Informations sur l'entreprise
Politique de sécurité

Table des matières

Contrôle des documents

Table des matières

Contrôle des documents

Nom du document	Politique de sécurité de l'information de l'entreprise
Classification	INTERNE
Numéro de révision	3.5
Date de révision	05/12/2024
Dépositaire	Responsable de la sécurité des entreprises
Approbation	Insights IS Forum
Audit	Annuel : Gestionnaire de sécurité d'entreprise
Prochaine révision	Décembre 2025

1. Vue d'ensemble

Cette politique est basée sur la norme ISO 27001:2022, la norme internationale reconnue en matière de sécurité de l'information. Cette norme garantit qu'Insights respecte les principes de sécurité suivants :

Confidentialité Toutes les informations sensibles sont protégées contre l'accès ou la divulgation non autorisés.

Intégrité Toutes les informations sont protégées contre toute altération ou destruction accidentelle, malveillante ou frauduleuse,

Disponibilité Les services d'information seront disponibles pendant les périodes convenues avec les utilisateurs et seront protégés contre les dommages accidentels ou malveillants ou contre le déni de service.

2. Objet de l'action

L'objectif de cette politique est de démontrer l'engagement d'Insights Learning and Development envers la sécurité des données dont il est responsable et de démontrer les contrôles et les responsabilités en place pour soutenir le système de gestion de la sécurité de l'information (SGSI), dont le cadre principal est la norme ISO 27001:2022.

3. Champ d'application

Le champ d'application de cette politique couvre toutes les parties internes et externes et soutient l'engagement continu d'Insights en faveur de la norme ISO 27001:2022.

4. Politique

4.1 Responsabilités de l'exécutif

L'exécutif d'Insights s'engage à satisfaire toutes les exigences applicables dans le cadre de cette politique et à améliorer continuellement le système de gestion de la sécurité de l'information (ISMS), et a donc établi cette politique de sécurité de l'information de manière à ce que :

- il est adapté à l'objectif d'Insights ;
- il comprend des objectifs en matière de sécurité de l'information et fournit un cadre pour la définition d'objectifs continus en matière de sécurité de l'information.

Cette politique de sécurité de l'information doit être disponible sous forme d'informations documentées, être communiquée au sein d'Insights et être mise à la disposition des parties intéressées, le cas échéant.

Le respect de cette politique et de toutes les autres politiques et procédures de sécurité est obligatoire pour l'ensemble du personnel.

Le directeur général approuve cette politique. Le Forum de la sécurité de l'information est chargé de veiller à ce que la politique soit mise en œuvre et respectée dans l'ensemble des activités couvertes par le SGSI.

4.2 Leadership et engagement

L'exécutif continuera à faire preuve de leadership et d'engagement en ce qui concerne le SGSI :

- veiller à ce que la politique et les objectifs en matière de sécurité de l'information soient établis et compatibles avec l'orientation stratégique de l'entreprise Insights ;

- assurer l'intégration des exigences du SGSI dans les processus d'Insights ;
- veiller à ce que les ressources nécessaires au SMSI soient disponibles ;
- communiquer l'importance d'une gestion efficace de la sécurité de l'information et de la conformité aux exigences du SMSI ( ) ;
- veiller à ce que le SMSI atteigne le(s) résultat(s) escompté(s) ;
- diriger et soutenir les personnes qui contribuent à l'efficacité du SMSI ;
- promouvoir l'amélioration continue et aider les autres fonctions de gestion concernées à démontrer leur leadership dans leurs domaines de responsabilité.

4.3 Objectifs de sécurité de l'information

Des objectifs en matière de sécurité de l'information ont été définis et sont compatibles avec l'orientation stratégique d'Insights. L'objectif principal est de travailler en conformité avec les sections de la norme de bonnes pratiques ISO 27001:2022 détaillées ci-dessous.
En outre, les objectifs de sécurité seront fixés par le forum sur la sécurité de l'information en tant que tâche permanente et lors des réunions d'examen de la gestion du SMSI.

4.4 Amélioration continue du cadre du SMSI

Insights s'efforcera d'améliorer en permanence le système de gestion de la sécurité de l'information conformément à une approche PLAN-DO-CHECK-ACT visant à améliorer les processus intégrés dans son SGSI.

L'importance accordée à la sécurité de l'information est démontrée par l'existence du Forum sur la sécurité de l'information ;

- l'examen et l'avancement des questions stratégiques de sécurité ;
- établir des relations en dehors d'Insights avec d'autres conseillers en matière de sécurité ;
- évaluer l'impact des nouvelles exigences légales ou réglementaires qui nous sont imposées ;
- contrôler l'efficacité du SGSI, par exemple à partir des résultats des rapports d'audit interne et des rapports sur les incidents de sécurité ;
- recommander/approuver des modifications du SGSI.

Le Forum sur la sécurité de l'information se réunit régulièrement pour examiner les activités susmentionnées afin d'assurer l'efficacité continue du SGSI d'Insights. Le processus de révision est défini dans la "Politique de révision de la gestion du Forum sur la sécurité de l'information".

La présente politique de sécurité de l'information de l'entreprise confirme l'engagement d'Insights en faveur d'une amélioration continue et met en évidence les domaines clés (appelés "thèmes") permettant de sécuriser efficacement ses informations, à savoir

- Contrôles organisationnels
- Contrôle des personnes
- Contrôles physiques
- Contrôles technologiques

4.5 Contrôles organisationnels

Les contrôles organisationnels relèvent de la responsabilité du Forum sur la sécurité de l'information et portent sur les domaines suivants :

- Politiques stratégiques de sécurité de l'information - qui couvre la présente politique, la politique des objectifs de sécurité et la politique de communication.
- Rôles et responsabilités - le responsable de la sécurité de l'entreprise préside le forum sur la sécurité de l'information.
- Gestion des identités et des accès - le responsable de la sécurité de l'entreprise et les chefs d'équipe sont chargés d'établir et de maintenir des contrôles d'accès logiques solides. Une politique appropriée est en place et doit être respectée par l'ensemble du personnel et des parties externes.
- Gestion des actifs - Les informations Insights doivent être classées en fonction de leur sensibilité et un propriétaire de l'information doit être désigné. Le responsable de la sécurité de l'entreprise tiendra un inventaire des actifs informationnels, qui sera mis à jour périodiquement, en fonction de leur profil de risque et protégé en conséquence.
- Relations - Les exigences en matière de sécurité de l'information visant à atténuer le risque

associé à l'accès du fournisseur aux actifs Insights doivent être convenues avec le fournisseur et documentées.

- Les accords avec les fournisseurs d'informatique en nuage doivent être établis, documentés et faire l'objet d'une révision permanente.
- Gestion des incidents - Les dossiers de gestion des incidents de sécurité doivent être centralisés, mis à jour et contrôlés en permanence. Tous les employés doivent savoir ce qui constitue un incident de sécurité réel ou potentiel, comment signaler l'incident et à qui le signaler. La responsabilité de la surveillance de toutes les failles de sécurité incombe au responsable de la sécurité de l'entreprise.
- Gestion de la continuité des activités - Insights doit garantir une approche cohérente et efficace de la gestion des incidents majeurs en matière de sécurité de l'information, y compris la communication sur les événements et les faiblesses en matière de sécurité et les implications pour la gestion de la continuité des activités.

- Conformité - Insights doit éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles liées à la sécurité de l'information et de toute exigence en matière de sécurité. Insights doit prendre des mesures techniques et organisationnelles pour protéger les données personnelles contre la destruction accidentelle ou illégale, la perte ou l'altération accidentelle, la divulgation ou l'accès non autorisé. En particulier, Insights doit prendre des mesures visant à garantir que :

    - Toute personne qui gère et traite des données à caractère personnel comprend qu'elle est contractuellement responsable du respect des bonnes pratiques en matière de protection des données.
    - Toutes les personnes qui gèrent et manipulent des données à caractère personnel sont formées de manière appropriée à cet effet ; et
    - Toutes les personnes qui gèrent et manipulent des données à caractère personnel sont supervisées de manière appropriée.

4.6. Contrôle des personnes

Les contrôles des personnes relèvent de la responsabilité de l'équipe des ressources humaines et portent sur les domaines suivants :

- Tous les employés doivent signer le manuel de l'employé qui les oblige à travailler conformément à toutes les politiques et procédures, y compris les exigences spécifiques en matière de sécurité de l'information.
- Une politique de sécurité des informations personnelles permet de s'assurer que les employés sont conscients qu'ils sont tenus de suivre les meilleures pratiques en matière de sécurité de l'information.
- Il existe également une procédure pour tous les employés qui quittent Insights (y compris les employés temporaires et contractuels) afin de désactiver leur compte réseau et de récupérer tous leurs biens.
- Tous les nouveaux employés (permanents, temporaires et contractuels) doivent être formés aux procédures dans les domaines décrits ci-dessus dans le cadre de leur programme d'initiation. Une formation continue doit être assurée sous la forme d'un programme de mises à jour régulières et de sessions de formation par le forum sur la sécurité de l'information.

4.7 Contrôles physiques

Les contrôles physiques relèvent de la responsabilité de l'équipe chargée des installations et portent sur les domaines suivants :

- Le personnel doit connaître et suivre l'ensemble détaillé des mesures, contrôles et procédures mis en place pour assurer un contrôle adéquat de la sécurité physique. Ces mesures, contrôles et procédures sont les suivants

    - les systèmes d'alarme et de vidéosurveillance des bâtiments
    - accès restreint au bâtiment et accès encore plus restreint à l'intérieur de celui-ci
    - casiers, tiroirs, coffres-forts et rangements sécurisés, rangements ignifugés
    - sauvegardes et archivages sécurisés hors site
    - un bureau et un écran dégagés

- les procédures pour l'émission de tout média
- la nécessité d'un contrôle permanent de toutes les mesures de sécurité physique

4.8. Contrôles technologiques

Les contrôles technologiques relèvent de la responsabilité de l'équipe Technologie et Sécurité de l'entreprise et portent sur les domaines suivants :

- Tous les dispositifs d'extrémité doivent être protégés de manière adéquate et chiffrés le cas échéant.
- Gestion des identités et des accès - Les administrateurs des systèmes informatiques (utilisateurs privilégiés) veillent à ce que les contrôles et procédures d'accès convenus soient gérés conformément à la politique établie.
- Cryptographie - Lorsque des contrôles cryptographiques sont utilisés par Insights, une politique sur l'utilisation des contrôles cryptographiques pour la protection des informations a été développée et mise en œuvre.
- Sécurité des opérations informatiques - Insights veillera à ce que les installations de traitement de l'information fonctionnent correctement et en toute sécurité. L'équipe Technologie et Sécurité de l'entreprise effectue un contrôle permanent de toutes les activités opérationnelles informatiques.
- Sécurité des communications informatiques - le personnel doit savoir que l'utilisation des technologies et des communications est établie, contrôlée et gérée par le responsable de la sécurité de l'entreprise. Il est chargé de veiller à ce que les mesures et processus de sécurité appropriés soient en place. Insights veillera à ce que la sécurité du réseau, des points d'accès et du travail à distance soit protégée de manière adéquate.
- Sécurité du développement des systèmes informatiques - le responsable de la sécurité de l'entreprise veille à ce que les processus de sécurité de l'information appropriés soient inclus dans tous les projets. Une approche de développement sécurisée comprenant une politique, des procédures, un environnement et des tests est en place.

4.9. Période de révision de la politique

Le forum sur la sécurité de l'information réexaminera la présente politique au moins une fois par an.

5. Conformité de la politique

Mesure de la conformité : L'équipe de sécurité et/ou le forum de la sécurité de l'information vérifieront le respect des points suivants

- la présente politique par le biais de diverses méthodes, y compris, mais sans s'y limiter, des visites périodiques, une surveillance vidéo,
- les rapports sur les outils de gestion, les audits internes et externes, et le retour d'information au propriétaire de la politique.

Exceptions : Toute exception à cette politique doit être approuvée par le dépositaire de la politique et l'approbateur.

En cas d'absence, comme un congé annuel, la responsabilité en incombera à un membre du personnel de garde et/ou du personnel de l'administration centrale er/ou desapprobateurs hiérarchique ou Forum de la sécurité de l'information.

Non-conformité : Un employé qui a violé cette politique et qui a un impact sur la réputation des Insights.

L'apprentissage et le développement ou le groupe Insights au sens large peuvent faire l'objet de mesuresdisciplinaires pouvant aller jusqu'à et

y compris le licenciement.

6. Normes, politiques et processus associés

Objet	Int ou Ext	Titre du document
1	Interne	Système de gestion des documents ISMS
2		
3		
4		
5		
6		

7. Définitions et termes

Non applicable

8. Historique des révisions

Révision	Date	Modifié par	Description
2.0	09/01/2020	Graham Watson	Politique approuvée par le directeur général
2.1	24/09/2021	Kevin McAuley	Modifications mineures basées sur des changements de rôles et de structures
3.0	30/11/2021	Kevin McAuley	Politique approuvée par le conseil d'administration
3.1	13/02/2023	Dave McClure	Mise à jour des politiques : ajout de nouvelles politiques
3.2	06/03/2023	Dave McClure	Rôles et responsabilités transférés dans la nouvelle politique
3.3	05/04/2023	Ian Gowen	Ajout d'un tableau de référence interne
3.4	28/04/2023	Ian Gowen	Modification de l'ordre des références internes
3.5	05/12/2024	Andy Moore	Examen annuel et approbation du directeur général

Signé : 

Date : 5e décembre 2024

Fiona Logan
Directeur général