| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insérez ici la dénomination de l'entité juridique enregistrée | | | | | | | |
| Numéro du document :<br>P20 | | | | | Titre du document :<br>**Politique de protection des terminaux contre les logiciels malveillants** | | | | | | | |
| Version :<br>1.0 | | Date d'entrée en vigueur :<br>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 | La protection des terminaux et les contrôles contre les logiciels malveillants sont requis pour atteindre les objectifs du SMSI |
| ISO/IEC 27002:2022 | Mesures 8.7, 8 | Fournit des contrôles techniques et des orientations relatifs à la protection antimalware, à la sécurité des terminaux et à la gestion des incidents |
| NIST SP 800-53 Rev.5 | SI-3, SI-4, CM-6 | Définit les exigences relatives à la protection contre le code malveillant, à la surveillance centralisée et aux configurations de référence |
| RGPD de l'UE | Article 32 | Impose des mesures techniques appropriées pour protéger les données à caractère personnel, y compris contre les logiciels malveillants |
| NIS2 de l'UE | Article 21(2)(d) | Exige le déploiement de mesures de détection et de prévention des menaces au niveau des terminaux |
| DORA de l'UE | Article 9 | Exige une gestion des risques liés aux TIC pour la protection contre les logiciels malveillants et les menaces transitant par les terminaux |
| COBIT 2019 | DSS05.01, DSS01.04, MEA03 | Couvre la protection, la surveillance et l'évaluation des contrôles appliqués aux terminaux |

## 1. Objet

1.1 La présente politique définit les contrôles obligatoires et les exigences opérationnelles applicables à la protection des terminaux de l'organisation, y compris les postes de travail fixes, les ordinateurs portables, les appareils mobiles et les serveurs, contre les logiciels malveillants et les menaces associées.

1.2 Elle établit les exigences minimales en matière de protection des terminaux, de détection des logiciels malveillants, de confinement, de réponse et de surveillance comportementale, afin de garantir la résilience des systèmes face aux souches de logiciels malveillants courantes et avancées.

1.3 La présente politique contribue directement à la conformité à la clause 8.1 de l'ISO/IEC 27001:2022 et à la mesure 8.7 de l'annexe A, et s'aligne sur les obligations régionales en cybersécurité prévues par le RGPD, NIS2 et DORA.

## 2. Champ d'application

**2.1 La présente politique s'applique à tous les terminaux, y compris :**

2.1.1 les postes de travail fixes, les ordinateurs portables, les appareils mobiles et les instances virtuelles détenus ou administrés par l'organisation ;

2.1.2 les appareils personnels autorisés au titre de la politique BYOD, sous réserve de l'installation d'une solution MDM ou d'un agent de protection du terminal ;

2.1.3 les serveurs et actifs d'infrastructure, y compris les machines virtuelles hébergées dans le cloud et les dispositifs en périphérie du réseau ;

2.1.4 les systèmes d'exploitation, pilotes, services locaux, agents de protection du terminal et contrôles de sécurité installés sur chaque nœud.

**2.2 La présente politique s'applique à l'ensemble du personnel exerçant une responsabilité administrative, technique ou opérationnelle sur un terminal, y compris :**

2.2.1 les employés internes et les prestataires ;

2.2.2 les prestataires de services managés (MSP), les services externalisés de support poste de travail et les administrateurs informatiques tiers ;

2.2.3 les utilisateurs autorisés à exploiter des systèmes portables, des ordinateurs portables avec accès VPN ou un accès mobile aux réseaux de l'organisation.

**2.3 La couverture des menaces au titre de la présente politique comprend notamment :**

2.3.1 les virus, vers, chevaux de Troie, rançongiciels, logiciels espions, rootkits, logiciels publicitaires, enregistreurs de frappe et botnets ;

2.3.2 les logiciels malveillants sans fichier, les charges utiles zero-day, les logiciels malveillants d'élévation de privilèges et les kits d'exploitation de navigateur ;

2.3.3 le code malveillant diffusé via des supports amovibles, des vecteurs d'hameçonnage, des téléchargements furtifs ou des attaques par USB.

## 3. Objectifs

3.1 Protéger l'intégrité, la disponibilité et la confidentialité des systèmes terminaux ainsi que des données qu'ils traitent au moyen de mécanismes fiables de prévention, de détection et de réponse face aux logiciels malveillants.

3.2 Empêcher l'exécution ou la propagation de code malveillant sur les réseaux de l'organisation par l'application de mesures techniques de protection, de configurations de durcissement de référence et de télémétrie en temps réel.

3.3 Intégrer la protection des terminaux aux autres contrôles du SMSI, notamment la gestion des vulnérabilités, le contrôle d'accès, la journalisation et la surveillance, ainsi que la réponse aux incidents.

3.4 Garantir une visibilité continue sur les terminaux au moyen de plateformes de protection administrées de manière centralisée, y compris des agents antivirus/antimalware, des solutions EDR (détection et réponse sur les terminaux) et la télémétrie SIEM.

3.5 Se conformer aux exigences légales, réglementaires et normatives imposant la sécurité des terminaux, par exemple l'article 32 du RGPD, l'article 21 de NIS2 et l'article 9 de DORA.

3.6 Définir les rôles responsables, imposer des SLA de traitement des correctifs et des alertes, et permettre de démontrer la conformité au moyen de la documentation et du reporting.

## 4. Rôles et responsabilités

### 4.1 Responsable de la sécurité des systèmes d'information (RSSI)

4.1.1 Est propriétaire de la présente politique et veille à son alignement avec le SMSI et la stratégie globale de sécurité.

4.1.2 Réalise chaque trimestre une revue des indicateurs de protection des terminaux, des tendances d'incident et de l'efficacité des outils.

4.1.3 Approuve les dérogations et les acceptations du risque résiduel liées à la couverture des terminaux.

**4.2 Responsable de la sécurité des terminaux / Responsable SOC**

4.2.1 Gère les systèmes de protection des terminaux, par exemple AV, EDR et MDM.

4.2.2 Supervise l'application de la politique, le paramétrage de la détection des menaces et les playbooks de réponse.

4.2.3 Tient à jour les statistiques de couverture, les journaux d'incidents liés aux logiciels malveillants et les configurations de référence des alertes.

[ ... 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 annuelle ou lorsqu'un des cas suivants survient :**

9.1.1 des campagnes majeures de logiciels malveillants ou des incidents de sécurité affectant les terminaux ;

9.1.2 l'apparition de nouveaux types de menaces, par exemple des logiciels malveillants sans fichier ou des variantes de rançongiciel, nécessitant une mise à jour des stratégies de détection ou de réponse ;

9.1.3 une évolution significative des plateformes de protection des terminaux ou des architectures d'agents ;

9.1.4 une mise à jour des exigences légales ou réglementaires affectant les contrôles appliqués aux terminaux.

9.2 La revue doit être initiée par le Responsable de la sécurité des terminaux et coordonnée avec les fonctions RSSI, juridique, risques et audit.

9.3 Les révisions approuvées doivent être documentées dans le registre de contrôle documentaire du SMSI, recevoir un nouvel identifiant de version et être communiquées à toutes les parties concernées.

9.4 Les versions remplacées doivent être archivées, soumises à des restrictions d'accès et conservées afin de préserver l'intégrité de la piste d'audit, conformément aux calendriers de conservation du SMSI.

**10. Politiques associées et articulations**

10.1 P1 - Politique de sécurité de l'information. Elle établit les principes fondamentaux applicables à la protection des systèmes, des données et des réseaux. La présente politique décline ces principes au niveau des terminaux au moyen de contrôles techniques et procéduraux contre les logiciels malveillants.

10.2 P4 - Politique de contrôle d'accès. Elle définit les restrictions d'accès des utilisateurs appliquées au niveau des terminaux, y compris les protections contre l'élévation de privilèges et les installations non autorisées de logiciels non évalués.

10.3 P5 - Politique de gestion des changements. Elle garantit que les mises à jour des logiciels de protection des terminaux, des règles de politique ou des configurations d'agents sont soumises à approbation et à des processus de déploiement contrôlés.

10.4 P12 - Politique de gestion des actifs. Elle fournit le référentiel de classification et d'inventaire des actifs nécessaire à la visibilité sur les terminaux, à la couverture des correctifs et à la définition du périmètre de protection contre les logiciels malveillants.

10.5 P22 - Politique de journalisation et de surveillance. Elle permet l'intégration des alertes des terminaux, de l'état de santé des agents et du renseignement sur les menaces dans des systèmes SIEM centralisés pour la détection en temps réel et la traçabilité forensique.

10.6 P30 - Politique de réponse aux incidents. Elle articule les incidents liés aux logiciels malveillants détectés au niveau des terminaux avec des flux de travail normalisés de confinement, d'éradication, d'investigation et de rétablissement, assortis de rôles attribués et de seuils d'escalade.

## 11. Normes et référentiels de référence

### 11.1 ISO/IEC 27001:

11.1.1 Clause 8.1 - Planification et maîtrise opérationnelles : exige la mise en œuvre de contrôles techniques, y compris des mesures de protection des terminaux, afin de maintenir les objectifs du SMSI.

### 11.2 ISO/IEC 27002:2022 - Mesures 8.7, 8 :

11.2.1 Fournit des orientations techniques détaillées sur les mesures antimalware, le déploiement sécurisé de logiciels, la surveillance et la préparation aux incidents pour les environnements terminaux.

### 11.3 NIST SP 800-53 Rev.5 :

11.3.1 SI-3 - Protection contre le code malveillant : exige l'utilisation d'outils antimalware avec analyse en temps réel, analyse à l'accès et analyse comportementale.

11.3.2 SI-4 - Surveillance des systèmes : prend en charge l'intégration de la télémétrie avec des plateformes centralisées de détection.

11.3.3 CM-6 - Paramètres de configuration : renforce les paramètres de contrôle de référence sur les terminaux, y compris l'application des agents de protection.

### 11.4 RGPD de l'UE (2016/679) :

11.4.1 Article 32 - Sécurité du traitement : exige que les organisations mettent en œuvre des mesures techniques appropriées pour protéger les données à caractère personnel, y compris contre les menaces liées aux logiciels malveillants.

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

11.5.1 Article 21(2)(d) : impose aux entités de déployer des mesures de détection et de prévention des menaces, y compris des mécanismes de défense contre les logiciels malveillants au niveau des terminaux.

### 11.6 DORA de l'UE (2022/2554) :

11.6.1 Article 9 - Exigences de gestion des risques liés aux TIC : impose aux entités financières d'adopter des mesures de protection pour prévenir, détecter et traiter les logiciels malveillants et les menaces véhiculées par les terminaux.

### 11.7 COBIT 2019 :

11.7.1 DSS05.01 - Protéger contre les logiciels malveillants : impose la détection et l'atténuation des logiciels malveillants sur l'ensemble des terminaux de l'organisation.

11.7.2 DSS01.04 - Gérer la disponibilité et la capacité : veille à ce que la protection contre les logiciels malveillants reste compatible avec la performance des systèmes et la continuité d'activité.

11.7.3 MEA03 - Surveiller, évaluer et apprécier la conformité : exige un audit périodique des contrôles appliqués aux terminaux et de l'efficacité de la protection.