Document de référencesur la sécurité

www.insights.com

Insights a investi dans un redéveloppement complet de ses plateformes technologiques, en mettant l'accent sur la sécurité et la conformité. La nouvelle plateforme client, qui est la prochaine itération d'Insights Online, met l'accent sur l'amélioration de l'expérience utilisateur et, plus important encore, sur des mesures de sécurité robustes intégrées au système. Nos applications clients ont été redéveloppées en utilisant des pratiques de codage sécurisées, un cycle de vie de développement sécurisé et des principes d'ingénierie de la sécurité, y compris des mesures telles que le cryptage et l'authentification multifactorielle. Cette approche de la protection de la vie privée et de la sécurité s'étend également à notre infrastructure d'appui.
Nous accordons une grande importance au retour d'information des utilisateurs et avons intégré les idées de nos clients dans le processus de redéveloppement. Pour l'avenir, nous nous engageons à apporter des améliorations et des mises à jour continues afin de garantir que notre plateforme reste sécurisée et conforme aux normes du secteur.

Certification ISO 27001:2022
Depuis ce réaménagement, Insights a obtenu la certification ISO 27001:2022. Cette prestigieuse certification témoigne de notre engagement à maintenir les normes les plus élevées en matière de sécurité de l'information.

Pourquoi la certification ISO 27001:2022 est-elle importante ?
La norme ISO 27001:2022 est une norme internationalement reconnue pour les systèmes de gestion de la sécurité de l'information (SGSI). L'obtention de cette certification démontre que notre organisation a mis en place un cadre solide pour gérer et protéger les informations sensibles. Elle implique une évaluation rigoureuse et une amélioration continue de nos pratiques de sécurité, garantissant que nous identifions, gérons et atténuons efficacement les risques.

Qu'est-ce que cela signifie pour nos clients ?
Une entreprise certifiée ISO 27001:2022 offre plusieurs avantages clés :

- **Une confiance accrue :** Les clients peuvent être assurés que leurs données sont traitées avec le plus grand soin et la plus grande sécurité, ce qui réduit le risque de violation des données et de cybermenaces.
- **Conformité aux réglementations :** De nombreux secteurs exigent la conformité à des normes de sécurité spécifiques. Notre certification ISO 27001:2022 aide les clients à répondre à ces exigences réglementaires.
- **Gestion des risques :** La certification signifie que nous avons une approche proactive de l'identification et de la gestion des risques de sécurité potentiels, garantissant la continuité et la résilience de l'entreprise.
- **Avantage concurrentiel :** Travailler avec une entreprise certifiée peut améliorer votre réputation et vous donner un avantage concurrentiel sur le marché, car cela témoigne d'un engagement en faveur des meilleures pratiques en matière de sécurité de l'information.
- **Amélioration continue :** Le cadre ISO 27001:2022 encourage l'évaluation et l'amélioration continues des mesures de sécurité, ce qui nous permet de rester à l'affût des nouvelles menaces et vulnérabilités.

En obtenant la certification ISO 27001:2022, Insights démontre son engagement à protéger les données des clients et à fournir un environnement sécurisé pour toutes les opérations commerciales.

Quelle est notre approche des tests de pénétration ?
Insights s'engage à fournir des solutions sécurisées à ses clients. Nous effectuons régulièrement des tests de pénétration sur nos applications en faisant appel à un fournisseur tiers approuvé par le CREST. En outre, nous appliquons les bons principes de sécurité tout au long de ces tests.

La dernière plate-forme pour les nouveaux clients a fait l'objet d'un test de pénétration d'une application web externe et ne présentait AUCUNE vulnérabilité.

Points forts en matière de sécurité

Vous trouverez ci-dessous les principaux dispositifs de sécurité que nous avons mis en place pour garantir le plus haut niveau de protection à nos clients :

Contrôle d'accès et authentification

Confiance zéro
Zero Trust est un cadre de sécurité qui exige que tous les utilisateurs, qu'ils soient à l'intérieur ou à l'extérieur du réseau Insights, soient authentifiés, autorisés et validés en permanence pour la configuration et la posture de sécurité avant de se voir accorder ou de conserver l'accès à la Nouvelle Plateforme Client. Cette approche s'aligne sur les objectifs de contrôle de la norme ISO 27001:2022, y compris le contrôle d'accès et les droits d'accès privilégiés afin d'assurer un accès "au moindre privilège".

Jeton unique
Le One Time Token empêche l'usurpation d'identité en garantissant que l'adresse électronique saisie ne peut être réutilisée, ce qui évite d'avoir à stocker des noms d'utilisateur et des mots de passe.

Signature unique
Le Single Sign-On (SSO) permet aux clients d'utiliser leurs propres fournisseurs d'identité pour sécuriser leurs utilisateurs au sein de l'application, en transférant toutes les mesures de sécurité aux systèmes de l'organisation.

Sécurité des réseaux et des infrastructures

Principe du moindre privilège
Ce principe garantit que les employés, les systèmes et les applications **n'ont que** l'accès nécessaire pour remplir leur rôle et leurs responsabilités. Les droits d'accès sont soigneusement déterminés en fonction des besoins opérationnels et des politiques de sécurité.

Pas d'IP publique
Les serveurs Insights n'ont pas de connexion directe avec l'internet, ce qui constitue une solution de sécurité périmétrique qui protège contre les menaces extérieures. Le trafic passe par un proxy sortant qui contient une liste blanche de domaines autorisés.

Équilibreur de charge d'application
Notre application Load Balancer gère le trafic internet, agissant comme une barrière entre l'internet et les serveurs. Il veille à ce que seul le trafic autorisé puisse communiquer avec le portail Insights et utilise toujours les derniers chiffrages et protocoles de sécurité SSL/TLS.

Surveillance et rejet du trafic suspect
Tout le trafic HTTP entrant passe par un pare-feu d'application Web (WAF) et le trafic suspect est automatiquement rejeté. Des notifications sont envoyées à notre équipe technologique pour qu'elle mène une enquête, ce qui garantit une gestion proactive des menaces.

Gestion rapide des correctifs logiciels
Tous nos environnements d'hébergement d'infrastructures et d'applications sont mis à jour toutes les 24 heures en utilisant les toutes dernières versions des systèmes d'exploitation et des applications, en veillant à ce que les derniers correctifs de sécurité soient appliqués afin de garantir la conformité avec les normes de sécurité les plus récentes et de se protéger contre les menaces émergentes.

Cryptage des données
Toutes les données stockées dans nos bases de données sont cryptées à l'aide de l'algorithme de cryptage standard AES-256. Cela garantit que même si les données sont consultées sans autorisation, il est impossible de les lire ou de les falsifier.

Données en transit
Les données échangées entre les bases de données et les applications sont protégées par les protocoles TLS (Transport Layer Security). Les données sont ainsi cryptées pendant le transfert, ce qui les protège contre l'interception et l'écoute clandestine.

Développement et sécurité opérationnelle

La sécurité dès la conception
Notre approche Secure by Design garantit que les équipes de développement Insights s'approprient le risque de cybersécurité de la conception à la production, en le gérant efficacement tout au long du cycle de vie. Cela conduit à la livraison d'un produit sécurisé grâce à une responsabilité plus claire, des processus simplifiés et le respect des normes de sécurité.

Mode bloc système
Nos systèmes bloquent par défaut toutes les applications et tous les utilisateurs, n'autorisant l'accès qu'à ceux qui sont spécifiés dans les politiques de sécurité. Ces politiques établissent des autorisations pour chaque utilisateur, processus et ressource.

Séparation des rôles des serveurs
Les serveurs ont des rôles distincts, ce qui réduit l'impact d'une violation du système à une seule partie du produit.

Séparation des données de l'évaluateur et de l'apprenant
Les données de recherche de l'évaluateur sont anonymisées et stockées séparément des données de l'apprenant, ce qui garantit la confidentialité et la sécurité des deux types d'informations.

Chiffrement renforcé des clients et des serveurs
Toutes les applications web utilisent TLS 1.2/1.3 et HTTP/2/3, ce qui leur a valu une note A+ de la part de SSL Labs. Cela garantit un cryptage solide et une communication sécurisée.

Pistes d'audit complètes
Tous les changements technologiques fournissent une piste d'audit complète et nécessitent un processus d'approbation, ce qui garantit la responsabilité et la traçabilité.

Audit des interactions avec les clients
L'audit est appliqué à toutes les interactions avec les clients, ce qui nous permet d'identifier spécifiquement toute utilisation abusive des données sur demande.

Limitation du taux
La limitation de la fréquence limite le nombre d'actions pouvant être répétées dans un certain laps de temps, ce qui contribue à prévenir les activités malveillantes des robots et à réduire la charge de travail des serveurs.

Protection contre les scripts intersites (XSS)
La Nouvelle Plateforme Client bloque les attaques XSS grâce à l'utilisation de politiques de sécurité du contenu renforcées, empêchant ainsi les fuites potentielles de données sur les clients.

Protection contre les injections SQL
La Nouvelle Plateforme Client atténue les attaques par injection SQL en utilisant la construction et l'exécution de requêtes dynamiques via des instructions paramétrées, protégeant ainsi les données des clients contre toute compromission.

Questions des clients
Nous nous soucions de la confidentialité et de la sécurité des données et nous nous efforçons de maintenir nos pratiques de sécurité au même niveau que les leaders du secteur.
Lisez nos questions les plus fréquentes sur la confidentialité et la sécurité des données.

Où sont stockées les données ?
Dans le cadre de la résidence du centre de données de l'UE, l'infrastructure informatique et l'ensemble du contenu du client (données de production, données de sauvegarde et métadonnées) sont hébergés au sein de l'UE.

Offrez-vous le même niveau de protection des données à tous vos utilisateurs ?
Oui, soyez assuré que vos données sont gérées et conservées en toute sécurité. Avec TLS 1.2 ou plus pour le transit et AES 256 au repos, en conformité avec les normes GDPR et CCPA, vos données sont sécurisées aux niveaux les plus élevés sans coût supplémentaire.

Vendez-vous des données à des fournisseurs tiers ?
Non, nous ne vendons pas les données de nos utilisateurs, comme indiqué dans notre politique de confidentialité.

Insights a fait des progrès significatifs dans l'amélioration de sa plateforme technologique, en se concentrant sur l'expérience utilisateur et les mesures de sécurité. L'obtention de la certification ISO 27001:2022 souligne notre engagement à maintenir des normes élevées en matière de gestion de la sécurité de l'information. Cette certification renforce non seulement la confiance des clients, mais garantit également la conformité avec les réglementations du secteur et favorise une gestion efficace des risques.

Notre approche proactive de la sécurité est également démontrée par des tests de pénétration réguliers, qui n'ont révélé aucune vulnérabilité dans notre dernière plateforme pour les nouveaux clients. Les principales caractéristiques de sécurité, telles que l'accès à confiance zéro, les jetons à usage unique et les protections rigoureuses du réseau, illustrent notre engagement à protéger les données des clients.

Comme nous continuons à donner la priorité à la sécurité, nous encourageons nos clients à nous faire part de toute question ou préoccupation qu'ils pourraient avoir au sujet de la confidentialité des données et des pratiques de sécurité. Nous restons déterminés à nous améliorer en permanence et à nous adapter aux menaces émergentes, afin de garantir un environnement sûr à tous nos utilisateurs.
Pour toute autre question ou pour accéder à des informations juridiques, les clients sont invités à contacter notre équipe de sécurité (security@insights.com) ou notre équipe juridique (legal@insights.com), selon le cas.

British Assessment Bureau

Part of the **Amtivo** group

CERTIFICATE OF REGISTRATION

The management system of certificate number **247224**

Insights Learning and Development Ltd

Terra Nova, 3 Explorer Road, Dundee, DD2 1EG, United Kingdom

has been assessed and certified as meeting the requirements of:

ISO/IEC 27001:2022

Provision of the delivery of the customer platform for training and development worldwide

This is in accordance with the Statement of Applicability **version 3.3, seen 10 September 2024.**.

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.

UKAS MANAGEMENT SYSTEMS

8289

Valid from:
Initial certification: 21 November 2023
Latest issue: 18 December 2024
Expiry date: 20 November 2026
Subject to annual assessments.

Authorised by

Mike Tims
Chief Executive Officer

british-assessment.co.uk

Certificate issued by Amtivo Group Limited T/A British Assessment Bureau Ltd.

Certification is conditional on maintaining the required performance standards throughout the certified period of registration.
Amtivo Group Limited. 30 Tower View, Kings Hill, Kent, ME19 4UY.