					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P21S					Titre du document : **Politique de sécurité réseau**							
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	-
ISO/IEC 27002:2022	Mesure 8	-
NIST SP 800-53 Rév. 5	AC-4, SC-7	-
RGPD de l'UE	Article 32	-
NIS2 de l'UE	Articles 21(2)(d), (e)	-
DORA de l'UE	Articles 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Objet

1.1. La présente politique a pour objet de garantir que toutes les communications réseau internes et externes sont protégées contre tout accès non autorisé, toute altération, toute écoute illicite ou toute utilisation abusive au moyen de mesures de sécurité clairement définies.

1.2. Elle définit les règles applicables à la conception sécurisée, à l'utilisation et à l'administration de l'infrastructure réseau, y compris les routeurs, les points d'accès sans fil, les connexions d'accès à distance et les réseaux segmentés.

1.3. Elle vise à réduire au minimum l'exposition aux menaces provenant d'Internet, à garantir la confidentialité des données transmises sur les réseaux internes et externes et à maintenir la disponibilité des services critiques.

1.4. Cette politique contribue à la certification ISO/IEC 27001:2022 et participe directement au respect des obligations légales et réglementaires au titre du RGPD, de NIS2 et de DORA, tout en fournissant des garanties techniques aux clients et aux auditeurs.

2. Champ d'application

2.1. La présente politique s'applique à tous les composants du réseau informatique de l'organisation, y compris :

2.1.1. L'infrastructure filaire et sans fil sur les sites de l'entreprise

2.1.2. Les routeurs, commutateurs, points d'accès, pare-feu et passerelles

2.1.3. Les connexions d'accès à distance, y compris les VPN, RDP et tunnels cloud

2.1.4. Les applications cloud accessibles depuis les réseaux internes ou externes

2.1.5. Les équipements connectés au réseau par les employés, les prestataires ou les invités

2.2. Cette politique régit à la fois les segments réseau physiques et logiques, y compris les réseaux invités, les dispositifs de l'Internet des objets (IoT) et les systèmes de back-office.

2.3. La politique couvre l'ensemble du personnel ayant accès au réseau de l'organisation, y compris :

2.3.1. Les employés

2.3.2. Les télétravailleurs et le personnel en mode hybride

2.3.3. Les fournisseurs externes, consultants et prestataires de services

2.3.4. Les invités utilisant un accès Wi-Fi temporaire

3. Objectifs

3.1. Garantir que le réseau de l'organisation est protégé contre les accès non autorisés et les cyberattaques externes

3.2. Mettre en œuvre une segmentation appropriée entre les réseaux de confiance et les réseaux non fiables (par exemple, Wi-Fi invité, accès des fournisseurs)

3.3. Permettre une connectivité à distance sécurisée sans compromettre les systèmes internes

3.4. Prévenir la propagation de logiciels malveillants et l'exfiltration de données via les canaux réseau

3.5. Assurer la surveillance, l'alerte et l'audit de l'activité réseau afin de faciliter la détection des incidents et la conformité

3.6. Garantir que seuls les équipements approuvés et sécurisés sont autorisés à se connecter aux réseaux internes

3.7. Répondre aux obligations au titre de l'ISO 27001, du RGPD et des référentiels de cybersécurité associés

4. Rôles et responsabilités

4.1. Directeur général (DG)

4.1.1. Est propriétaire de la présente politique et veille à l'allocation de ressources appropriées pour la conception et l'administration sécurisées du réseau

4.1.2. Examine les dérogations aux mesures de sécurité réseau et approuve les accords d'accès réseau des fournisseurs

4.1.3. Examine les incidents ou constats d'audit liés à des faiblesses de sécurité réseau

4.2. Prestataire de support informatique / fonction informatique interne

4.2.1. Met en œuvre, configure et maintient l'ensemble des pare-feu, routeurs, commutateurs et contrôleurs sans fil

4.2.2. Gère la segmentation entre les réseaux internes, invités et externes

4.2.3. Surveille les journaux et les alertes relatifs aux tentatives d'accès non autorisées ou aux anomalies réseau

4.2.4. Veille à ce que les mises à jour des micrologiciels et des configurations soient appliquées de manière sécurisée et dans des délais appropriés

[... 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. La présente politique doit être revue au moins une fois par an par le directeur général, avec le prestataire de support informatique et le coordinateur à la protection des données.

9.2. Déclencheurs de revue intermédiaire

9.2.1. Une revue de la politique doit également être déclenchée dans les cas suivants :

9.2.1.1. Changements majeurs dans l'architecture réseau (par exemple, nouveaux systèmes VPN ou pare-feu)

9.2.1.2. Incident lié au réseau (par exemple, intrusion, propagation d'un rançongiciel ou exfiltration de données)

9.2.1.3. Évolutions juridiques, réglementaires ou des référentiels affectant la protection du réseau

9.2.1.4. Nouvelles plateformes fournisseurs nécessitant des méthodes d'accès ou des protocoles alternatifs

9.3. Gestion des versions et documentation

9.3.1. Les révisions de la politique doivent être enregistrées avec un numéro de version, une date et un résumé des changements

9.3.2. Les versions précédentes doivent être archivées pendant au moins 3 ans

9.3.3. Les mises à jour doivent être communiquées aux employés concernés, avec attestation de prise de connaissance de la politique lorsque des changements significatifs de comportement sont introduits

10. Politiques associées et articulations

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

10.1.1. P9S – Politique de télétravail : met en œuvre des méthodes d'accès à distance sécurisées, les exigences VPN et la protection des terminaux pour les utilisateurs hors site.

10.1.2. P12S – Politique de gestion des actifs : garantit que tous les systèmes connectés au réseau sont identifiés, catégorisés et suivis avec des statuts de sécurité à jour.

10.1.3. P17S – Politique de protection des données et de la vie privée : garantit que la segmentation réseau, les contrôles d'accès et la journalisation soutiennent les principes de protection des données au titre du RGPD.

10.1.4. P22S – Politique de journalisation et de surveillance : précise les exigences relatives à la collecte et à la revue des journaux provenant des équipements réseau, des connexions à distance et des contrôleurs sans fil.

10.1.5. P30S – Politique de réponse aux incidents : définit les actions requises en réponse aux violations du réseau, aux tentatives d'accès non autorisées ou à la propagation de logiciels malveillants via les réseaux internes.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Clause 8.1 – Exige la mise en œuvre de contrôles visant à garantir des opérations sécurisées et résilientes, y compris pour les réseaux.

11.2. ISO/IEC 27002

11.2.1. Mesure 8.20 – Fournit des orientations techniques et procédurales pour sécuriser l'accès réseau, la segmentation et la surveillance.

11.3. NIST SP 800-53 Rév. 5

11.3.1. AC-4 – Impose le contrôle des flux d'information au sein des réseaux et entre les systèmes.

11.3.2. SC-7 – Exige la protection des frontières, le routage sécurisé et la segmentation réseau afin de réduire le risque d'accès non autorisé.

11.4. RGPD de l'UE

11.4.1. Article 32 – Exige des mesures techniques et organisationnelles appropriées afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes et services en réseau qui traitent des données à caractère personnel.

11.5. Directive NIS2 de l'UE

11.5.1. Article 21(2)(d) – Impose des mesures techniques fondées sur les risques, y compris en matière de sécurité réseau et de contrôle d'accès.

11.5.2. Article 21(2)(e) – Exige la segmentation et l'isolement des systèmes afin d'empêcher la propagation des cyberincidents.

11.6. DORA de l'UE

11.6.1. Article 9 – Exige que les entités mettent en œuvre des contrôles de gestion des risques liés aux TIC, y compris pour les réseaux et les communications sécurisés.

11.6.2. Article 10 – Exige que les stratégies de résilience numérique couvrent la protection de l'infrastructure réseau et de la connectivité à distance.

11.7. COBIT 2019

11.7.1. DSS05.02 – Exige une protection efficace de l'infrastructure informatique et des environnements réseau contre les menaces internes et externes.

11.7.2. APO13.01 – Exige des stratégies de gestion des risques incluant la segmentation réseau et la surveillance dans le cadre de l'atténuation des menaces.