					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P38					Titre du document : **Politique relative aux communications sécurisées et à l'authentification multifacteur**							
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 la réglementation

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
RGPD (UE)	Art. 32(1)(b)	
NIS2 (UE)	Art. 21(2)(j)	
DORA (UE)	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Objet

1.1 Définir les exigences relatives à l'utilisation de solutions d'authentification multifacteur ou d'authentification continue pour l'accès aux systèmes, conformément à l'article 21(2)(j) de NIS2.

1.2 Établir des contrôles applicables aux communications vocales, vidéo, textuelles et d'urgence sécurisées afin de protéger la confidentialité et l'intégrité des informations.

2. Champ d'application

2.1 La présente politique s'applique à l'ensemble des mécanismes d'authentification et des systèmes de communication (appels vocaux, visioconférence, messagerie et systèmes de notification d'urgence) utilisés par l'organisation.

2.2 Elle couvre l'ensemble des employés et des prestataires, ainsi que toute partie externe utilisant les canaux de communication de l'organisation ou accédant à ses systèmes de réseau et d'information.

3. Objectifs

3.1 Garantir que seuls les utilisateurs dûment authentifiés obtiennent un accès aux systèmes, en réduisant le risque d'accès non autorisé grâce à la mise en œuvre de l'authentification multifacteur.

3.2 Garantir que les communications internes et d'urgence sont transmises au moyen de méthodes sécurisées (par exemple, des canaux chiffrés), afin d'empêcher toute écoute illicite ou toute altération.

3.3 Se conformer aux exigences de NIS2 en matière d'authentification forte et de communications sécurisées, afin de renforcer la cyberrésilience globale.

4. Rôles et responsabilités

4.1 RSSI / Sécurité informatique : définir et maintenir les mécanismes d'authentification multifacteur et les outils de communication sécurisés ; assurer la mise en œuvre technique de la présente politique.

4.2 Administrateurs informatiques : mettre en œuvre l'authentification multifacteur pour les systèmes concernés, configurer les plateformes de communication sécurisées approuvées et assurer le suivi de la conformité.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Surveillance et audit

9.1 La sécurité informatique doit assurer une surveillance continue des journaux d'authentification afin de détecter toute tentative de connexion à facteur unique ou tout échec anormal d'authentification

multifacteur. Les journaux des systèmes de communication sécurisés, lorsqu'ils existent, doivent également faire l'objet d'une surveillance afin de détecter les tentatives d'accès non autorisé ou les modifications de configuration.

9.2 L'audit interne doit revoir annuellement la conformité du déploiement de l'authentification multifacteur (en vérifiant que tous les systèmes critiques imposent l'authentification multifacteur) et confirmer que seuls les canaux sécurisés approuvés sont utilisés pour les communications sensibles. Les constats doivent être communiqués à la direction, accompagnés de recommandations.

10. Revue et maintenance

10.1 La présente politique doit faire l'objet d'une revue au moins annuelle, ainsi qu'à la suite de tout incident de sécurité majeur ou de tout nouveau risque identifié relatif à l'authentification ou aux communications (par exemple, nouveaux vecteurs de menace contre l'authentification multifacteur, découverte d'un usage de communications non sécurisées).

10.2 Des mises à jour doivent être apportées si nécessaire pour tenir compte de l'évolution des technologies (par exemple, adoption de solutions d'authentification continue plus robustes) ou pour se conformer aux orientations réglementaires mises à jour (telles que de futures recommandations de l'ENISA sur les communications sécurisées).

11. Politiques associées et articulations

11.1 P01 – Politique de sécurité de l'information. Définit les mesures de protection de l'authentification et des communications à l'échelle de l'entreprise.

11.2 P04 – Politique de contrôle d'accès. Établit la gouvernance des accès dont l'authentification multifacteur définie dans la P38 assure l'application.

11.3 P11 – Politique de gestion des comptes utilisateurs et des privilèges. Articule l'authentification multifacteur avec la gestion du cycle de vie des accès à privilèges.

11.4 P18 – Politique relative aux contrôles cryptographiques. Définit les méthodes cryptographiques approuvées et la gestion des clés pour les communications sécurisées.

11.5 P21 – Politique de sécurité réseau. Sécurise les canaux de transport utilisés par la voix, la vidéo et la messagerie.

11.6 P22 – Politique de journalisation et de surveillance. Encadre la surveillance des événements d'authentification et de l'utilisation des canaux sécurisés.

11.7 P32 – Politique de continuité d'activité et de reprise après sinistre. Encadre la sécurisation des communications d'urgence pendant les situations de crise.

11.8 P08 – Politique de sensibilisation et de formation à la sécurité de l'information. Définit la formation des utilisateurs sur l'authentification multifacteur et les bonnes pratiques d'utilisation des canaux.

12. Références

12.1 Directive NIS2 (UE 2022/2555), article 21(2), point (j) (utilisation de l'authentification multifacteur et de communications sécurisées)

12.2 Règlement d'exécution (UE) 2024/2690 de la Commission, annexe, section 11 (exigences relatives au contrôle d'accès, y compris l'authentification multifacteur pour les comptes à privilèges)

12.3 ISO/IEC 27001:2022 et ISO/IEC 27002:2022