INTESCIA
DATA FOR SUCCESS

Politique Générale de Sécurité des Systèmes d'Information

(PGSSI)

Lettre de la Direction Générale concernant la cybersécurité

La sécurité des systèmes d'information occupe une place de plus en plus centrale dans les activités du Groupe Intescia. Nos services numériques, nos plateformes SaaS et les données que nous traitons constituent aujourd'hui des actifs essentiels, tant pour notre fonctionnement interne que pour les services que nous fournissons à nos clients.

Dans un contexte marqué par l'accélération des usages numériques, l'augmentation des menaces cyber et le renforcement des exigences réglementaires, la sécurité ne peut plus être abordée uniquement comme un sujet technique. Elle relève pleinement de la gouvernance de l'entreprise, de la maîtrise des risques et de la relation de confiance que nous entretenons avec nos clients et partenaires.

La présente Politique Générale de Sécurité des Systèmes d'Information a pour objectif de formaliser un cadre commun et lisible en matière de sécurité. Elle traduit la volonté de la direction de définir des principes clairs, adaptés aux réalités opérationnelles du Groupe Intescia, à son modèle SaaS et à la diversité de ses environnements techniques, qu'ils soient hébergés dans le cloud ou au sein d'infrastructures locales.

Cette politique ne vise pas à figer un dispositif définitif ni à détailler l'ensemble des mesures mises en œuvre. Elle a vocation à poser des orientations de haut niveau, à structurer les pratiques existantes et à servir de socle aux politiques et procédures internes plus opérationnelles. Elle s'inscrit dans une démarche pragmatique, progressive et proportionnée, tenant compte à la fois des enjeux propres à l'entreprise et des attentes de sécurité généralement exprimées par nos clients, notamment dans des contextes de grands comptes ou d'environnements régulés.

La sécurité des systèmes d'information est une responsabilité partagée. Elle repose sur l'implication de la gouvernance, des équipes techniques, des équipes produit, mais aussi de l'ensemble des collaborateurs et partenaires qui contribuent aux activités du Groupe Intescia. Cette politique constitue un cadre de référence commun destiné à favoriser une compréhension partagée des enjeux et des principes de sécurité.

La direction du Groupe Intescia affirme, à travers ce document, son engagement à soutenir et à faire évoluer dans le temps un dispositif de sécurité cohérent avec les ambitions de l'entreprise, ses activités et les exigences de son environnement.

Christophe Vanackère

Président / CEO – INTESCIA

SOMMAIRE

1. Objectif et portée du document

La présente Politique Générale de Sécurité des Systèmes d'Information (PGSSI) a pour objet de définir les principes, orientations et objectifs généraux retenus par le Groupe Intescia en matière de sécurité des systèmes d'information, dans le cadre de la protection de ses systèmes, de ses services SaaS, de ses infrastructures hybrides (cloud et on-premise) et des données qu'il traite.

Elle s'applique à l'ensemble des activités, systèmes, infrastructures, services numériques et données relevant du Groupe Intescia, ainsi qu'aux personnes, entités et tiers intervenant dans ces environnements. Elle couvre Intescia One ainsi que l'ensemble des filiales du Groupe.

Sont notamment concernés, sans que cette liste soit limitative, les plateformes SaaS exploitées par le Groupe Intescia, les environnements de production, de développement et de test, les outils internes, ainsi que les données traitées pour le compte de ses clients.

La présente PGSSI constitue un cadre de référence de niveau général. Elle est déclinée et complétée par la Politique de Sécurité des Systèmes d'Information (PSSI), ainsi que par l'ensemble des politiques, règles et procédures internes associées, lesquelles en précisent les modalités de mise en œuvre.

Le présent document est communiqué à titre informatif et ne présente aucun caractère contractuel. Il ne saurait être interprété comme constituant un engagement de résultat, une garantie ou une obligation spécifique à l'égard de tiers. Seuls les engagements expressément stipulés dans les documents contractuels applicables sont opposables au Groupe Intescia. En cas de contradiction entre les stipulations du présent document et celles d'un document contractuel, ces dernières prévaudront.

La PGSSI est accessible publiquement afin de partager les principes et orientations du Groupe Intescia en matière de sécurité des systèmes d'information avec ses clients, partenaires et parties prenantes.

2. Contexte et enjeux

Le Groupe Intescia conçoit et exploite des solutions SaaS et des services numériques fondés sur la collecte, l'analyse, l'enrichissement et la valorisation de données, dans des environnements techniques hybrides combinant des infrastructures cloud et des ressources hébergées en datacenter.

Dans ce contexte, la sécurité des systèmes d'information vise à contribuer au maintien d'un niveau de protection cohérent et adapté des environnements techniques exploités par le Groupe Intescia, qu'ils soient hébergés dans des infrastructures cloud ou au sein de ressources locales.

Elle s'inscrit dans une approche globale visant à maintenir un niveau de sécurité en adéquation avec les enjeux et les risques associés aux activités du Groupe Intescia.

Le Groupe Intescia s'inscrit dans une démarche de transparence vis-à-vis de ses clients et partenaires concernant ses pratiques de sécurité.

La présente PGSSI a été élaborée en tenant compte des enjeux propres aux activités du Groupe Intescia ainsi que des attentes et exigences de sécurité exprimées par ses clients, dans un objectif de confiance et de maîtrise des risques.

3. Cadre réglementaire et référentiels

La démarche de sécurité du Groupe Intescia s'inscrit dans une démarche d'alignement progressive avec les cadres réglementaires et référentiels reconnus, applicables aux services numériques et data délivrées, notamment :

- ISO/IEC 27001 : relative au système de management de la sécurité de l'information.
- ISO/IEC 27002 : relative aux mesures de sécurité opérationnelles qui en découlent.
- ISO/IEC 27005 : relative à la gestion des risques de sécurité de l'information.
- ISO/IEC 27017 : relative aux contrôles de sécurité applicables aux services cloud.
- EBIOS Risk Manager : méthode d'analyse et de gestion des risques de sécurité de l'information développée par l'ANSSI, alignée avec la norme ISO/IEC 27005.
- NIS 2 : directive européenne relative à la cybersécurité des entités essentielles et importantes.
- DORA : règlement européen sur la résilience opérationnelle numérique des entreprises du secteur financiers.
- Data Act : règlement européen encadrant l'accès, le partage et l'utilisation des données.
- AI Act : règlement européen encadrant l'usage de l'intelligence artificielle
- RGPD : règlement européen relatif à la protection des données à caractère personnel.

Ces cadres et référentiels sont pris en compte comme références d'orientation, de manière proportionnée aux enjeux, aux risques et au contexte opérationnel des activités du Groupe Intescia et de ses clients.

4. Principes directeurs de la sécurité de l'information

La sécurité des systèmes d'information du Groupe Intescia repose sur les principes directeurs suivants :

Principe	Description
Confidentialité	Les informations et données font l'objet de mesures visant à les protéger contre tout accès non autorisé, en fonction de leur sensibilité.
Intégrité	Les données, modèles et systèmes font l'objet de mesures visant à limiter les altérations non autorisées ou non maîtrisées.
Disponibilité	Les systèmes et services sont conçus dans l'objectif de contribuer à la disponibilité des informations et des services nécessaires aux activités.
Traçabilité	Les actions significatives réalisées sur les systèmes et services peuvent faire l'objet de mécanismes de journalisation destinés à favoriser la traçabilité et l'analyse en cas d'incident.
Maîtrise des accès	Les accès sont accordés selon le principe du moindre privilège et adaptés aux rôles et aux responsabilités.
Responsabilité	Chaque partie prenante est responsable du respect des règles de sécurité applicables à son périmètre, dans le cadre de ses activités.
Gestion des risques	Les décisions de sécurité s'appuient sur des analyses de risques.
Résilience	Les systèmes et services intègrent des mécanismes permettant d'anticiper, détecter et gérer les incidents ou perturbations dans l'objectif de contribuer à la continuité des activités.
Protection des données	Les données sont traitées dans le respect des exigences réglementaires et contractuelles applicables, selon des modalités définies dans les dispositifs internes.
Sécurité dès la conception	La sécurité est prise en compte dès la conception et tout au long du cycle de vie des services numériques et des systèmes intégrant des technologies d'intelligence artificielle
Amélioration continue	Le dispositif de sécurité évolue en fonction du contexte, des menaces et des retours d'expérience.

Ces principes guident l'ensemble des décisions relatives à la sécurité de l'information.

5. Gouvernance de la sécurité de l'information

La sécurité de l'information est intégrée dans la gouvernance globale du Groupe Intescia.

La direction définit les orientations générales et soutient la mise en œuvre d'un dispositif de sécurité adapté aux enjeux de l'entreprise.

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) coordonne la démarche de sécurité, contribue à l'analyse des risques, participe au pilotage du dispositif de sécurité et accompagne les équipes dans la mise en œuvre des mesures de sécurité.

Le SMSI s'appuie sur une collaboration entre les équipes techniques, produit, opérations et, lorsque nécessaire, les fonctions juridiques et de protection des données.

Le dispositif de sécurité s'inscrit dans une logique de pilotage et de suivi, permettant d'adapter les orientations de sécurité en fonction des risques, des évolutions du contexte et des retours d'expérience.

6. Gestion des risques numériques

Le Groupe Intescia adopte une approche structurée de gestion des risques numériques. Cette démarche vise à identifier, analyser et traiter les risques susceptibles d'affecter les systèmes, les services et les données.

L'analyse des risques prend notamment en compte les actifs critiques, les menaces et vulnérabilités identifiées, les impacts potentiels sur les activités et les clients, ainsi que les dépendances technologiques et les tiers.

Les mesures de sécurité mises en œuvre sont adaptées au niveau de risque identifié et peuvent évoluer en fonction du contexte, des menaces et des retours d'expérience.

7. Sécurité des systèmes d'information

La sécurité des systèmes d'information vise à contribuer au maintien d'un niveau protection cohérent et adapté des environnements techniques exploités par le Groupe Intescia, qu'ils soient hébergés dans des infrastructures cloud ou au sein de ressources locales.

Elle s'inscrit dans une approche globale visant à maintenir un niveau de sécurité adapté aux enjeux et aux risques associés aux activités du Groupe Intescia.

Elle couvre notamment :

- La protection des infrastructures, systèmes et environnements techniques.
- La gestion des vulnérabilités et des mises à jour de sécurité.
- La supervision et la détection d'événements de sécurité.
- La sauvegarde, la restauration et la protection des données.

- La prise en compte des spécificités liées aux différents modes d'hébergement.

Ces principes contribuent à préserver la disponibilité, l'intégrité et la confidentialité des systèmes d'information supportant les activités et services du Groupe Intescia.

8. Gestion des accès et des identités

La gestion des accès aux systèmes et services du Groupe Intescia repose sur des principes de sécurité visant à limiter l'exposition aux risques et à protéger les ressources et données sensibles.

Elle s'appuie notamment sur :

- Le principe du moindre privilège, selon lequel les accès sont limités aux droits strictement nécessaires aux missions confiées.
- Des mécanismes de contrôle des accès adaptés aux contextes et aux environnements.
- La prise en compte du cycle de vie des identités, depuis leur création jusqu'à leur modification et leur suppression.
- L'adaptation des mécanismes d'authentification et de contrôle en fonction de la sensibilité des ressources et des usages.

Ces principes contribuent à limiter les risques liés aux accès non autorisés et aux usages inappropriés des systèmes et services.

9. Sécurité des services et des données

La sécurité des services et des données couvre les services numériques fournis par Le Groupe Intescia ainsi que les données traitées dans ce cadre.

Elle vise à définir, au niveau des principes, la manière dont les enjeux de sécurité sont pris en compte lors de la conception, de l'évolution et de l'exploitation des services SaaS, ainsi que dans l'usage et la protection des données associées.

Ces principes ont pour objectif de renforcer la confiance des clients, de limiter les risques liés à l'utilisation des services numériques, ainsi qu'à contribuer à la protection des données et des services numériques.

10. Usage de l'intelligence artificielle

Le Groupe Intescia peut s'appuyer sur des technologies d'intelligence artificielle dans le cadre de ses activités, notamment pour la conception, l'exploitation et l'amélioration de ses services numériques et de ses solutions SaaS.

Dans ce contexte, l'utilisation de ces technologies s'inscrit dans une démarche globale de sécurité de l'information, de gestion des risques et de prise en compte des exigences réglementaires applicables.

Les principes suivants guident l'usage de l'intelligence artificielle au sein du Groupe Intescia :

- La prise en compte des enjeux de sécurité de l'information dans l'utilisation des systèmes d'intelligence artificielle, notamment en matière de confidentialité, d'intégrité et de disponibilité des données ;
- L'identification et l'évaluation des risques liés aux usages de l'intelligence artificielle, incluant notamment les risques liés aux données, aux modèles et aux dépendances technologiques ;
- La prise en compte des exigences réglementaires applicables, notamment en matière de protection des données et de réglementation relative à l'intelligence artificielle ;
- L'encadrement des usages des outils intégrant des fonctionnalités d'intelligence artificielle, en fonction des contextes d'utilisation et des niveaux de sensibilité ;
- L'intégration des principes de sécurité dès la conception et tout au long du cycle de vie des systèmes utilisant des technologies d'intelligence artificielle.

Ces principes ont vocation à être déclinés et précisés dans les politiques et procédures internes applicables.

11. Gestion des incidents de sécurité

Le Groupe Intescia définit des principes d'organisation visant à encadrer la prise en compte des événements de sécurité susceptible d'affecter les systèmes, les services numériques ou les données.

Ces principes contribuent à limiter les impacts potentiels sur les activités, les services et les parties prenantes, ainsi qu'à maintenir la confiance de ses clients.

Les situations de sécurité significatives peuvent être analysées, le cas échéant, afin d'alimenter la réflexion et l'évolution du dispositif de sécurité.

Lorsque requis, les obligations réglementaires ou contractuelles applicables sont prises en compte.

12. Continuité d'activité et résilience

La sécurité des systèmes d'information intègre des principes de continuité et de résilience visant à renforcer la capacité du Groupe Intescia à faire face aux situations de perturbation susceptibles d'affecter ses activités ou ses services numériques.

Ces principes tiennent compte de la nature des services fournis, de la diversité des environnements techniques exploités, ainsi que des dépendances internes et externes associées.

Ils ont pour objectif d'orienter la réflexion et les choix relatifs à la résilience des services, sans préjuger des modalités opérationnelles mises en œuvre.

13. Gestion des tiers et partenaires

Les activités du Groupe Intescia peuvent s'appuyer, le cas échéant, sur des prestataires, partenaires ou fournisseurs intervenant dans la conception, l'exploitation ou l'hébergement de ses services numériques.

La présente politique définit des principes de prise en compte des enjeux de sécurité liés aux relations avec les tiers, en fonction de la nature des services concernés, des niveaux d'accès et des risques associés.

Ces principes visent à contribuer à la maîtrise des risques au sein de l'écosystème numérique du Groupe Intescia, sans se substituer aux dispositions contractuelles ou aux politiques internes applicables.

14. Protection des données

La protection des données constitue un enjeu majeur pour Le Groupe Intescia, compte tenu de la nature de ses activités et des services numériques qu'elle propose.

Les principes définis dans la présente politique contribuent à la protection des données traitées, qu'il s'agisse de données propres à l'entreprise ou de données traitées pour le compte de ses clients.

Les traitements de données sont réalisés en tenant compte des exigences réglementaires applicables et des engagements contractuels définis, selon des modalités précisées dans des documents internes dédiés.

15. Amélioration continue

La sécurité des systèmes d'information s'inscrit dans une démarche d'amélioration continue, visant à faire évoluer le dispositif de sécurité aux besoins du Groupe Intescia, à l'évolution de ses activités et à son environnement de menaces.

La présente politique a vocation à être revue et ajustée régulièrement afin de rester en adéquation avec les enjeux identifiés, les retours d'expérience et les évolutions du contexte réglementaire et technologique.

16. Approbation

La présente Politique Générale de Sécurité des Systèmes d'Information est approuvée dans le cadre de la gouvernance du Groupe Intescia.

Elle fait l'objet d'une validation formelle par les fonctions suivantes :

Fonction	Signature	Date
CEO	Signé par : 274C0CB53E064B3...	28/5/2026 | 16:38 CEST
CTO	Signed by: 2E640306E410436... Baptiste Bouffaut	28/5/2026 | 16:38 CEST
DSI	Signé par : Vincent Waroquier	28/5/2026 | 16:38 CEST
RSSI	Signé par : 2F180D0B5A9A47C...	28/5/2026 | 16:38 CEST

Elle entre en vigueur à compter de sa date de validation.

Elle est susceptible d'être revue et mise à jour afin de rester en adéquation avec les évolutions du contexte et des enjeux de sécurité.

Cette approbation est formalisée au moyen d'un processus de signature électronique, garantissant l'intégrité et l'authenticité du document.

17. Annexes

17.1. Historique du document

Version	Modifications	Auteur	Validation	Date
1.3	- Validation du document	RSSI	Direction	Mai 2026
1.2	- Usage de l'IA	RSSI	-	Mars 2026
1.1	- Annexes	RSSI	-	Janvier 2026
1.0	- Rédaction du document	RSSI	-	Octobre 2025

17.2. Table des abréviations

Abréviation	Définition
PGSSI	Politique Générale de Sécurité des Systèmes d'Information
SMSI	Système de Management de la Sécurité de l'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Système d'Information

ANSSI	Agence nationale de la sécurité des systèmes d'information
RGPD	Règlement Général sur la Protection des Données
NIS 2	Network and Information Security 2
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ISO	International Organization for Standardization