Politique de Sécurité de l'Information

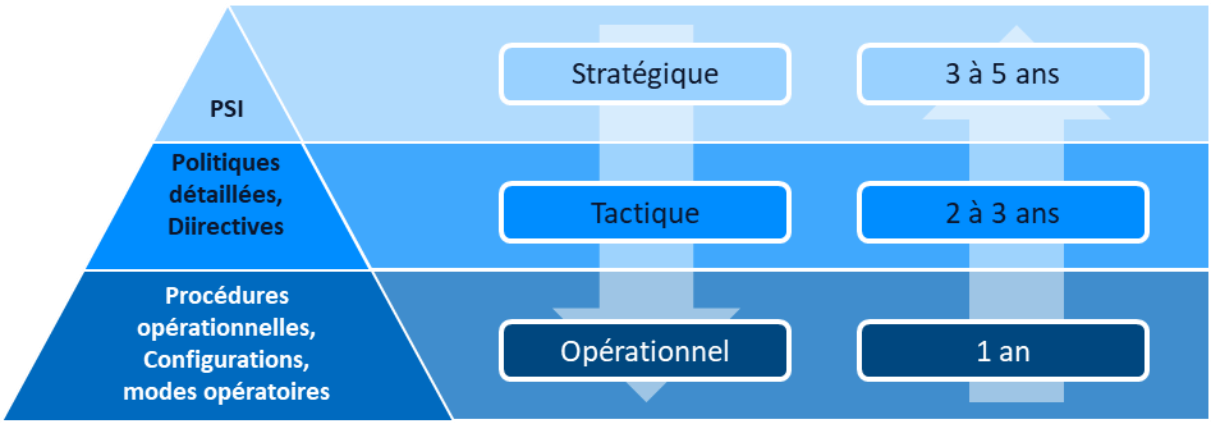
Table des matières

Suivi des révisions

Versions	Auteur	Date	Commentaires
V0.1	RSSI externe Almond	23/01/2025	Initialisation du document

1. Objet et champ d'application

Ce document « **Politique de Sécurité de l'Information** » (**PSI**) est de portée « politique générale ». Il est le document fondateur de la sécurité de l'information au sein du Groupe POZEO et il est complété par des documents de portée « politiques détaillées et procédures opérationnelles ».



Cette PSI s'applique à l'ensemble du patrimoine opérationnel et des systèmes d'information du Groupe POZEO. Cette PSI prend en compte l'activité, les contraintes et les risques auxquels sont exposés les sociétés du Groupe POZEO.

Le champ d'application de cette Politique couvre donc :

- L'ensemble des entités de l'organisation ;
- L'ensemble des activités de l'organisation, dont :
    - L'accompagnement des clients dans leurs projets de fidélisation et d'amélioration du bien-être des salariés.
    - La fourniture des solutions de marketing opérationnel pour les clients
- L'ensemble du système d'information, ce qui inclut les data centers, y compris dans leurs dimensions externalisées, matérielles comme immatérielles et les systèmes informatiques.

Les parties prenantes dont les attentes de sécurité sont prises en comptes par la PSI sont les suivantes :

- Les parties internes, et notamment :
    - Les directions opérationnelles, métiers et support (Direction Générale, Direction des Ressources Humaines, Direction Administrative et Financière et Services informatiques),
    - Les employés du Groupe POZEO,
- Les parties externes, et notamment :
    - Le personnel externe (prestataires),
    - Les sous-traitants et fournisseurs,
    - Les clients et usagers des services du Groupe POZEO.

2. Objectifs

Cette politique vise trois objectifs de sécurité principaux :

- Garantir l'alignement de la gestion de la sécurité de l'information avec les valeurs de l'entreprise et les orientations stratégiques définies par la Direction ;

- Formaliser les pratiques du Groupe POZEO afin de garantir l'homogénéité et la qualité des mesures de sécurité mises en œuvre ;

- Maintenir la relation de confiance entre les clients et le Groupe POZEO en préservant leur patrimoine informationnel.

Elle a pour finalité de contribuer à :

- Maitriser les risques auxquels est exposée l'entreprise ;
- Assurer la disponibilité des services métiers rendus aux clients ;
- Assurer la confidentialité des informations confiées au Groupe POZEO par ses clients ;
- Assurer le respect des lois, réglementations et contrats en vigueur ;
- Promouvoir l'amélioration continue.

Les objectifs de sécurité sont ensuite déclinés selon les critères de confidentialité, d'intégrité, de disponibilité et de traçabilité de l'information pour :

- Répondre aux attentes de sécurité des parties prenantes ;
- Éviter les violations des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information ;
- Éviter les violations des exigences de sécurité ;
- Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.
- Préciser la nature et la fréquence des tests de vulnérabilité et de pénétration à mener sur les périmètres concernés, en vue de mettre en évidence les éventuelles vulnérabilités présentes sur les systèmes concernés à un instant donné.

La PSI présente les principes de sécurité à appliquer ainsi que les indicateurs à collecter à des fins de pilotage et d'amélioration.

Elle s'inspire des exigences et bonnes pratiques formulées en matière de mise en œuvre d'un système de management de la sécurité de l'information (**SMSI**), telles que contenues dans la norme **ISO/IEC 27001 : 2022**.

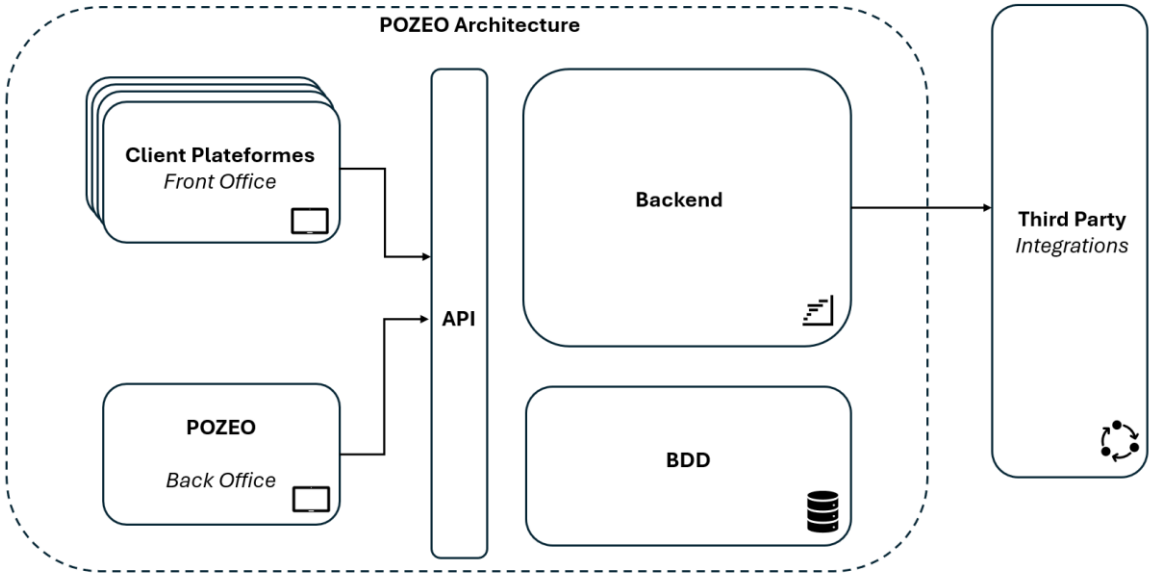
3. Application de la politique

3.1. Périmètre des activités

Le périmètre des activités couvert par cette PSI sur le marché français regroupe :

- Marketing opérationnel
- Chèques cinéma
- Chèques culture
- Chèques cadeaux multi-enseignes, et loisirs
- CSE d'entreprises
- Subventions
- Panel d'offres
- Billetterie

3.1. Périmètre technique



3.2. Dérogation

Certains impératifs peuvent rendre nécessaire la mise en place d'une dérogation à la présente Politique.

Dans le cas d'une telle demande, celle-ci est qualifiée par la Secrétaire Générale fin de valider le besoin, de qualifier les risques correspondants et de définir une proposition de date de fin de dérogation.

La date de révision de la dérogation permet de s'assurer que celle-ci peut être supprimée sans dommage pour les activités de l'entreprise. Dans le cas où celle-ci ne pourrait être supprimée, elle ferait l'objet d'une nouvelle évaluation et d'une nouvelle décision de prise en compte (incluant une nouvelle date de fin).

3.3. Cycle de vie de la politique

Le cycle de vie de la politique est constitué des étapes suivantes :

- Constitution ;
- Révision ;
- Validation ;
- Communication ;
- Diffusion ;

La Politique de Sécurité de l'Information (PSI) repose sur deux dimensions temporelles :

- La première dimension consiste dans le cadre de gouvernance. Elle est structurante, de haut niveau, et susceptible d'évoluer sur une échelle « long terme »,

Cela englobe : Le pilotage de la sécurité à son niveau stratégique, la gouvernance mise en œuvre et le pilotage de l'amélioration continue.

- La deuxième dimension de la PSI est fonctionnelle, susceptible d'évoluer sur une échelle « moyen terme ».

Cela porte sur : Les objectifs de sécurité, les indicateurs associés, les besoins de l'organisation en termes de sécurité de l'information.

Ces deux dimensions réunies constituent le corpus complet de la Politique de Sécurité d'Information.

- **Révision** ;

La présente Politique doit être révisée, à minima chaque année ou sur proposition de la Secrétaire Générale.

La proposition de modification est justifiée, par exemple, par un changement d'environnement, de contexte règlementaire, d'organisation structurante ou encore un changement de stratégie, voire en cas de survenance d'incidents majeurs.

- **Validation** ;

La politique est validée par la Direction Générale avant de pouvoir être mise en application.

- **Communication** ;

Le Groupe POZEO s'engage à communiquer aux parties intéressées la présente politique ainsi que toute information utile dans le cadre de l'application de cette politique en cas de demande justifiée après signature d'un engagement de confidentialité.

- **Diffusion** ;

La politique validée est accessible à l'ensemble du personnel du Groupe POZEO ou travaillant à son profit. Elle est remise aux prestataires de services et fournisseurs pour s'assurer de son applicabilité dans les services qu'ils produisent.

4. Exigence de la Politique de Sécurité de l'Information

4.1. Organisation

L'organisation mise en place par Groupe POZEO est garante de la bonne gestion de la sécurité de l'information.

Elle s'appuie sur des acteurs et une comitologie permettant d'assurer le suivi de la gestion de la sécurité du Système d'Information, tant en termes d'alignement que de suivi des objectifs opérationnels.

Les missions et les responsabilités des différents acteurs sont définies dans des fiches de fonction qui recouvrent l'ensemble des besoins de sécurité.

4.2. Pilotage et suivi

La Sécurité de l'Information est pilotée par des acteurs se réunissant à l'occasion de comités de sécurité. Ces comités rassemblent des acteurs pertinents selon les sujets abordés par le comité.

Les acteurs du pilotage de la sécurité se réunissent :

- Semestriellement : lors des Comex pour le suivi des indicateurs stratégiques de pilotage de la sécurité
- Annuellement : en revue de direction annuelle SMSI du pilotage global de la sécurité.

4.3. Gestion des risques

Le Groupe POZEO établit et maintien la Cartographie des Risques de Sécurité lui permettant d'identifier et d'apprécier ses risques.

La Cartographie des Risques de Sécurité est mise à jour dans le cadre d'un processus permettant :

- Une revue complète annuelle,
- Une mise à jour continue à l'occasion de chaque projet d'évolution du Système d'Information par l'identification des enjeux de sécurité dans tous les projets et une analyse détaillée pour les projets les plus sensibles.

4.4. Informations documentées

Le Groupe POZEO s'assure de la création et du maintien du socle documentaire afférent à la gestion de la sécurité de l'information.

La réalisation de ce corpus documentaire s'appuie sur les normes et référentiels documentaires en vigueur dans le domaine de la sécurité de l'information.

4.5. Mesures de sécurité

La réalisation de la Politique de Sécurité de l'Information s'appuie sur les lignes directrices et stratégiques applicables au Groupe POZEO. Elles se composent de directives qui contiennent des mesures issues de la norme ISO/IEC 27001 : 2022 et des meilleures pratiques associées à ces mesures selon les domaines suivants :

- **Mesures de sécurité organisationnelles**,

- **Mesures de sécurité applicables aux personnes**,
- **Mesures de sécurité physique**,
- **Mesures de sécurité technologiques**.

Les thématiques qui y sont mentionnées portent en particulier sur :

1. Politiques de Sécurité de l'Information : cela concerne l'implication de la hiérarchie et l'existence d'un processus pour la mise en place de mesures et procédures de sécurité qui doivent être respectées pour la protection de l'information ainsi que de son environnement.

2. Organisation de la Sécurité de l'Information : il en va de la nécessité de disposer au sein du Groupe POZEO d'un groupe de personnes dédié à la mise en place et au contrôle de mesures de sécurité qui seront publiées sous forme de directives et de standards. Ce groupe définit aussi la sécurité des accès par des tiers et en cas de sous-traitance.

3. Sécurité des Ressources Humaines : sont décrites les mesures de formation et de sensibilisation du personnel, ainsi que les dispositions à prendre lors d'incidents de sécurité ou de défauts de fonctionnement.

4. Gestion des actifs : cela revient à décrire comment répertorier l'ensemble des actifs du Groupe POZEO et de ses clients et comment les classifier. Il s'accompagne de directives et de moyens pour la mise en œuvre des procédures de traitement selon la classification établie.

5. Contrôle d'accès : on définit la mise en place d'une gestion des utilisateurs et de leur droit d'accès aux informations. Les procédures de sécurité concernant le travail à distance sont elles aussi définies.

6. Cryptographie : cela porte sur les mesures à respecter afin de garantir une utilisation correcte de la cryptographie.

7. Sécurité physique et environnementale : concerne toutes les mesures utilisées pour protéger les lieux et les équipements traitant l'information.

8. Sécurité liée à l'exploitation : cela traite des procédures d'exploitation sécurisées des informations.

9. Sécurité des communications : cela doit garantir la protection de l'information sur les réseaux et des moyens de traitements de l'information sur lesquelles elle s'appuie.

10. Acquisition, développement et maintenance des Systèmes d'Information : on y définit les exigences de sécurité des systèmes (mesures cryptographiques, sécurité des fichiers et des connexions, moyens de sécurité incorporés dans les applications, etc.) ainsi que les procédures pour les tests et l'intégration de nouveaux logiciels dans un système déjà opérationnel.

11. Relation avec les fournisseurs : toutes les mesures destinées à maintenir le niveau de sécurité de l'information et de service conforme aux accords conclus entre fournisseurs.

12. Gestion des incidents liés à la Sécurité de l'Information : traite des procédures mises en œuvre pour détecter et enregistrer dès que possible les incidents de sécurité afin de les analyser et déclencher des mesures appropriées pour résoudre tout problème éventuel. Il décrit aussi la nécessité de classifier ces incidents et de les signaler par le biais d'une organisation appropriée.

13. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité : cela concerne les mesures à intégrer dans le plan de continuité d'activité pour assurer la continuité de la sécurité en cas de sinistre.

14. Conformité : mise en place de procédures pour le déroulement d'audits de contrôle dans un cadre de règlements et de lois s'appliquant aux informations manipulées et à l'environnement du Groupe POZEO.

4.6. Indicateurs de pilotage

Les indicateurs sont indispensables au pilotage de toute activité. Pour suivre la bonne mise en œuvre de la gestion de la sécurité de l'Information, le Groupe POZEO a défini plusieurs indicateurs de haut niveau :

- La couverture de la Cartographie des Risques de Sécurité exprimant le niveau de connaissance des besoins de sécurité à l'échelle de l'organisation,
- La tenue et le suivi des différents comités exprimant le suivi permanent de la gestion de la sécurité de l'Information à tous les niveaux de l'organisation,
- La mise en œuvre du plan d'action sécurité exprimant le suivi des projets opérationnels permettant la sécurisation effective de l'organisation.

4.7. Revue et audits

Le Groupe POZEO met en œuvre des processus pour mesurer le niveau d'application de la PSI, le niveau de conformité par rapport aux réglementations applicables et la recherche de l'amélioration continue.

Des revues indépendantes des aspects organisationnels et techniques du SMSI doivent être menées lors de l'audit interne ou par suite de changements majeurs. Elles sont planifiées et réalisées sous la responsabilité de la Secrétaire Générale.

4.8. Charte utilisateur

La charte utilisateur est un complément des textes officiels et légaux. Adoptée dans les mêmes conditions que le règlement intérieur du Groupe POZEO, cette charte fait partie intégrante de celui-ci.

Elle fixe les conditions d'accès et les règles d'utilisation des moyens informatiques, des données personnelles et des ressources extérieures via les outils de communication du GROUPE POZEO et de ses filiales.

Les utilisateurs sont priés de prendre connaissance de cette charte et en accusant réception de cette charte, ils s'engagent à en respecter toutes les prescriptions.