					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P08S					Titre du document : **Politique de sensibilisation et de formation à la sécurité de l'information**							
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 7	
ISO/IEC 27002:2022	Mesure 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
Directive NIS2 de l'UE	Article 21(2)(i)	
Règlement DORA de l'UE	Article 13	
COBIT 2019	BAI08, DSS	
RGPD de l'UE	Article 32, 39	

1. Objet

1.1. La présente politique définit les exigences visant à garantir que l'ensemble des employés et prestataires comprennent leurs responsabilités en matière de sécurité de l'information.

1.2. Elle vise à réduire la probabilité d'erreur humaine, à améliorer la capacité à détecter et à signaler les incidents, et à instaurer une culture de sensibilisation à la sécurité au sein de l'organisation.

1.3. La politique contribue à la conformité à l'ISO/IEC 27001, à NIS2, au RGPD et à DORA en intégrant la sensibilisation à la sécurité dans les pratiques de travail quotidiennes et dans les attentes liées aux rôles.

2. Champ d'application

2.1. La présente politique s'applique à l'ensemble des employés, prestataires, stagiaires et tiers disposant d'un accès aux systèmes ou aux données de l'entreprise.

2.2. Elle couvre :

2.2.1. La formation d'intégration initiale pour les nouveaux arrivants

2.2.2. La formation annuelle de rappel à la sécurité

2.2.3. Les actions ponctuelles de sensibilisation (par ex. communications liées à un incident, affiches ou conseils)

2.3. Elle s'applique à l'ensemble des fonctions, départements et lieux de travail.

3. Objectifs

3.1. Garantir que l'ensemble du personnel reçoive, en temps utile, une formation de sensibilisation à la sécurité compréhensible et adaptée.

3.2. Permettre aux employés d'identifier et d'éviter les menaces courantes telles que l'hameçonnage, les logiciels malveillants et les fuites de données.

3.3. Établir une traçabilité de l'achèvement des formations afin de démontrer la conformité aux exigences légales, contractuelles et d'audit.

3.4. Maintenir un contenu de formation à jour reflétant les politiques de l'organisation, les menaces et les réglementations applicables.

3.5. Favoriser un état d'esprit proactif au sein du personnel, dans lequel la sécurité fait partie des responsabilités quotidiennes.

4. Rôles et responsabilités

4.1. Directeur général

4.1.1. Approuve les exigences de formation et veille à l'allocation des ressources nécessaires.

4.1.2. Examine les rapports d'achèvement et fait remonter les cas de non-conformité lorsque nécessaire.

4.2. Responsable administratif / Ressources humaines

4.2.1. Coordonne les modalités de mise à disposition de la formation pour les nouveaux recrutés et la formation annuelle de rappel.

4.2.2. Tient à jour les enregistrements de formation et les journaux de suivi des achèvements.

4.2.3. Veille à l'obtention des attestations de prise de connaissance par le personnel des principales politiques de sécurité de l'information et des accords de confidentialité.

[... 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 faire l'objet d'une revue annuelle par le Directeur général et les Ressources humaines afin de garantir qu'elle reflète les risques, les réglementations et les besoins du personnel en vigueur.

9.2. Mises à jour intermédiaires

9.2.1. La politique et le contenu de formation doivent également faire l'objet d'une revue et être révisés après :

9.2.1.1. Un incident de sécurité significatif

9.2.1.2. Des changements juridiques ou contractuels

9.2.1.3. Une restructuration organisationnelle ou des migrations de systèmes

9.3. Gestion des versions et diffusion

9.3.1. Chaque mise à jour doit inclure :

9.3.1.1. Le numéro de version et la date d'entrée en vigueur

9.3.1.2. Un résumé des changements

9.3.1.3. L'approbation du Directeur général

9.3.1.4. Une archive de toutes les versions antérieures conservée pendant au moins trois ans

9.4. Communication au personnel

9.4.1. Les mises à jour de la politique doivent être communiquées à l'ensemble du personnel, et une attestation doit être obtenue en cas de modification substantielle.

10. Politiques associées et articulations

10.1. La présente politique est articulée avec les documents suivants :

10.1.1. P2S – Politique relative aux rôles et responsabilités de gouvernance : attribue la responsabilité de la coordination et de la supervision des formations

10.1.2. P3S – Politique d'utilisation acceptable : renforce les attentes comportementales couvertes par la formation

10.1.3. P4S – Politique de contrôle d'accès : garantit que les utilisateurs comprennent l'importance de la sécurité des accès

10.1.4. P7S – Politique d’intégration et de départ : intègre la formation dans le processus d'entrée

10.1.5. P30S – Politique de réponse aux incidents : garantit que le personnel sait signaler les incidents rapidement et correctement

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Clause 7.3 – Exige des organisations qu'elles veillent à ce que le personnel soit conscient de ses responsabilités et des impacts en matière de sécurité

11.2. ISO/IEC 27002

11.2.1. Mesure 6.3 – Détaille les attentes relatives au périmètre et aux modalités de mise à disposition de la formation à la sécurité

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Exige une formation de sensibilisation pour les utilisateurs disposant d'un accès aux systèmes

11.3.2. AT-4 – Couvre la formation fondée sur les rôles et les conséquences de la non-conformité

11.4. RGPD de l'UE

11.4.1. Article 32 – Implique des mesures de sécurité, y compris la formation du personnel, afin de protéger les données à caractère personnel

11.4.2. Article 39 – Exige, le cas échéant, que les DPD supervisent la sensibilisation et la formation

11.5. Directive NIS2 de l'UE

11.5.1. Article 21(2)(i) – Exige des programmes continus de sensibilisation à la cybersécurité et de formation

11.6. Règlement DORA de l'UE

11.6.1. Article 13 – Exige des entités financières qu'elles mettent en œuvre des actions d'éducation et de formation pour l'ensemble du personnel ayant des responsabilités liées aux TIC

11.7. COBIT 2019

11.7.1. BAI08 – Manage Knowledge : garantit que le personnel est compétent et formé

11.7.2. DSS05 Gestion des services de sécurité – Met l'accent sur la sensibilisation en tant que mesure de protection clé