Hvidbog om sikkerhed

www.insights.com

Insights har investeret i en omfattende ombygning af vores teknologiske platforme med fokus på sikkerhed og compliance. Den nye kundeplatform, som er den næste udgave af Insights Online, fokuserer på en forbedret brugeroplevelse og, endnu vigtigere, robuste sikkerhedsforanstaltninger, der er indbygget i systemet. Vores kundeapplikationer er blevet genudviklet ved hjælp af sikker kodningspraksis, en sikker udviklingslivscyklus og sikkerhedstekniske principper, herunder foranstaltninger som kryptering og multifaktorautentificering. Denne tilgang med privatlivets fred og sikkerhed i centrum gælder også for vores understøttende infrastruktur.
Vi værdsætter vores brugeres feedback og har integreret indsigter fra vores kunder i udviklingsprocessen. Fremadrettet vil vi løbende gennemføre forbedringer og opdateringer for at sikre, at vores platform forbliver sikker og opfylder branchens standarder.

ISO 27001:2022-certificering
Siden denne ombygning har Insights med succes gennemført ISO 27001:2022-certificeringen. Denne prestigefyldte certificering er et udtryk for vores engagement i at opretholde de højeste standarder for informationssikkerhed.

Hvorfor er ISO 27001:2022-certificering vigtig?
ISO 27001:2022 er en internationalt anerkendt standard for informationssikkerhedsledelsessystemer (ISMS). At opnå denne certificering viser, at vores organisation har implementeret en robust ramme til at styre og beskytte følsomme oplysninger. Det indebærer en streng vurdering og løbende forbedring af vores sikkerhedspraksis og sikrer, at vi effektivt identificerer, håndterer og afbøder risici.

Hvad betyder det for vores kunder?
En ISO 27001:2022-certificeret virksomhed giver flere vigtige fordele:

- **Øget tillid og tryghed:** Kunderne kan være sikre på, at deres data håndteres med den største omhu og sikkerhed, hvilket reducerer risikoen for databrud og cybertrusler.
- **Overholdelse af regler:** Mange brancher kræver overholdelse af specifikke sikkerhedsstandarder. Vores ISO 27001:2022-certificering hjælper kunderne med at opfylde disse lovkrav.
- **Risikostyring:** Certificeringen betyder, at vi har en proaktiv tilgang til at identificere og håndtere potentielle sikkerhedsrisici og sikre forretningskontinuitet og modstandsdygtighed.
- **Konkurrencefordel:** At arbejde med en certificeret virksomhed kan forbedre dit omdømme og give dig en konkurrencefordel på markedet, da det afspejler en forpligtelse til bedste praksis inden for informationssikkerhed.
- **Kontinuerlig forbedring:** ISO 27001:2022-rammen tilskynder til løbende evaluering og forbedring af sikkerhedsforanstaltninger, hvilket sikrer, at vi er på forkant med nye trusler og sårbarheder.

Ved at opnå ISO 27001:2022-certificering viser Insights sin dedikation til at beskytte kundedata og skabe et sikkert miljø for alle forretningsaktiviteter.

Hvordan griber vi penetrationstest an?
Insights er forpligtet til at levere sikre løsninger til vores kunder. Vi udfører regelmæssigt penetrationstests på vores applikationer ved hjælp af en CREST-godkendt tredjepartsleverandør. Derudover anvender vi de korrekte sikkerhedsprincipper i disse tests.

Den seneste New Customer Platform blev udsat for en ekstern penetrationstest af webapplikationer og havde NUL sårbarheder.

Højdepunkter om sikkerhed

Nedenfor er de vigtigste sikkerhedsfunktioner, vi har implementeret for at sikre det højest mulige beskyttelsesniveau for vores kunder:

Adgangskontrol og autentificering

Nul tillid
Zero Trust er en sikkerhedsramme, der kræver, at alle brugere, uanset om de er inden for eller uden for Insights' netværk, skal godkendes, autoriseres og løbende valideres med hensyn til sikkerhedskonfiguration og -holdning, før de får eller bevarer adgang til New Customer Platform. Denne tilgang er i overensstemmelse med ISO 27001:2022-standardens kontrolmål, herunder adgangskontrol og privilegerede adgangsrettigheder for at sikre "least privilege"-adgang.

Engangs-token
One Time Token forhindrer identitetstyveri ved at sikre, at en indsamlet e-mailadresse ikke kan genbruges, så man ikke behøver at gemme brugernavne og adgangskoder.

Enkelt sign-on
Single Sign-On (SSO) giver kunderne mulighed for at bruge deres egne identitetsudbydere til at sikre deres brugere i applikationen og overlade alle sikkerhedsforanstaltninger til organisationens egne systemer.

Sikkerhed i netværk og infrastruktur

Princippet om ”least privilege”
Dette princip sikrer, at medarbejdere, systemer og applikationer **kun** har den adgang, der er nødvendig for at opfylde deres roller og ansvar. Adgangsrettighederne fastlægges omhyggeligt, så de stemmer overens med de operationelle behov og sikkerhedspolitikkerne.

Ingen offentlig IP
Insights-servere har ingen direkte forbindelse til internettet, hvilket giver en perimeter-sikkerhedsløsning, der beskytter mod eksterne trusler. Trafikken går gennem en udgående proxy, som indeholder en whitelist over tilladte domæner.

Load Balancer til applikationer
Vores applikation Load Balancers styrer internettrafikken og fungerer som en barriere mellem internettet og serverne. Den sikrer, at kun tilladt trafik kan kommunikere med Insights Portalen, og bruger altid de nyeste SSL/TLS-chiffre og -protokoller.

Overvågning og afvisning af mistænkelig trafik
Al indgående HTTP-trafik passerer gennem en Web Application Firewall (WAF), og mistænkelig trafik afvises automatisk, og vores teknologiteam får besked om at undersøge det, hvilket sikrer proaktiv trusselshåndtering.

Hurtig styring af softwarepatches
Alle vores hostingmiljøer for infrastruktur og applikationer opdateres hver 24. time med de allernyeste versioner af operativsystemer og applikationer, hvilket sikrer, at de nyeste sikkerhedsopdateringer anvendes for også at sikre overholdelse af de nyeste sikkerhedsstandarder og for at beskytte mod nye trusler.

Kryptering af data
Alle data, der lagres i vores databaser, er krypteret ved hjælp af industristandarden AES-256-krypteringsalgoritme. Det sikrer, at data ikke kan læses eller manipuleres, selv om der er adgang til dem uden tilladelse.

Data i transit
Data, der udveksles mellem databaser og programmer, beskyttes ved hjælp af TLS-protokoller (Transport Layer Security). Dette krypterer data under overførslen og beskytter dem mod at blive opfanget og aflyttet.

Udvikling og operationel sikkerhed

Sikker gennem design
Vores Secure by Design-tilgang sikrer, at Insights Development Teams ejer cybersikkerhedsrisikoen fra koncept til produktion og styrer den effektivt gennem hele livscyklussen. Det fører til levering af et sikkert produkt gennem klarere ansvarsfordeling, forenklede processer og overholdelse af sikkerhedsstandarder.

Systembloktilstand
Vores systemer blokerer som standard alle programmer og brugere og giver kun adgang til dem, der er specificeret i sikkerhedspolitikkerne. Disse politikker fastlægger tilladelser for hver bruger, proces og ressource.

Adskillelse af serverroller
Servere har adskilte roller, hvilket reducerer virkningen af et systembrud til en enkelt del af produktet.

Adskillelse af evaluator- og deltagerdata
Evaluatorens forskningsdata anonymiseres og opbevares adskilt fra deltagerdata, hvilket sikrer privatlivets fred og sikkerhed for begge typer information.

Hærdet klient- og serverkryptering
Alle webapplikationer betjenes ved hjælp af TLS 1.2/1.3 og HTTP/2/3, hvilket resulterer i en A+ score fra SSL Labs. Dette sikrer robust kryptering og sikker kommunikation.

Omfattende revisionsspor
Alle teknologiske ændringer giver et omfattende revisionsspor og kræver en godkendelsesproces, der sikrer ansvarlighed og sporbarhed.

Revision af kundeinteraktion
Revision anvendes på alle kundeinteraktioner, så vi specifikt kan identificere ethvert misbrug af data efter anmodning.

Begrænsning af hastighed
Hastighedsbegrænsning begrænser, hvor ofte handlinger kan gentages inden for en bestemt tidsramme, hvilket hjælper med at forhindre ondsindet botaktivitet og reducere serverbelastningen.

Beskyttelse mod cross-site scripting (XSS)
New Customer Platform blokerer XSS-angreb ved hjælp af hærdede Content Security Policies, hvilket forhindrer potentielle lækager af kundedata.

Beskyttelse mod SQL-injektion
New Customer Platform afbøder SQL-injektionsangreb ved hjælp af dynamisk konstruktion og udførelse af forespørgsler via parameteriserede udsagn, hvilket beskytter kundedata mod kompromittering.

Kundeforespørgsler
Vi tager databeskyttelse og -sikkerhed seriøst og bestræber os på at holde vores sikkerhedspraksis på niveau med branchens førende virksomheder.
Læs vores oftest stillede spørgsmål om databeskyttelse og -sikkerhed.

Hvor er dataene gemt?
Under EU Data Centre Residency er computerinfrastrukturen og alt kundeindhold (produktionsdata, backupdata og metadata) hostet i EU.

Tilbyder du det samme niveau af databeskyttelse til alle dine brugere
Ja, du kan være sikker på, at dine data administreres og opbevares sikkert. Med TLS 1.2 eller højere til transit og AES 256 i hvile, i overensstemmelse med GDPR- og CCPA-standarder, er dine data sikret på højeste niveau uden ekstra omkostninger.

Sælger du data til tredjepartsleverandører
Nej, vi sælger ikke vores brugerdata, som det fremgår af vores privatlivspolitik.

Insights har gjort betydelige fremskridt med at forbedre sin teknologiplatform med fokus på brugeroplevelse og sikkerhedsforanstaltninger. Den vellykkede opnåelse af ISO 27001:2022-certificering understreger vores forpligtelse til at opretholde høje standarder inden for informationssikkerhedsstyring. Denne certificering styrker ikke kun kundernes tillid, men sikrer også overholdelse af branchens regler og fremmer effektiv risikostyring.

Vores proaktive tilgang til sikkerhed demonstreres yderligere gennem regelmæssige penetrationstests, som ikke har vist nogen sårbarheder i vores seneste New Customer Platform. Vigtige sikkerhedsfunktioner som Zero Trust-adgang, One Time Tokens og streng netværksbeskyttelse er eksempler på vores dedikation til at beskytte kundedata.

Da vi fortsat prioriterer sikkerhed, opfordrer vi vores kunder til at tale med os om eventuelle spørgsmål eller bekymringer, de måtte have om databeskyttelse og sikkerhedspraksis. Vi er fortsat forpligtet til løbende at forbedre og tilpasse os nye trusler for at sikre et sikkert miljø for alle vores brugere.
For yderligere forespørgsler eller for at få adgang til juridiske oplysninger opfordres kunderne til at kontakte vores sikkerhedsteam (security@insights.com) eller juridiske team (legal@insights.com) efter behov.

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.