les systèmes internes via un réseau privé virtuel (VPN).

2.2. Elle couvre :

2.2.1. tous les appareils mobiles : smartphones, tablettes et ordinateurs portables (fournis par l'entreprise ou appareils personnels BYOD) ;

2.2.2. tous les systèmes d'exploitation (par exemple iOS, Android, Windows, macOS) ;

2.2.3. tous les lieux d'utilisation (bureau, domicile, à distance, espaces publics).

2.3. La politique s'applique à l'ensemble des environnements de travail et doit être mise en œuvre indépendamment du propriétaire de l'appareil.

3. Objectifs

3.1. Prévenir la perte de données : garantir que l'utilisation mobile n'expose pas les données sensibles de l'entreprise ou des clients à un accès non autorisé, au vol ou à un usage abusif.

3.2. Définir des règles claires pour le BYOD : fixer des conditions opposables pour l'utilisation d'appareils personnels à des fins professionnelles, avec des mesures de protection juridiques et techniques appropriées.

3.3. Soutenir la conformité réglementaire : satisfaire aux exigences issues d'ISO/IEC 27001, du RGPD, de NIS2 et des autres obligations légales au moyen de pratiques de sécurité mobile opposables.

3.4. Réduire le risque opérationnel : limiter la probabilité de perturbation des opérations causée par l'usage abusif, la compromission ou la défaillance d'un appareil mobile.

3.5. Préserver la confiance des clients : démontrer aux clients et partenaires que leurs données demeurent protégées, y compris lorsqu'elles sont consultées depuis des appareils mobiles ou personnels.

4. Rôles et responsabilités

4.1. Directeur général (DG) :

4.1.1. assume la responsabilité de la présente politique ;

4.1.2. approuve tout usage d'appareils mobiles et tout accès BYOD aux systèmes de l'entreprise ;

4.1.3. veille à ce que les accords BYOD soient signés, conservés et suivis ;

4.1.4. vérifie que les prestataires informatiques externes appliquent les mesures de protection mobile requises.

4.2. Personnel désigné ou support informatique :

4.2.1. assiste à la mise en service, à l'enregistrement et à la configuration des appareils mobiles utilisés à des fins professionnelles ;

4.2.2. met en œuvre les contrôles d'accès liés à la mobilité, les restrictions applicatives et les règles de surveillance ;

4.2.3. apporte son support dans le cadre de la réponse aux incidents liés aux appareils mobiles (appareils perdus, volés ou compromis).

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exigences de revue et de mise à jour

9.1. Revue annuelle

9.1.1. Le Directeur général (DG) doit revoir la présente politique au moins une fois tous les 12 mois.

9.1.2. La revue doit vérifier le maintien de l'alignement avec les exigences d'ISO/IEC 27001, l'évolution des technologies mobiles et les changements dans les activités de l'entreprise.

9.1.3. Les mises à jour doivent également tenir compte des incidents récents, des résultats d'audit et des évolutions réglementaires (par exemple RGPD, NIS2, DORA).

9.2. Événements déclencheurs d'une revue intermédiaire

9.2.1. La présente politique doit être mise à jour immédiatement si l'un des événements suivants survient :

9.2.1.1. incident majeur de sécurité mobile (par exemple une violation résultant d'un appareil perdu ou compromis) ;

9.2.1.2. changement de plateformes prises en charge ou d'outils de gestion de la mobilité ;

9.2.1.3. évolution légale ou réglementaire affectant l'usage d'appareils personnels ou la protection des données ;

9.2.1.4. introduction de nouvelles applications, de nouveaux services ou de nouveaux outils tiers utilisés sur des appareils mobiles.

9.3. Documentation des changements

9.3.1. Toutes les revues et mises à jour doivent être documentées, y compris la date de revue, les modifications apportées et l'approbation du DG.

9.3.2. Un historique de gestion des versions doit être conservé à des fins d'audit.

9.4. Communication et accès

9.4.1. Le DG doit veiller à ce que l'ensemble des utilisateurs (employés, prestataires, tiers) soient informés des changements.

9.4.2. Les versions mises à jour doivent être facilement accessibles, par exemple dans des dossiers partagés ou sur des plateformes internes.

10. Politiques associées et articulations

10.1. La présente politique fait partie de l'ensemble des politiques de sécurité de l'information de la PME et doit être mise en œuvre conjointement avec les documents suivants :

10.1.1. P4S – Politique de contrôle d'accès : définit les exigences applicables à la gestion des accès sécurisés aux systèmes, y compris ceux accessibles depuis des appareils mobiles. Elle impose l'hygiène des mots de passe et les contrôles de session.

10.1.2. P8S – Politique de sensibilisation et de formation à la sécurité de l'information : garantit que les utilisateurs reçoivent une formation sur l'utilisation sécurisée des appareils mobiles, le signalement des incidents et les conditions du BYOD.

10.1.3. P17S – Politique de protection des données et de la vie privée : établit un traitement conforme au RGPD des données à caractère personnel et des données de l'entreprise sur les plateformes mobiles, en particulier lorsque des appareils personnels sont utilisés à des fins professionnelles.

10.1.4. P9S – Politique de télétravail : s'articule avec les exigences d'utilisation mobile lors du travail hors site ou à domicile, y compris les mesures de protection relatives à l'usage des appareils et à l'accès réseau.

10.1.5. P30S – Politique de réponse aux incidents : fournit le cadre de réponse applicable aux incidents liés aux appareils mobiles, y compris les appareils compromis ou perdus.

10.2. Ces politiques associées constituent ensemble un dispositif complet de contrôles de sécurité pour les appareils mobiles dans les PME ne disposant pas de personnel informatique dédié, afin de garantir l'opposabilité, la transparence et la capacité à répondre aux exigences de certification.

11. Normes et référentiels de référence

11.1. La présente politique contribue à l'alignement global avec les normes de sécurité et de conformité suivantes :

11.2. ISO/IEC 27001 :

11.2.1. Clause 5.1 – Leadership and Commitment : garantit la supervision par la direction et la responsabilité relatives aux accès mobiles et au BYOD ;

11.2.2. Clause 6.1 – Actions to Address Risks : exige l'évaluation et le traitement des risques de sécurité mobile ;

11.2.3. Clause 8.1 – Operational Planning and Control : impose des procédures cohérentes d'accès mobile afin de protéger les données métier.

11.3. ISO/IEC 27002 :

11.3.1. Mesures 5.10 (Use of Mobile Devices), 5.11 (Teleworking), 5.12 (Remote Access) et 5.13 (BYOD) : fournissent des lignes directrices de mise en œuvre pour gérer les risques liés aux appareils dans le contexte d'une petite entreprise.

11.4. NIST SP 800-53 Rev.5 :

11.4.1. AC-19 – Access Control for Mobile Devices : exige des paramètres de sécurité pour l'usage autorisé des appareils mobiles ;

11.4.2. AC-20 – Use of External Systems : encadre les risques liés au BYOD et à l'accès à distance ;

11.4.3. CM-6 – Configuration Settings : impose des paramètres sécurisés par défaut et adaptés sur les plateformes mobiles ;

11.4.4. MP-7 – Media Use : traite de l'usage approprié et des restrictions applicables au stockage mobile et à l'accès aux données.

11.5. RGPD de l'UE (2016/679) :

11.5.1. Article 5(1)(f) – Intégrité et confidentialité : exige la protection des données au moyen d'une sécurité appropriée des données à caractère personnel, en particulier sur les plateformes mobiles ;

11.5.2. Article 32 – Sécurité du traitement : impose l'utilisation de mesures techniques et organisationnelles appropriées pour sécuriser les données consultées ou stockées sur des appareils mobiles.

11.6. Directive NIS2 de l'UE (2022/2555) :

11.6.1. Article 21(2)(d) – Mesures de sécurité des équipements : exige des contrôles de sécurité pour le matériel et les logiciels utilisés pour accéder à des systèmes essentiels à l'activité, y compris les appareils personnels.

11.7. DORA de l'UE (2022/2554) :

11.7.1. Article 9 – ICT Risk Management Framework : exige la protection des terminaux mobiles utilisés pour les communications métier critiques et les services cloud ;

11.7.2. Article 10 – ICT Business Continuity : impose le maintien d'un accès sécurisé aux systèmes métier, y compris en cas de perturbation ou de télétravail.

11.8. COBIT 2019 :

11.8.1. APO13 – Manage Security : exige que l'organisation mette en œuvre des politiques relatives aux appareils mobiles et au BYOD alignées sur le niveau de risque de l'entreprise ;

11.8.2. DSS01 – Manage Operations : garantit la mise en œuvre technique de mécanismes d'accès sécurisés ;

11.8.3. DSS05 – Manage Security Services : encadre l'implication des tiers dans le maintien d'environnements mobiles sécurisés et la coordination de la réponse aux incidents.