					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P34					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	5.2, 6.1, 7.5, 8	Applique les contrôles de sécurité et les exigences de conformité
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Fournit des contrôles détaillés pour la gestion des appareils mobiles
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Contrôle d'accès, accès à distance, configuration et exigences de sécurité pour les usages mobiles
RGPD de l'UE	5(1)(f), 25, 32	Exigences obligatoires en matière de protection de la vie privée, de chiffrement des données et de sécurité du traitement
NIS2 de l'UE	21(2)(d)	Mesures techniques et organisationnelles de protection des accès mobiles
DORA de l'UE	9, 10	Gestion des risques liés aux TIC et exigences de sécurité applicables aux usages mobiles
COBIT 2019	APO13.02, DSS01.04, BAI09	Plans de sécurité de l'information, configuration des actifs et contrôles pour les environnements mobiles

1. Objet

1.1 La présente politique définit les exigences de sécurité, de conformité et d'exploitation applicables à l'utilisation des appareils mobiles et des technologies personnelles (BYOD – Bring Your Own Device) lors de l'accès aux systèmes, applications ou données de l'organisation.

1.2 Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations de l'entreprise consultées ou traitées au moyen de terminaux mobiles, y compris les smartphones, tablettes, ordinateurs portables et appareils hybrides.

1.3 Elle impose également les contrôles techniques et procéduraux requis pour atténuer les risques tels que la fuite de données, l'accès non autorisé, la perte ou le vol d'appareil, ainsi que la compromission d'applications mobiles.

1.4 La présente politique soutient la conformité réglementaire et contractuelle tout en permettant un usage sécurisé des appareils mobiles par les employés, les prestataires et les tiers autorisés.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble du personnel — y compris les employés, prestataires, stagiaires et fournisseurs de services tiers — qui utilisent des appareils mobiles pour accéder aux données, systèmes, applications ou plateformes de communication de l'entreprise.

2.2 Elle couvre tous les équipements informatiques mobiles, y compris notamment :

2.2.1 les smartphones et tablettes (iOS, Android, etc.) ;

2.2.2 les ordinateurs portables et ultrabooks (Windows, macOS, Linux) ;

2.2.3 les objets connectés et appareils intelligents hybrides capables de synchroniser des données.

2.3 Elle s'applique que l'appareil soit la propriété de l'entreprise ou personnel dans le cadre d'un accord BYOD.

2.4 La politique couvre tous les vecteurs d'accès, y compris les réseaux privés virtuels (VPN), les bureaux virtuels, les applications cloud, la messagerie, les plateformes de collaboration (par exemple SharePoint, Teams) et les outils de synchronisation de fichiers (par exemple OneDrive, Dropbox lorsqu'ils sont autorisés).

2.5 Elle couvre les usages en télétravail, sur site, en déplacement ou dans le cadre d'organisations de travail hybrides.

3. Objectifs

3.1 Réduire le risque de compromission, de fuite ou de perte de données lié à une utilisation non sécurisée des appareils mobiles.

3.2 Imposer des contrôles de sécurité cohérents et opposables sur l'ensemble des terminaux mobiles, quel que soit le modèle de propriété (entreprise ou BYOD).

3.3 Garantir que l'utilisation des appareils mobiles est conforme à l'ISO/IEC 27001 et aux autres référentiels réglementaires applicables à la protection des données, à la sécurité de l'information et à la cybersécurité.

3.4 Permettre l'intégration sécurisée des appareils mobiles dans les processus opérationnels, de communication et de collaboration de l'organisation.

3.5 Définir clairement les responsabilités et les processus relatifs à la gestion des appareils mobiles (MDM), y compris l'enrôlement des appareils, l'effacement à distance, le chiffrement, l'authentification et la surveillance.

3.6 Protéger les droits à la vie privée des personnes utilisant leurs propres appareils tout en préservant les données sensibles de l'organisation.

4. Rôles et responsabilités

4.1 Responsable de la sécurité des systèmes d'information (RSSI) / responsable de la sécurité de l'information

4.1.1 Définit la politique et les normes techniques applicables aux usages mobiles et au BYOD.

4.1.2 Supervise la conformité, la réponse aux incidents et la gestion des dérogations relatives aux contrôles applicables aux appareils mobiles.

4.1.3 Se coordonne avec les Ressources humaines et les Affaires juridiques afin de garantir une mise en œuvre juridiquement recevable et cohérente à l'échelle de l'organisation.

4.2 Administrateur informatique / administrateur MDM

4.2.1 Gère l'attribution des accès, l'enrôlement des appareils et leur configuration au moyen de solutions MDM.

4.2.2 Met en œuvre les contrôles au niveau des appareils (par exemple chiffrement, codes PIN, contrôles applicatifs).

4.2.3 Réalise l'effacement à distance, le verrouillage des appareils et la révocation des accès lorsque nécessaire.

[... 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 La présente politique doit faire l'objet d'une revue au moins annuelle par le RSSI ou le responsable de la sécurité de l'information désigné afin de garantir son alignement avec :

9.1.1 les évolutions des plateformes de systèmes d'exploitation mobiles, des technologies MDM ou des normes d'authentification ;

9.1.2 les évolutions réglementaires ou contractuelles affectant la protection des données mobiles (par exemple RGPD, DORA, NIS2) ;

9.1.3 les révisions des ensembles de contrôles ISO/IEC 27001:2022, ISO/IEC 27002:2022 ou NIST SP 800-53 Rev.5 ;

9.1.4 les retours issus des audits, des revues post-incident ou des signalements du personnel.

9.2 Des revues intermédiaires peuvent être déclenchées par :

9.2.1 des incidents de sécurité impliquant des appareils mobiles ou des plateformes BYOD ;

9.2.2 une notification du fournisseur relative à des vulnérabilités à haut risque affectant les plateformes prises en charge ;

9.2.3 l'introduction de nouvelles applications mobiles ou plateformes de collaboration utilisées pour les opérations métier.

9.3 Les mises à jour de la politique doivent être :

9.3.1 documentées dans l'historique des versions de la politique ;

9.3.2 communiquées à l'ensemble du personnel et aux prestataires concernés ;

9.3.3 reconfirmées au moyen d'une attestation de prise de connaissance mise à jour pour tous les utilisateurs BYOD.

9.4 Toutes les revues et mises à jour doivent être formellement approuvées par la direction générale et consignées dans le registre des modifications de politique.

10. Politiques associées et articulations

10.1 La présente politique est articulée avec plusieurs politiques clés du cadre SMSI de l'organisation. Les principales articulations sont les suivantes :

10.1.1 P1 – Politique de sécurité de l'information : établit les principes généraux de gouvernance applicables à l'ensemble des contrôles de sécurité de l'information, y compris ceux encadrant l'utilisation des appareils mobiles.

10.1.2 P3 – Politique d'utilisation acceptable : définit les comportements autorisés et les restrictions liés à l'usage des technologies, directement applicables aux accès mobiles et au BYOD.

10.1.3 P9 – Politique de télétravail : définit des obligations de sécurité complémentaires pour les environnements de travail mobiles, en complément des contrôles spécifiques aux appareils mobiles prévus par la présente politique.

10.1.4 P13 – Politique de classification et d'étiquetage des données : encadre la manière dont les données présentes sur les appareils mobiles doivent être traitées selon leur niveau de classification, avec un impact sur le stockage, le transfert et l'application du chiffrement.

10.1.5 P22 – Politique de journalisation et de surveillance : soutient la collecte et la revue des journaux d'accès mobiles afin de détecter les anomalies ou les manquements.

10.1.6 P30 – Politique de réponse aux incidents : encadre la gestion et l'escalade des incidents liés au mobile (par exemple perte d'appareil, accès non autorisé).

10.1.7 P33 – Politique d'audit et de surveillance de la conformité : fournit la base des vérifications périodiques de la conformité en matière de sécurité mobile, y compris le respect de la politique BYOD.

11. Normes et référentiels de référence

11.1 La présente politique est alignée sur des référentiels de cybersécurité reconnus au niveau international et sur des obligations légales visant à garantir l'usage sécurisé des appareils mobiles et des technologies personnelles (BYOD) dans les environnements d'entreprise.

11.2 ISO/IEC 27001 :

11.2.1 Clause 5.10 – Utilisation acceptable des actifs de l'entreprise et de l'information : impose des contrôles relatifs à l'usage responsable des actifs de l'entreprise, y compris les appareils mobiles.

11.2.2 Clause 5.11 – Télétravail : encadre les pratiques sécurisées lors de l'accès aux systèmes en dehors des locaux de l'entreprise.

11.2.3 Clause 5.12 – Utilisation des appareils mobiles : impose des contrôles fondés sur les risques pour les terminaux mobiles et les configurations BYOD.

11.2.4 Clause 5.13 – Transfert d'information : impose la protection des informations transférées via des canaux mobiles.

11.3 ISO/IEC 27002:2022 – Mesures 5.10 à 5.13 :

11.3.1 Les mesures de l'annexe A 5.10 à 5.13 précisent la manière dont l'accès mobile, le chiffrement, la surveillance et l'atténuation des pertes doivent être mis en œuvre dans un SMSI. Elles fournissent des orientations détaillées de mise en œuvre pour sécuriser les terminaux mobiles, imposer la conteneurisation, surveiller l'intégrité des appareils et garantir des configurations BYOD respectueuses de la vie privée.

11.4 NIST SP 800-53 Rev.5 :

11.4.1 AC-19 – Contrôle d'accès pour les appareils mobiles : définit des protections de référence, y compris le chiffrement, l'authentification et la mise en œuvre du MDM.

11.4.2 AC-17 – Accès à distance : impose une authentification sécurisée et des protections de session pour les utilisateurs mobiles à distance.

11.4.3 CM-7 – Principe de fonctionnalité minimale : soutient la suppression des applications et fonctionnalités inutiles des terminaux mobiles afin de réduire le risque.

11.4.4 MP-5 – Protection du transport des supports : encadre la transmission sécurisée des données depuis les systèmes mobiles vers des destinations externes ou cloud.

11.4.5 SC-12 – Établissement des clés cryptographiques : impose l'utilisation de protocoles cryptographiques sécurisés pour les communications et le stockage mobiles.

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

11.5.1 Article 5(1)(f) – Intégrité et confidentialité : impose aux organisations de protéger les données à caractère personnel présentes sur les appareils mobiles contre tout accès non autorisé ou illicite.

11.5.2 Article 25 – Protection des données dès la conception et par défaut : impose d'intégrer les exigences de vie privée dans les processus BYOD et MDM.

11.5.3 Article 32 – Sécurité du traitement : impose des contrôles fondés sur les risques (par exemple chiffrement, authentification, contrôle d'accès) pour les données à caractère personnel sur les plateformes mobiles.

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

11.6.1 Article 21(2)(d) : impose que l'accès mobile aux systèmes et informations critiques soit protégé par des mesures techniques et organisationnelles appropriées, telles que le contrôle des terminaux, le chiffrement et la surveillance.

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

11.7.1 Article 9 – Cadre de gestion des risques liés aux TIC : impose aux entités du secteur financier d'atténuer les risques liés au mobile et à l'accès à distance dans le cadre de la résilience opérationnelle.

11.7.2 Article 10 – Exigences de sécurité des systèmes TIC : impose une architecture mobile sécurisée, des mécanismes de surveillance et de réponse pour les cybermenaces provenant d'appareils mobiles.

11.8 COBIT 2019 :

11.8.1 APO13.02 – Établir et maintenir un plan de sécurité de l'information : impose que l'utilisation des appareils mobiles, y compris le BYOD, soit intégrée aux stratégies de sécurité de l'organisation.

11.8.2 DSS01.04 – Gérer la configuration et l'intégrité des actifs : s'applique au contrôle de configuration et au déploiement sécurisé des appareils mobiles.

11.8.3 BAI09.01 – Établir et maintenir des contrôles : soutient la mise en œuvre de mesures de protection techniques et procédurales pour des opérations mobiles et distantes sécurisées.