i3-GROUP

Sécurité des données dans le Groupe

La protection des données est fondamentale pour nos opérations. Nous avons obtenu dans le group la certification ISO 27001 le 12 mai 2023, suite à la mise en œuvre d'un système complet de gestion de la sécurité de l'information (ISMS) et en répondant aux exigences de la norme du système de gestion de la sécurité de l'information : ISO/IEC 27001:2022.

Cette certification, maintenue en 2026, reflète notre engagement envers les plus hauts standards en matière de sécurité de l'information.

Notre approche multifacette de la sécurité des données comprend les mesures suivantes :

Système de gestion de la sécurité de l'information (ISS)

Nous avons développé un cadre ISMS robuste pour protéger les actifs organisationnels et assurer une amélioration continue. Les principales caractéristiques incluent :

1. Documentation claire des risques et des contrôles, mise à jour régulièrement via ISOPlanner.
2. Des audits internes en cours pour évaluer l'efficacité de l'ISMS et traiter les vulnérabilités émergentes.
3. Méthodologie complète d'évaluation des risques conforme à l'ISO 27001, axée sur l'identification, l'atténuation et le suivi des risques.

Amélioration continue (PDCA)

Nous utilisons le cycle PDCA (Plan-Do-Check-Act) pour améliorer continuellement notre Système de Gestion de la Sécurité de l'Information (ISMS), conformément aux règles de l'ISO 27001. Dans l'étape du Plan, nous examinons les risques potentiels de sécurité, fixons des objectifs et établissons des règles pour protéger les informations. Dans l'étape Do, nous mettons ces règles en pratique dans nos ISMS. Lors de l'étape de vérification, nous vérifions et testons si tout fonctionne comme prévu. Enfin, lors de l'étape Act, nous corrigeons tout problème et améliorons nos ISMS pour rester sécurisés et à jour. Après cela, le cycle recommence avec Planificer, assurant des améliorations continues de la sécurité.

Politiques de données

Pour anticiper l'évolution des menaces, nous examinons régulièrement et améliorons ses politiques de sécurité de l'information :

4. **Politique de classification de l'information :** Définit la gestion appropriée des données publiques, internes et confidentielles.
5. **Politique de contrôle d'accès :** Met en place un accès basé sur les rôles aux informations sensibles, garantissant que les données ne sont accessibles qu'au personnel autorisé.
6. **Politique de conservation des données :** Établit des directives claires pour la conservation et l'élimination sécurisée des données, réduisant ainsi l'exposition à des risques inutiles.

i3-GROUP

Intégrité des données et confidentialité

Nous garantissons l'intégrité des données stockées et transmises via :

- Validation régulière des protocoles de chiffrement, respectant les normes industrielles telles que AES-256 et TLS1.3.
- Des processus de sauvegarde sécurisés permettant une récupération fiable des données en cas de perte ou de corruption.

Formation à la cybersécurité

Pour soutenir notre politique, nous investissons dans la formation continue des employés afin d'instaurer une culture de sensibilisation à la sécurité. Les programmes incluent :

- Formation en cybersécurité spécifique à chaque poste, adaptée aux responsabilités individuelles.
- Des quiz de sensibilisation à la sécurité et des mécanismes de retour d'information pour évaluer la compréhension des employés.
- Simulations avancées de phishing pour améliorer la détection et la réponse aux menaces.

Gestion des incidents

Nous avons mis en place un cadre complet de réponse aux incidents pour traiter et résoudre rapidement les incidents de sécurité. Les éléments clés incluent :

- Des canaux de signalement d'incidents sont accessibles à tous les employés.
- Des protocoles d'escalade clairs pour impliquer les parties prenantes appropriées et minimiser les temps de réponse.
- Des revues post-mortem des incidents afin d'identifier les causes profondes et d'éviter la récidive.

i3-GROUP

Sécurité des terminaux

Pour protéger les points d'accès aux systèmes de l'entreprise, nous appliquons des mesures de sécurité strictes, notamment :

- Chiffrement obligatoire de tous les appareils, y compris ordinateurs portables, téléphones portables et tablettes.
- Capacités d'effacement à distance pour protéger les données sur les appareils perdus ou volés.
- Gestion régulière des correctifs pour garantir que les appareils restent à jour avec les derniers correctifs de sécurité.

Conformité au RGPD

La protection des données est intégrée dans tous nos systèmes et processus dès le départ. Nous respectons strictement les principes du RGPD, en veillant à :

- Collecte de données minimale et anonymisation lorsque cela est applicable.
- Chiffrement sécurisé de toutes les données personnelles, en transit comme au repos.
- Évaluations de l'impact sur la vie privée pour les nouveaux systèmes et processus qui gèrent les informations sensibles.

i3-GROUP

Nous intégrons les principes du RGPD dans tous les processus :

Registre de traitement : Nous maintenons un registre complet qui détaille toutes les activités de traitement des données, garantissant transparence et responsabilité dans la gestion des données personnelles et sensibles.

Collecte minimale de données et anonymisation : Nous limitons la collecte de données à ce qui est strictement nécessaire et anonymisons les données lorsque cela est applicable.

Évaluations d'impact sur la vie privée : Tous les nouveaux systèmes et processus supervisant les informations sensibles font l'objet d'évaluations d'impact sur la vie privée afin d'évaluer et d'atténuer les risques.

Déclaration de confidentialité : Nous fournissons des informations claires à toutes les parties prenantes sur la manière dont les données personnelles sont collectées, utilisées et protégées. La déclaration complète de confidentialité est accessible au public et définit les droits des personnes concernées, y compris l'accès, la correction et la suppression de leurs données.

En 2026, nous avons mis à jour notre Déclaration de confidentialité afin d'offrir une plus grande transparence et clarté sur la manière et les raisons pour lesquelles nous traitons les données personnelles. Cette mise à jour reflète notre engagement à mieux informer nos clients sur les types de données que nous collectons, les usages que nous utilisons et les mesures que nous prenons pour les protéger.

Politique de rétention de l'information : Nous avons une politique de conservation de l'information qui définit les périodes de conservation de toutes les informations de notre organisation.

i3-GROUP

Type de données	Période de conservation	Emplacement	Mise au rebut
Données des candidats	Maximum 4 semaines après la fin de la procédure de demande ou 1 an après la candidature, uniquement si le demandeur accepte d'être conservé dans son dossier.	Numériquement sur serveur de fichiers	Supprimer
Dossiers financiers (factures, déclarations fiscales	7 ans	Copie papier dans un placard verrouillé	Shredder
Dossiers financiers (factures, déclarations fiscales)	7 ans	Numériquement dans un système ERP	Supprimer
Dossiers du personnel (tickets de paiement, contrat)	7 ans après la fin de carrière	Numériquement dans le système RH	Supprimer
Dossiers du personnel (pièce d'identité, relevé fiscal salarial)	5 ans après la fin de la relation	Numériquement dans le système RH	Supprimer
Dossiers du personnel (formulaires de révision, ...)	1 an après la fin de vie	Numériquement sur serveur de fichiers	Supprimer
Dossiers clients	7 ans après la dernière transaction	Numériquement dans un système CRM	Supprimer
Autres records (non-concurrence, éducation, carrière, assurance)	jusqu'à la validité ou réalisation convenue	Numériquement dans le système RH	Supprimer
Code source	Illimité	Numériquement sur un ou plusieurs serveurs de fichiers	Supprimer
Email	Illimité, sauf s'il contient l'un des types de données ci-dessus	Numériquement sur le serveur de messagerie	Supprimer

i3-GROUP

Mesures pour protéger les données tierces contre l'accès non autorisé ou Divulgation

Nous adoptons une approche à plusieurs niveaux pour protéger les données tierces, en veillant à la conformité avec le RGPD et les normes ISO 27001 :

Contrôle d'accès et chiffrement

- **Contrôle d'accès basé sur les rôles (RBAC) :** L'accès aux données sensibles est réservé au personnel autorisé en fonction de ses rôles et responsabilités.
- **Normes de chiffrement :** Toutes les données tierces sont chiffrées à la fois en transit (avec TLS 1.3) et au repos (via AES-256).

Surveillance et réponse aux incidents

1. **Surveillance continue :** Nous utilisons des outils de surveillance en temps réel pour détecter les tentatives d'accès non autorisées ou les anomalies dans les systèmes tiers.
2. **Protocoles de réponse aux violations :** en cas de suspicion de violation, nous disposons d'un protocole défini, exigeant un signalement immédiat par le tiers et des efforts collaboratifs de remédiation.
3. **Traces d'audit :** Une journalisation complète garantit que tout accès et activité liés aux données tierces est auditable.

Gouvernance des données fournisseurs

Notre engagement envers la sécurité des données dépasse notre organisation pour inclure une gouvernance rigoureuse de notre chaîne d'approvisionnement. Les fournisseurs sont des partenaires essentiels pour maintenir l'intégrité et la confidentialité de nos données et nous assurons leur conformité.

Limitation du partage d'informations

Les fournisseurs n'ont accès qu'aux données nécessaires à l'exécution de leurs opérations commerciales. Ce principe de minimisation de l'exposition aux données aide à réduire le risque d'accès non autorisé ou d'utilisation abusive tout en protégeant les informations sensibles.

i3-GROUP

Protection des données et conformité

Pour garantir le respect des réglementations sur la protection des données, nous exigeons :

- **Accords de traitement des données (DPA) :** Tous les fournisseurs doivent signer des accords définissant des mesures spécifiques pour protéger les données personnelles, financières et sensibles à l'entreprise.
- **Conformité au stockage des données :** Les fournisseurs doivent stocker les données au sein de l'Union européenne ou dans des juridictions respectant les normes d'adéquation du RGPD.
- **Examens réguliers :** Nous évaluons périodiquement la conformité des fournisseurs aux politiques internes de protection des données et de sécurité lors des évaluations programmées.

Mesures de sécurité

Les fournisseurs doivent respecter des exigences de sécurité strictes, notamment :

- **Chiffrement des données :** Toutes les données doivent être chiffrées à la fois en transit et au repos en utilisant des protocoles de chiffrement standards de l'industrie.
- **Transmission sécurisée :** Les canaux de communication entre nous et les fournisseurs doivent utiliser des protocoles sécurisés tels que TLS 1.3.