| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insérez ici la dénomination de l'entité juridique enregistrée | | | | | | | |
| Numéro du document :<br>P25 | | | | | Titre du document :<br>**Politique relative aux exigences de sécurité des applications** | | | | | | | |
| Version :<br>1.0 | | Date d'entrée en vigueur :<br>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 | Mesures 8.25–8.28 | — |
| NIST SP 800-53 Rev.5 | SA-11, SA-15, SI-10 | — |
| RGPD de l'UE | Articles 25, 32 | — |
| Directive NIS2 de l'UE | Articles 21(2)(f), 23 | — |
| DORA de l'UE | Articles 9, 11 | — |
| COBIT 2019 | BAI03, BAI09, DSS | — |

**1. Objet**

1.1 La présente politique définit les exigences de sécurité obligatoires applicables à la couche applicative pour les logiciels développés, acquis, intégrés ou déployés par l'organisation. Elle impose que toutes les applications soient conçues, mises en œuvre et maintenues conformément aux principes de développement sécurisé, aux obligations réglementaires et à l'appétence au risque de l'organisation.

1.2 La politique impose l'intégration de la sécurité tout au long du cycle de vie des applications, notamment pour l'authentification des utilisateurs, le traitement des données, la protection des interfaces et les interactions sécurisées avec les interfaces de programmation applicative (API) ou les services.

1.3 Par l'adoption de cette politique, l'organisation vise à prévenir l'introduction de vulnérabilités logicielles, à protéger les données sensibles et à garantir la traçabilité et la résilience face à l'exploitation malveillante et aux usages abusifs.

**2. Champ d'application**

**2.1 La présente politique s'applique à l'ensemble des éléments suivants :**

2.1.1 Les applications développées en interne ou obtenues auprès de sources externes, y compris les environnements SaaS et les outils développés sur mesure

2.1.2 Les applications soutenant des opérations métier critiques, l'accès des clients ou le traitement de données réglementées

2.1.3 Les équipes de développement, DevOps, d'assurance qualité, produit et de sécurité

2.1.4 Les développeurs tiers, éditeurs de logiciels et partenaires d'intégration disposant d'un accès aux applications de l'organisation ou aux interfaces de programmation applicative (API)

2.2 Elle s'applique à l'ensemble des environnements : développement, test, préproduction, production et reprise après sinistre, qu'ils soient hébergés sur site, dans des centres de données privés ou dans des environnements cloud publics.

**3. Objectifs**

3.1 Définir des exigences de sécurité minimales, fonctionnelles et non fonctionnelles, devant être respectées par toutes les applications, indépendamment de la méthode de développement ou de la pile technologique.

3.2 Garantir l'intégration de protections au niveau applicatif, notamment la validation des entrées, l'encodage des sorties, la gestion des erreurs et la sécurité des sessions.

3.3 Exiger une mise en œuvre sécurisée des mécanismes d'authentification, d'autorisation et de contrôle d'accès, en cohérence avec les politiques d'identité et d'accès de l'organisation.

3.4 Imposer des interactions sécurisées avec les interfaces de programmation applicative (API), les interfaces web et les composants tiers au moyen de protocoles approuvés et de mesures de sécurité adaptées.

3.5 Permettre la détection précoce et l'atténuation des vulnérabilités grâce à l'analyse statique et dynamique, aux revues de code et à la modélisation des menaces.

3.6 Protéger les données sensibles conformément aux exigences réglementaires en imposant le chiffrement, la classification et des règles de conservation des données.

3.7 Garantir la validation continue du niveau de sécurité des applications après déploiement, au moyen de tests, de surveillance et de dispositifs de préparation à l'audit.

**4. Rôles et responsabilités**

**4.1 Responsable de la sécurité des systèmes d'information (RSSI)**

4.1.1 Est propriétaire de la présente politique et veille à son alignement avec la stratégie de sécurité de l'information et le niveau de risque de l'organisation.

4.1.2 Approuve les exigences de sécurité des applications et impose les contrôles obligatoires dans les fonctions de développement et d'achats.

**4.2 Responsable de la sécurité des applications / Responsable DevSecOps**

4.2.1 Définit les contrôles de sécurité de référence et les méthodologies de test applicables aux composants applicatifs.

4.2.2 Supervise l'intégration sécurisée d'outils tels que SAST, DAST, IAST et SCA dans la chaîne de livraison logicielle.

4.2.3 Tient à jour la liste de contrôle des exigences de sécurité des applications et les critères de validation.

[ ... 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 annuelle, ou plus fréquemment en réponse à :**

9.1.1 Des divulgations de vulnérabilités critiques affectant des frameworks ou dépendances couramment utilisés

9.1.2 Des évolutions des obligations réglementaires relatives à la sécurité des applications (par exemple : NIS2, DORA)

9.1.3 Des changements majeurs dans les pratiques de développement logiciel, l'outillage ou l'architecture cloud de l'organisation

9.1.4 Des constats issus d'audits internes ou de tests d'intrusion externes

9.2 La revue doit être pilotée par le Responsable de la sécurité des applications, en coordination avec le RSSI, les responsables de l'ingénierie DevOps, les affaires juridiques, les achats et les responsables assurance qualité.

9.3 Toutes les révisions doivent faire l'objet d'une gestion de version dans le registre de contrôle documentaire du SMSI et être diffusées à l'ensemble des équipes de développement et produit concernées.

9.4 Les versions remplacées doivent être archivées pendant au moins trois ans afin d'assurer la traçabilité, l'auditabilité et le support aux investigations en cas d'incident.

**10. Politiques associées et articulations**

10.1 P1 – Politique de sécurité de l'information. Établit le cadre fondamental de protection des systèmes et des données, dans lequel les contrôles au niveau applicatif sont requis afin de prévenir les accès non autorisés, les fuites de données et l'exploitation malveillante.

10.2 P4 – Politique de contrôle d'accès. Définit les normes de gestion des identités et des sessions devant être appliquées par toutes les applications, y compris l'authentification forte, le moindre privilège et les exigences de revue des accès.

10.3 P5 – Politique de gestion des changements. Encadre la promotion du code applicatif et des configurations vers les environnements de production afin de garantir le blocage des changements non autorisés ou non testés.

10.4 P17 – Politique de protection des données et de la vie privée. Exige que les applications mettent en œuvre la protection de la vie privée dès la conception et garantissent le traitement licite, le chiffrement et la conservation des données à caractère personnel et des données sensibles dans tous les environnements.

10.5 P24 – Politique de développement sécurisé. Fournit le cadre général d'intégration de la sécurité dans le cycle de vie de développement logiciel, dont la présente politique précise les exigences concrètes et les contrôles techniques à mettre en œuvre au niveau de la couche applicative.

10.6 P30 – Politique de réponse aux incidents. Implique une gestion structurée des incidents de sécurité applicative, y compris des vulnérabilités identifiées après déploiement ou lors de tests d'intrusion, et définit les procédures d'escalade, de confinement et de rétablissement.

## 11. Normes et référentiels de référence

### 11.1 ISO/IEC 27001:2022

11.1.1 Clause 8.1 – Planification et maîtrise opérationnelles : impose l'intégration de la sécurité des applications dans les processus et les systèmes afin de garantir la confidentialité, l'intégrité et la disponibilité.

### 11.2 ISO/IEC 27002:2022

11.2.1 Mesures 8.25–8.26 : détaillent les attentes en matière de sécurité de la couche applicative, y compris les pratiques de programmation sécurisée, la modélisation des menaces, les contrôles d'architecture et la validation des logiciels tiers.

11.2.2 Annexe A, mesure 8.25 – Cycle de vie de développement sécurisé : impose l'intégration de la sécurité sur l'ensemble du cycle de vie des applications.

11.2.3 Annexe A, mesure 8.26 – Exigences de sécurité des applications : impose la définition et l'application de contrôles techniques visant à protéger les applications contre les usages abusifs et la compromission.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Tests et évaluation de sécurité par les développeurs : impose des tests statiques, dynamiques et des tests d'intrusion pendant le développement.

11.3.2 SA-15 – Processus, normes et outils de développement : établit des normes formelles pour le développement sécurisé des applications.

11.3.3 SI-10 – Validation des entrées d'information : impose des mécanismes de contrôle visant à prévenir les attaques par injection et les attaques liées à l'analyse syntaxique.

### 11.4 RGPD de l'UE (2016/679)

11.4.1 Article 25 – Protection des données dès la conception et par défaut : impose l'intégration de la protection des données et de la vie privée dans la logique applicative et les flux de traitement.

11.4.2 Article 32 – Sécurité du traitement : impose des mesures techniques appropriées, telles que la validation des entrées, le chiffrement et des contrôles d'accès sécurisés.

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

11.5.1 Article 21(2)(f) : impose la gestion des vulnérabilités et des pratiques sécurisées sur l'ensemble du cycle de vie des applications pour les entités essentielles et importantes.

11.5.2 Article 23 – Notification des incidents de sécurité : nécessite des capacités de journalisation et de surveillance au niveau applicatif afin de détecter et de signaler les incidents significatifs.

**11.6 DORA de l'UE (2022/2554)**

11.6.1 Article 9 – Gestion des risques liés aux TIC : impose aux entités financières de garantir que les applications sont sécurisées, testées et résilientes face aux cybermenaces.

11.6.2 Article 11 – Tests des outils TIC : encourage la réalisation périodique de tests d'intrusion et d'exercices de red team sur les applications et services critiques.

**11.7 COBIT 2019**

11.7.1 BAI03 – Gérer l'identification et la construction des solutions : établit les exigences de conception et de contrôle pendant le développement des applications.

11.7.2 BAI09 – Gérer les applications : met l'accent sur la maintenance sécurisée, la surveillance et l'amélioration des systèmes en production.

11.7.3 DSS05 – Gérer les services de sécurité : relie la protection des applications aux opérations et contrôles de sécurité plus larges de l'organisation.