					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P08					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 7.3, Annexe A, mesure 6.3	Établit les exigences de sensibilisation et de formation couvertes par la présente politique
ISO/IEC 27002:2022	Mesure 6	Soutient une sensibilisation et une formation appropriées, fondées sur les rôles
NIST SP 800-53 Rev.5	AT-1 à AT-5	S'aligne sur la politique et les procédures, la sensibilisation, la formation fondée sur les rôles, les enregistrements de formation et les contacts avec les groupes de sécurité
RGPD de l'UE	Articles 32, 39 ; considérant 78	Imposent une formation du personnel habilité à traiter des données à caractère personnel et une sensibilisation générale du personnel
NIS2 de l'UE	Articles 21(2)(a, b), 21(3)	Exige des politiques de formation aux risques et à la sécurité, ainsi que des actions de sensibilisation
DORA de l'UE	Articles 5, 8, 13	Exige la sensibilisation aux risques liés aux TIC et la formation dans le cadre des contrôles de résilience
COBIT 2019	APO07, DSS05, MEA	Renforce la sensibilisation des effectifs, la formation des utilisateurs et la surveillance de la conformité

1. Objet

1.1 La présente politique établit le cadre formel visant à garantir que l'ensemble du personnel est sensibilisé à ses responsabilités en matière de sécurité de l'information et reçoit la formation nécessaire pour protéger la confidentialité, l'intégrité et la disponibilité des actifs informationnels.

1.2 Elle met en œuvre la clause 7.3 et l'annexe A, mesure 6.3, de l'ISO/IEC 27001 en imposant un programme structuré de sensibilisation et de formation, fondé sur les risques et adapté aux rôles au sein de l'organisation ainsi qu'à l'évolution des menaces.

1.3 La politique contribue à réduire les vulnérabilités d'origine humaine, à promouvoir des comportements de sécurité appropriés et à renforcer en continu les pratiques sécurisées, en conformité avec les exigences réglementaires et contractuelles.

2. Champ d’application

2.1 La présente politique s'applique à toutes les personnes internes et externes ayant accès aux systèmes d'information, aux données ou aux installations de l'organisation, y compris :

2.1.1 les employés (à temps plein, à temps partiel, temporaires)

2.1.2 les sous-traitants, consultants, fournisseurs et stagiaires

2.1.3 les tiers disposant d'un accès logique ou physique dans le cadre d'accords de service

2.2 Le champ d'application comprend :

2.2.1 la formation initiale de sensibilisation à la sécurité dans le cadre du processus d'intégration

2.2.2 la formation spécifique aux rôles (par exemple, développeurs, finance, utilisateurs à privilèges)

2.2.3 les formations de rappel périodiques et les campagnes de sensibilisation

2.2.4 la formation ad hoc en réponse à des incidents ou à de nouvelles menaces

2.3 Les modalités de formation couvertes par la présente politique comprennent la formation en ligne, les sessions d'information en présentiel, les simulations, les tests de connaissances, les affiches, les lettres d'information sur la sécurité et les accusés de réception obligatoires.

3. Objectifs

3.1 Garantir que l'ensemble du personnel comprend ses responsabilités en matière de protection des actifs de l'organisation et de respect des politiques de sécurité.

3.2 Fournir une sensibilisation et une formation continues et mesurables, alignées sur l'exposition aux risques liée aux rôles.

3.3 Intégrer des comportements sécurisés dans les opérations quotidiennes en renforçant des pratiques telles que l'utilisation sécurisée des mots de passe, le signalement des incidents et la résistance à l'hameçonnage.

3.4 Garantir la conformité réglementaire et la préparation aux audits pour les obligations de formation à la sécurité de l'information dans l'ensemble des secteurs et des juridictions.

3.5 Réduire les incidents de sécurité résultant de la négligence, d'un manque de sensibilisation ou d'une erreur de jugement grâce au renforcement des comportements et à l'amélioration continue.

4. Rôles et responsabilités

4.1 Direction générale

4.1.1 Approuve la stratégie de formation à la sécurité de l'information de l'organisation et veille à ce qu'elle dispose des ressources nécessaires et soit intégrée aux priorités de l'entreprise.

4.1.2 Supervise la conformité au niveau managérial et veille au respect de la présente politique dans l'ensemble des départements.

4.2 RSSI / responsable du SMSI

4.2.1 Est responsable de la présente politique et définit le cadre de sensibilisation et de formation en fonction des besoins liés aux risques, à la conformité et à l'activité.

4.2.2 Supervise la conception, le déploiement, le suivi et la revue de l'ensemble des actions de formation à la sécurité.

4.2.3 Veille à ce que la formation soit mise à jour périodiquement et tienne compte de l'évolution des menaces et des technologies émergentes.

[... 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 Fréquence de revue

9.1.1 La présente politique et le programme de formation associé doivent faire l'objet d'une revue :

9.1.1.1 chaque année, ou

9.1.1.2 après des incidents majeurs impliquant une erreur humaine ou une menace interne

9.1.1.3 lors de l'introduction de nouvelles technologies ou de nouvelles menaces significatives

9.1.1.4 en réponse à toute évolution des obligations juridiques, contractuelles ou de certification

9.2 Processus de revue

9.2.1 La revue est conduite par le RSSI, en coordination avec :

9.2.1.1 les départements RH et formation

9.2.1.2 les fonctions juridiques et les délégués à la protection des données

9.2.1.3 les fonctions sécurité informatique et risque opérationnel

9.2.2 Toute mise à jour doit :

9.2.2.1 être approuvée par le comité de pilotage du SMSI

9.2.2.2 faire l'objet d'une gestion de version et être documentée dans le registre documentaire du SMSI

9.2.2.3 être communiquée aux utilisateurs si des modifications substantielles affectent le périmètre de la formation ou les responsabilités

9.3 Gouvernance de la mise à jour du contenu

9.3.1 Les modules de formation et les supports de sensibilisation doivent faire l'objet d'une revue tous les 12 mois afin de garantir :

9.3.1.1 leur pertinence au regard du paysage des menaces

9.3.1.2 leur exactitude réglementaire

9.3.1.3 leur compatibilité de format (par exemple, accessibilité, localisation)

9.3.2 Tout contenu obsolète ou trompeur doit être retiré immédiatement et remplacé par des contenus approuvés.

10. Politiques associées et articulations

10.1 La présente politique est soutenue par les politiques suivantes et soutient leur mise en œuvre :

10.1.1 P01 – Politique de sécurité de l'information : établit la sensibilisation à la sécurité comme contrôle fondamental du SMSI de l'organisation.

10.1.2 P03 – Politique d'utilisation acceptable : impose une attestation de l'utilisateur dans le cadre de la formation et précise les responsabilités liées à l'usage quotidien des technologies.

10.1.3 P07 – Politique d'intégration et de départ : garantit que la formation est intégrée dès l'entrée et suivie tout au long de la relation de travail.

10.1.4 P06 – Politique de gestion des risques : relie la formation centrée sur le facteur humain à la modélisation des menaces et aux stratégies de réduction du risque résiduel.

10.1.5 P33 – Politique d'audit et de surveillance de la conformité : valide, lors des audits, que les contrôles de sensibilisation sont opérationnels, mesurables et efficaces.

10.2 Ensemble, ces politiques constituent un cadre complet de contrôles comportementaux intégrant la sensibilisation, la responsabilisation et le renforcement de la culture de sécurité.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 7.3 – Sensibilisation : impose aux organisations de veiller à ce que les travailleurs aient connaissance des politiques de sécurité de l'information et de leurs responsabilités. La présente politique met en œuvre cette exigence au moyen d'une intégration structurée, d'une formation périodique et d'une participation mesurable aux campagnes.

11.1.2 Annexe A, mesure 6.3 – Sensibilisation, éducation et formation à la sécurité de l'information : pleinement couverte au moyen de programmes de formation initiaux, fondés sur les rôles et continus, adaptés aux profils de risque des utilisateurs.

11.2 ISO/IEC 27002:2022 – Mesure 6

11.2.1 Soutient l'élaboration et la diffusion d'une sensibilisation et d'une formation adaptées aux rôles, en mettant l'accent sur le renforcement des comportements sécurisés et sur les mises à jour périodiques fondées sur le renseignement sur les menaces et les retours d'audit.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 à AT-5 (famille Sensibilisation et formation) : la présente politique est alignée sur AT-1 (politique et procédures), AT-2 (formation de sensibilisation), AT-3 (formation fondée sur les rôles), AT-4 (enregistrements de formation à la sécurité) et AT-5 (contact avec les groupes de sécurité).

11.3.2 IA-5, AC-2 : renforce la responsabilité des utilisateurs en matière d'authentification sécurisée et d'utilisation acceptable, au cœur des résultats comportementaux des programmes de sensibilisation.

11.3.3 IR-1 à IR-8 : la préparation à la réponse aux incidents est renforcée par des campagnes de sensibilisation ciblées et des simulations.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 32 – Sécurité du traitement : impose que le personnel traitant des données à caractère personnel soit formé à reconnaître, prévenir et signaler les risques pesant sur ces informations. La présente politique garantit que le personnel habilité à traiter des données à caractère personnel et tous les rôles concernés reçoivent la formation appropriée.

11.4.2 Article 39 – Missions du délégué à la protection des données : comprend la sensibilisation et la formation du personnel participant aux opérations de traitement.

11.4.3 Considérant 78 : encourage des mesures de sensibilisation appropriées afin de garantir des pratiques de sécurité robustes et le respect de la politique.

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

11.5.1 Article 21(2)(a, b) : exige que les entités adoptent des politiques relatives à l'analyse des risques et à la formation à la sécurité pour l'ensemble du personnel concerné. La présente politique répond à cette exigence en établissant des processus de formation continus et adaptés à la sensibilité des rôles.

11.5.2 Article 21(3) : encourage la promotion de la sensibilisation aux risques de cybersécurité auprès de la direction et du personnel au moyen d'actions de sensibilisation et de simulations.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 13 – Stratégie de résilience opérationnelle numérique : impose que la sensibilisation aux risques liés aux TIC et la formation fassent partie du modèle de gouvernance. La présente politique garantit que le risque humain est traité par une formation continue et des simulations de menaces.

11.6.2 Articles 5 et 8 : soulignent l'importance des cadres de contrôle interne, dont la sensibilisation et la formation constituent des composantes fondamentales de la résilience TIC et de l'hygiène cyber.

11.7 COBIT 2019

11.7.1 APO07 – Gestion des ressources humaines : renforce la nécessité de développer la sensibilisation aux responsabilités de sécurité et de l'intégrer dans la gestion des effectifs.

11.7.2 DSS05 – Gestion des services de sécurité : établit des contrôles relatifs à la formation des utilisateurs et au signalement des incidents, qui sont tous deux au cœur de la présente politique.

11.7.3 MEA03 – Surveiller, évaluer et apprécier la conformité : exige une revue de l'efficacité du comportement des utilisateurs et du respect de la politique, mise en œuvre ici au moyen de tests d'hameçonnage, de questionnaires et d'indicateurs de campagne de sensibilisation.