					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P25S					Titre du document : **Politique relative aux exigences de sécurité des applications**							
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	Contrôles opérationnels, y compris la sécurité des applications
ISO/IEC 27002:2022	Mesures 8.25–8.26	Conception sécurisée, développement sécurisé, tests de sécurité et revue de code
NIST SP 800-53 Rev.5	SA-11, SI-10	Tests développeur/applicatifs, analyse de code, prévention des défauts
RGPD de l'UE	Article 25	Protection des données dès la conception et par défaut
NIS2 de l'UE	Article 21(2)(a), (e)	Mesures techniques visant à sécuriser les applications et à détecter les risques
DORA de l'UE	Articles 9(2)(c), 10(2)(c)	Sécurité des applications au service de la résilience opérationnelle numérique
COBIT 2019	BAI03	Gestion de la conception et de l'acquisition de logiciels sécurisés

1. Objet

1.1 La présente politique définit les contrôles minimaux et obligatoires de sécurité des applications applicables à l'ensemble des logiciels et solutions systèmes utilisés par l'organisation, qu'ils soient développés en interne ou acquis auprès de fournisseurs externes.

1.2 Elle impose que les applications soient conçues, mises en œuvre et maintenues de manière à protéger les données des clients, des employés et de l'activité contre tout accès non autorisé, usage abusif, altération ou destruction.

1.3 La présente politique soutient les efforts de l'organisation pour obtenir et maintenir la certification ISO/IEC 27001, satisfaire aux obligations issues du RGPD et de NIS2, et réduire les risques opérationnels liés à des déploiements logiciels non sécurisés.

1.4 Elle contribue à établir une approche cohérente et vérifiable en audit de la sécurité des applications pour les PME en définissant une liste de contrôle uniforme des fonctionnalités et pratiques de sécurité, adaptée aux environnements disposant de ressources techniques internes limitées.

2. Champ d’application

2.1 La présente politique s'applique à l'ensemble des applications, systèmes, outils et plateformes qui :

2.1.1 sont développés en interne, personnalisés ou scriptés pour un usage interne

2.1.2 sont acquis sous forme de logiciels commerciaux, de SaaS ou de systèmes hébergés dans le cloud

2.1.3 traitent, stockent ou transmettent des données à caractère personnel, des enregistrements métier ou des informations opérationnelles sensibles

2.1.4 sont accessibles aux employés, prestataires, clients ou partenaires via les réseaux internes, Internet ou des plateformes mobiles

2.2 La politique couvre :

2.2.1 les développeurs (internes ou sous contrat)

2.2.2 les éditeurs de logiciels et les prestataires de services cloud

2.2.3 le personnel de support informatique ou les administrateurs responsables du déploiement et du support

2.2.4 les propriétaires d'application et les utilisateurs métier intervenant dans l'approbation et la supervision des systèmes

3. Objectifs

3.1 Veiller à ce que toutes les applications utilisées par l'organisation intègrent des contrôles de sécurité vérifiables permettant d'atténuer les vulnérabilités logicielles courantes.

3.2 Protéger la confidentialité, l'intégrité et la disponibilité des données traitées par les applications, quel que soit leur environnement d'hébergement.

3.3 Exiger des tests de sécurité, une revue formelle et une validation de la sécurité des applications avant l'approbation de toute nouvelle application ou de toute mise à jour majeure pour un usage en production.

3.4 Permettre un traitement sécurisé et cohérent des identifiants d'authentification, des données de session et des droits d'accès dans l'ensemble des systèmes critiques pour l'activité.

3.5 Exiger des capacités de journalisation sécurisée, de traçabilité d'audit et de surveillance dans toutes les applications afin de permettre la détection d'activités suspectes et la réponse associée.

3.6 Réduire les risques juridiques et de conformité en veillant à ce que les applications respectent les exigences réglementaires de sécurité applicables.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Assume la responsabilité globale de la sécurité des applications au sein de l'organisation.

4.1.2 Approuve la présente politique et veille à ce que toutes les acquisitions et tous les projets de développement s'y conforment.

4.1.3 Veille à ce que les fournisseurs et prestataires de services soient contractuellement tenus de respecter les exigences de sécurité des applications.

4.1.4 Examine et approuve les dérogations fondées sur le risque lorsque la conformité complète ne peut pas être atteinte en raison de contraintes métier.

4.2 Propriétaire d'application (s'il est désigné)

4.2.1 Identifie les besoins de sécurité propres à l'application lors de la sélection du système ou du lancement du projet.

4.2.2 Vérifie que les fonctionnalités clés telles que la protection de la connexion, le chiffrement et les journaux d'activité sont bien incluses.

4.2.3 Participe aux revues préalables au déploiement et confirme que les contrôles de sécurité répondent aux besoins métier.

[... 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 revue par le Directeur général au moins une fois par année civile afin de :

9.1.1 refléter les évolutions des exigences réglementaires (par exemple RGPD, NIS2, DORA)

9.1.2 intégrer les menaces nouvelles ou émergentes ainsi que les nouvelles techniques d'attaque

9.1.3 mettre à jour le libellé et les exigences pour refléter les évolutions des plateformes, des fournisseurs ou des méthodes de développement

9.2 Des revues intermédiaires doivent également être menées lorsque :

9.2.1 de nouvelles applications sont introduites

9.2.2 des applications existantes font l'objet de mises à jour significatives ou d'une intégration importante

9.2.3 un incident ou une violation lié(e) à une application survient

9.2.4 de nouveaux risques sont identifiés à partir d'avis externes ou d'alertes sectorielles

9.3 Toute mise à jour de la présente politique doit être :

9.3.1 approuvée par le Directeur général

9.3.2 documentée avec l'historique des versions et le motif du changement

9.3.3 communiquée à tous les employés, développeurs et fournisseurs impliqués dans la gestion des applications

9.3.4 conservée de manière sécurisée à des fins d'audit et de conformité

10. Politiques associées et articulations

10.1 La présente politique est directement soutenue par les politiques de sécurité alignées sur les PME suivantes et contribue à leur mise en œuvre :

10.1.1 P2S – Politique relative aux rôles et responsabilités de gouvernance : attribue la responsabilité d'approuver les applications, d'assurer l'application de la politique et de gérer les fournisseurs.

10.1.2 P4S – Politique de contrôle d'accès : veille à ce que l'accès aux applications soit conforme aux principes de moindre privilège et de contrôle des sessions.

10.1.3 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : veille à ce que les utilisateurs et les développeurs soient formés à reconnaître et signaler les menaces liées aux applications.

10.1.4 P17S – Politique de protection des données et de la vie privée : définit les mesures de protection des données devant être appliquées par toute application traitant des données à caractère personnel.

10.1.5 P14S – Politique de conservation et d'élimination des données : encadre la manière dont les journaux, sauvegardes et données sensibles générés par les applications doivent être conservés, archivés et détruits de manière sécurisée.

10.1.6 P30S – Politique de réponse aux incidents : décrit les étapes d'identification, de signalement et de confinement des événements de sécurité liés aux applications.

10.2 Ensemble, ces politiques garantissent que la sécurité des applications est pleinement intégrée au système de management de la sécurité de l'information (SMSI) de l'organisation et qu'elle contribue au respect des exigences d'audit.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Exige que les organisations établissent des contrôles opérationnels pour traiter les risques de sécurité de l'information, y compris ceux liés aux applications et aux systèmes logiciels.

11.2 ISO/IEC 27002

11.2.1 Mesure 8.25 – Recommande la mise en œuvre de pratiques de conception sécurisée, de développement sécurisé et de revue de code sur l'ensemble des applications, y compris celles fournies par des fournisseurs.

11.2.2 Mesure 8.26 – Recommande des tests formels des contrôles de sécurité des applications, en particulier dans les domaines du contrôle d'accès, de la validation des entrées et de la gestion des sessions.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Définit des exigences relatives aux tests développeur, à l'analyse de code et à l'analyse dynamique des applications avant déploiement.

11.3.2 SI-10 – Traite de la détection et de la prévention des défauts logiciels courants, en mettant l'accent sur la sensibilisation des développeurs et les mesures de protection techniques.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 25 – « Protection des données dès la conception et par défaut » impose d'intégrer la protection de la vie privée et la sécurité au cœur de la conception des applications traitant des données à caractère personnel.

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

11.5.1 Article 21(2)(a) et (e) – Exige des entités essentielles et importantes qu'elles mettent en œuvre des mesures techniques pour sécuriser les applications et détecter les risques liés aux logiciels.

11.6 DORA de l'UE (2022/2554)

11.6.1 Articles 9(2)(c), 10(2)(c) – Exigent des PME du secteur financier qu'elles intègrent des contrôles de sécurité au niveau applicatif et réalisent des évaluations régulières afin de maintenir la résilience opérationnelle numérique.

11.7 COBIT 2019

11.7.1 BAI03 – « Manage Solutions Identification and Build » encadre le développement ou l'acquisition de logiciels sécurisés alignés sur les risques, la conformité et les exigences métier, y compris dans des environnements de PME soumis à des contraintes de ressources.