					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P20S					Titre du document : **Politique de protection des terminaux contre les logiciels malveillants**							
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	Clause 8	Contrôles opérationnels de protection contre les logiciels malveillants
ISO/IEC 27002:2022	Mesure 8	Mesures de contrôle pour la protection des terminaux
NIST SP 800-53 Rev.5	SI-3, SI-4	Protection contre le code malveillant et réponse aux incidents
NIS2 (UE)	Articles 21(2)(d), (e)	Protection contre les logiciels malveillants et gestion des risques pour les entités essentielles et importantes
DORA (UE)	Articles 10(1), 15	Résilience opérationnelle et vérification des tiers
COBIT 2019	DSS05.02, DSS05.04	Protection des terminaux et des réseaux et surveillance
RGPD (UE)	Articles 32(1)(b), 33	Mesures techniques et organisationnelles et notification des violations

1. Objet

1.1 La présente politique définit les exigences minimales techniques, procédurales et comportementales applicables à la protection de tous les terminaux — tels que les ordinateurs portables, postes de travail, appareils mobiles et supports amovibles — contre les logiciels malveillants, y compris les virus, rançongiciels, logiciels espions, rootkits et autres menaces associées.

1.2 Elle vise à garantir que les terminaux sont équipés, maintenus et utilisés de manière à réduire le risque d'infection par des logiciels malveillants, de propagation et de compromission des systèmes.

1.3 L'organisation reconnaît que les terminaux constituent des points d'entrée fréquents pour les logiciels malveillants et doivent, à ce titre, faire l'objet d'un durcissement, d'une surveillance et d'une protection fondés sur une défense multicouche.

1.4 La présente politique soutient les objectifs de certification ISO/IEC 27001:2022 de l'organisation et s'aligne sur le règlement général sur la protection des données (RGPD), la directive NIS2, le règlement sur la résilience opérationnelle numérique du secteur financier (DORA) et les autres référentiels applicables.

2. Champ d'application

2.1 La présente politique s'applique à :

2.1.1 Tous les terminaux de l'organisation, y compris les postes de travail, ordinateurs portables, tablettes, téléphones mobiles et terminaux de point de vente

2.1.2 Les appareils personnels (BYOD) utilisés pour accéder aux applications métier ou aux données

2.1.3 Les supports de stockage amovibles tels que les clés USB et les disques durs externes

2.1.4 Tous les systèmes d’exploitation, logiciels de terminaux ou outils de communication exécutés sur ces plateformes

2.2 Elle s’applique également à :

2.2.1 Le personnel interne, les prestataires, les stagiaires et les fournisseurs de services managés (MSP)

2.2.2 Les appareils utilisés sur site, à distance ou dans le cadre de modalités de travail hybrides

2.2.3 Les terminaux connectés au cloud ou hors ligne stockant des données métier ou des données à caractère personnel

3. Objectifs

3.1 Prévenir les infections par des logiciels malveillants et leur propagation au sein des systèmes internes, des terminaux utilisateurs et des connexions externes

3.2 Détecter et contenir rapidement les menaces liées aux logiciels malveillants à l’aide de technologies automatisées de sécurité des terminaux et de circuits d’escalade définis

3.3 Garantir que seuls des appareils autorisés, sécurisés et supervisés sont utilisés pour accéder aux informations de l’entreprise

3.4 Définir des responsabilités claires pour le personnel ainsi que des règles de comportement utilisateur afin de réduire le risque d’incidents liés aux logiciels malveillants

3.5 Maintenir des enregistrements traçables et auditables des détections de logiciels malveillants, des réponses apportées et de la conformité à la politique

3.6 Protéger les données à caractère personnel et les données métier contre toute compromission due à des logiciels malveillants au moyen de stratégies de défense en profondeur

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Est responsable de la présente politique et veille à la disponibilité de ressources suffisantes pour la protection des terminaux

4.1.2 Approuve les logiciels antivirus, les outils de gestion des appareils mobiles (MDM) et les règles d’accès des tiers

4.1.3 Examine les rapports d’incidents liés aux logiciels malveillants, les synthèses d’impact et les notifications de violation impliquant des terminaux

4.2 Prestataire de support informatique / administrateur informatique interne

4.2.1 Sélectionne et déploie les solutions antivirus, antimalware et de détection et réponse sur les terminaux (EDR)

4.2.2 Veille à l’application cohérente des mises à jour et à la conservation des journaux

4.2.3 Traite les alertes liées aux logiciels malveillants, isole les systèmes infectés et conduit les actions de remédiation

4.2.4 Met en œuvre les contrôles relatifs à l’utilisation des supports USB et des périphériques externes

[... 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 Exigence de revue annuelle

9.1.1 La présente politique doit faire l’objet d’une revue formelle au moins une fois par an par le directeur général, en coordination avec le prestataire de support informatique et le coordinateur à la protection des données

9.2 Mises à jour déclenchées par événement

9.2.1 La politique doit également être mise à jour lorsque :

9.2.1.1 Une nouvelle menace majeure liée aux logiciels malveillants ou une épidémie cible les terminaux utilisés par l'organisation

9.2.1.2 Les outils antivirus ou EDR sont modifiés, mis à niveau ou remplacés

9.2.1.3 Un incident lié à un logiciel malveillant révèle des faiblesses dans le champ d'application de la politique ou dans sa mise en œuvre

9.2.1.4 Les exigences légales ou réglementaires (par exemple RGPD, DORA, NIS2) évoluent

9.3 Gestion des versions et communication

9.3.1 Toute modification de la politique doit être documentée avec un numéro de version, une date et un résumé des changements

9.3.2 Le personnel doit être informé des mises à jour, en particulier lorsqu'elles modifient les exigences opérationnelles ou comportementales

9.3.3 Les versions antérieures doivent être conservées dans les archives de la politique pendant au moins 3 ans afin de répondre aux besoins d'audit

10. Politiques associées et articulations

10.1 La présente politique doit être mise en œuvre conjointement avec les politiques PME suivantes :

10.1.1 P9S – Politique de télétravail : garantit que les exigences de protection des terminaux sont appliquées sur les appareils utilisés hors site ou dans des contextes hybrides

10.1.2 P12S – Politique de gestion des actifs : appuie le suivi et le contrôle de tous les terminaux, afin de garantir que seuls des appareils autorisés et protégés sont utilisés

10.1.3 P17S – Politique de protection des données et de la vie privée : renforce la prévention contre les logiciels malveillants en tant que contrôle essentiel de protection des données afin de protéger les données à caractère personnel et les données sensibles contre toute compromission

10.1.4 P22S – Politique de journalisation et de surveillance : établit les exigences de journalisation des événements liés aux logiciels malveillants et de maintien de la visibilité sur les alertes afin de permettre une réponse précoce

10.1.5 P30S – Politique de réponse aux incidents : définit les étapes d'escalade, de confinement et de notification externe si un logiciel malveillant entraîne une compromission des données ou une perturbation opérationnelle

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Exige la mise en œuvre de contrôles opérationnels pour réduire les risques tels que les attaques par logiciels malveillants

11.2 ISO/IEC 27002

11.2.1 Mesure 8.7 – Décrit les pratiques de contrôle contre les logiciels malveillants, y compris l'antivirus, l'analyse en temps réel, les mises à jour et la formation des utilisateurs

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Exige le déploiement de mécanismes de protection contre le code malveillant sur l'ensemble des terminaux

11.3.2 SI-4 – Imposent des actions de surveillance, détection, analyse et réponse face aux menaces et alertes au niveau des terminaux

11.4 RGPD (UE)

11.4.1 Article 32(1)(b) – Exige des contrôles techniques et organisationnels (tels que l'antivirus) pour protéger les données à caractère personnel

11.4.2 Article 33 – Imposent la notification d'une violation lorsque des logiciels malveillants compromettent l'intégrité, la confidentialité ou la disponibilité des données

11.5 Directive NIS2 de l'UE

11.5.1 Article 21(2)(d) – Exige des mesures pour prévenir les menaces liées aux logiciels malveillants et y répondre au sein des entités essentielles et importantes

11.5.2 Article 21(2)(e) – Imposent des stratégies de gestion des risques de cybersécurité à plusieurs niveaux, y compris la protection des terminaux contre les logiciels malveillants

11.6 DORA (UE)

11.6.1 Article 10(1) – Exige que les systèmes TIC soient protégés contre les logiciels malveillants et autres menaces au titre de la résilience opérationnelle

11.6.2 Article 15 – Imposent aux organisations financières de vérifier la protection contre les logiciels malveillants chez les prestataires de services tiers

11.7 COBIT 2019

11.7.1 DSS05.02 – Met l'accent sur les mesures de protection visant à défendre les terminaux et les réseaux contre les menaces liées aux logiciels malveillants

11.7.2 DSS05.04 – Appuie la surveillance et l'alerte relatives aux événements de sécurité liés aux logiciels malveillants dans le cadre des opérations courantes