| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insérez ici la dénomination de l'entité juridique enregistrée | | | | | | | |
| Numéro du document :<br>P21 | | | | | Titre du document :<br>**Politique de sécurité réseau** | | | | | | | |
| 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 | N/A |
| ISO/IEC 27002:2022 | Mesures 8.20-8.22 | N/A |
| NIST SP 800-53 Rev.5 | SC-7, AC-4, SC-32 | N/A |
| RGPD de l'UE | Article 32 | N/A |
| NIS2 de l'UE | Article 21(2)(d) | N/A |
| DORA de l'UE | Article 9 | N/A |
| COBIT 2019 | DSS01.03, DSS05.01, MEA03 | N/A |

**1. Objet**

1.1 La présente politique a pour objet de définir les exigences de l'organisation relatives à la protection de ses réseaux internes et externes contre les accès non autorisés, les interruptions de service, l'interception de données et les usages abusifs.

1.2 Elle impose la protection de l'ensemble de l'infrastructure réseau — physique, virtuelle, cloud et hybride — au moyen de contrôles multicouches tels que la segmentation, l'application de règles de pare-feu, le routage sécurisé et la supervision centralisée.

1.3 Cette politique met en œuvre la clause 8.1 de l'ISO/IEC 27001 ainsi que les mesures de l'annexe A 8.20 à 8.22, afin d'assurer la conformité aux obligations légales et réglementaires applicables au titre de l'article 32 du RGPD, de l'article 21 de NIS2 et de l'article 9 de DORA.

**2. Champ d’application**

**2.1 Cette politique s'applique à tous les réseaux et composants d'infrastructure associés, notamment :**

2.1.1 les routeurs, commutateurs, points d'accès sans fil et pare-feu ;

2.1.2 les réseaux virtuels cloud (par exemple AWS VPC, Azure VNet), les concentrateurs VPN et les systèmes SD-WAN ;

2.1.3 les réseaux LAN internes, les zones démilitarisées (DMZ), les accès à distance et les connexions intersites ou avec des tiers ;

2.1.4 les systèmes de support tels que le DNS, le DHCP, les serveurs proxy et les appliances de supervision.

2.2 La présente politique s'impose à l'ensemble du personnel et aux prestataires tiers qui administrent, configurent, supervisent ou interagissent avec les réseaux de l'organisation, que ce soit sur site ou dans le cloud.

2.3 Tous les systèmes et applications connectés aux réseaux de l'organisation — indépendamment de leur emplacement ou de leur propriété — doivent être conformes aux présentes exigences de sécurité réseau.

**3. Objectifs**

3.1 Garantir la confidentialité, l'intégrité et la disponibilité des données transmises sur les réseaux au moyen de contrôles d'accès robustes, d'un routage sécurisé et de dispositifs de supervision.

3.2 Prévenir les accès non autorisés, les mouvements latéraux et l'exploitation des ressources réseau par la mise en œuvre de la segmentation, du zonage et de la protection périmétrique.

3.3 Maintenir des configurations réseau cohérentes, fondées sur les normes du secteur et le renseignement sur les menaces, afin de se prémunir contre l'évolution des cybermenaces.

3.4 Sécuriser les communications externes, les interconnexions cloud et les accès à distance au moyen de canaux chiffrés, d'une authentification forte et de la vérification de conformité des terminaux.

3.5 Assurer une visibilité sur l'activité réseau au moyen d'une journalisation centralisée, de l'inspection du trafic en temps réel et de mécanismes d'alerte automatisés.

3.6 Garantir la conformité réglementaire en alignant l'ensemble des opérations réseau sur les exigences de l'ISO/IEC 27001:2022, du RGPD, de NIS2, de DORA et de COBIT 2019.

## 4. Rôles et responsabilités

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

4.1.1 Est responsable de la présente politique et veille à sa révision ainsi qu'à son alignement avec la stratégie globale de cybersécurité de l'organisation.

4.1.2 Approuve les modèles de segmentation réseau, les jeux de règles de pare-feu applicables aux systèmes sensibles et les demandes de dérogation.

### 4.2 Responsable de la sécurité réseau / Responsable de la sécurité de l'infrastructure

4.2.1 Gère l'architecture de défense du réseau, y compris les pare-feu, les systèmes de détection/prévention d'intrusion (IDS/IPS), les VPN et le routage sécurisé.

4.2.2 Supervise la segmentation réseau, les affectations de VLAN, le zonage du trafic et la connectivité externe.

4.2.3 Veille à la révision continue du filtrage entrant/sortant et à l'application du modèle Zero Trust à l'ensemble des couches réseau.

[ ... 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 révision annuelle par le Responsable de la sécurité réseau en collaboration avec le RSSI et être mise à jour en fonction :

9.1.1 des menaces émergentes (par exemple nouvelles techniques d'attaque, vulnérabilités de protocole) ;

9.1.2 des évolutions de l'infrastructure (par exemple migrations de systèmes vers le cloud, déploiements SD-WAN) ;

9.1.3 des mises à jour réglementaires ou normatives affectant les protections réseau ;

9.1.4 des constats d'audit, des tendances d'incident ou des dégradations de performance causées par les contrôles.

### 9.2 Des revues doivent également être déclenchées par :

9.2.1 des changements majeurs d'architecture réseau ;

9.2.2 la mise en œuvre de nouvelles plateformes de pare-feu, de VPN ou de réseaux cloud ;

9.2.3 la mise hors service d'actifs clés ou de zones de confiance.

### 9.3 Les mises à jour doivent être consignées dans le registre de contrôle documentaire du SMSI et diffusées :

9.3.1 aux équipes d'infrastructure et d'exploitation réseau ;

9.3.2 au SOC et aux équipes d'ingénierie sécurité ;

9.3.3 aux équipes applicatives ayant des dépendances système sur les flux réseau ;

9.3.4 à tous les prestataires tiers disposant d'une interconnexion active.

9.4 Toutes les versions précédentes de la politique doivent être archivées de manière sécurisée avec des annotations d'historique des modifications afin de préserver l'auditabilité et la traçabilité des changements.

## 10. Politiques associées et articulations

10.1 P1 - Politique de sécurité de l'information. Établit les principes fondamentaux de sécurité et impose des protections multicouches, y compris les contrôles d'accès et les contrôles de menace fondés sur le réseau.

10.2 P4 - Politique de contrôle d'accès. Garantit que la segmentation réseau est appliquée en cohérence avec les rôles utilisateurs, le principe du moindre privilège et les règles d'attribution des droits d'accès.

10.3 P5 - Politique de gestion des changements. Encadre les modifications de pare-feu, les ajustements de règles VPN et les changements de routage au moyen d'un processus documenté et traçable à des fins d'audit.

10.4 P12 - Politique de gestion des actifs. Soutient l'identification et la classification des systèmes en réseau et garantit que tous les actifs connectés sont gérés dans les périmètres définis par la politique.

10.5 P22 - Politique de journalisation et de supervision. Encadre la collecte, la corrélation et la conservation des journaux réseau, y compris les événements de pare-feu, les tentatives d'accès et les détections d'anomalies.

10.6 P30 - Politique de réponse aux incidents. Définit les procédures d'escalade, de confinement et d'éradication en réponse aux menaces ou intrusions transitant par le réseau, telles que les attaques DDoS, les mouvements latéraux ou les accès non autorisés.

## 11. Normes et référentiels de référence

11.1 La présente politique est alignée sur des normes internationales et des exigences réglementaires définissant les opérations réseau sécurisées, la segmentation, la protection périmétrique et l'accès distant sécurisé.

### 11.2 ISO/IEC 27001

11.2.1 Clause 8.1 - Planification et maîtrise opérationnelles : impose l'intégration de contrôles techniques, y compris des protections réseau, dans les processus opérationnels.

### 11.3 ISO/IEC 27002:2022

11.3.1 Mesures 8.20-8.22. Fournit des orientations sur la protection des réseaux, la segmentation des services et la sécurisation des services réseau au moyen du contrôle d'accès et de la supervision.

### 11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Protection des frontières : impose des contrôles périmétriques, la segmentation et des interconnexions sécurisées.

11.4.2 AC-4 - Mise en application des flux d'information : soutient le zonage et les restrictions de trafic fondées sur des règles.

11.4.3 SC-32 - Partitionnement des systèmes d'information : promeut la séparation logique des systèmes d'information.

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

11.5.1 Article 32 - Sécurité du traitement : impose des mesures techniques — telles que les pare-feu et la segmentation — pour protéger les données à caractère personnel.

### 11.6 Directive européenne NIS2 (2022/2555)

11.6.1 Article 21(2)(d) : impose une sécurité efficace des réseaux et des systèmes d'information, la protection périmétrique, la configuration sécurisée et les contrôles de séparation.

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

11.7.1 Article 9 - Gestion des risques liés aux TIC : impose aux entités financières de protéger les réseaux et les interconnexions contre les accès non autorisés, les fuites de données et les perturbations opérationnelles.

**11.8 COBIT 2019**

11.8.1 DSS01.03 - Surveillance de l'infrastructure : impose une maîtrise proactive de l'état du réseau et de la connectivité.

11.8.2 DSS05.01 - Protéger contre les logiciels malveillants : inclut la segmentation et le contrôle des frontières afin de limiter la propagation.

11.8.3 MEA03 - Surveiller, évaluer et apprécier la conformité : renforce l'application de la politique réseau et les évaluations de conformité.