Kepler Cloud

Informationssäkerhet och rutiner

Informationssäkerhet

Driftmiljö och svenska leverantörer
Vi är för närvarande inte certifierade enligt ISO 27001, Vi följer dock principerna för denna standard och har implementerat rutiner och processer som skyddar data genom hela livscykeln, vilket är en utav dom första och viktigaste stegen i en ISO certifierings process. Våra säkerhetsåtgärder inkluderar:

- **Dataskydd:**
  Säker hantering av data, inklusive kryptering vid både överföring och vila.

- **Åtkomstkontroller:**
  Strikta policies för åtkomstkontroller för att säkerställa att endast behöriga personer har tillgång till känslig information.

- **Övervakning och loggning:**
  Löpande övervakning av våra system för att upptäcka och förebygga säkerhetshot.

- **Incidenthantering:**
  En tydlig plan för hantering av säkerhetsincidenter, inklusive upptäckt, analys, och åtgärder för att minimera skador och förhindra framtida incidenter.

Efterlevnad och standarder
Kepler Technologies AB strävar efter att vara i linje med branschens bästa praxis och följa relevanta lagar och regler, inklusive GDPR för dataskydd.

Våra säkerhetsrutiner och processer är utformade för att efterleva internationella standarder som ISO 27001 och ISO 9001, även om vi för närvarande inte är formellt certifierade.

Ansvar och utbildning
Alla medarbetare hos Kepler Cloud genomgår regelbundna utbildningar i informationssäkerhet för att säkerställa att det är medvetna om potentiella hot och risker, samt hur det kan förhindra och reagera på dem. Vi betonar vikten av säkerhetsmedvetenhet i hela organisationen och ser detta som en grundsten för vår framgång.

Vi har tydliga ansvarsområden och roller för informationssäkerhet, vilket hjälper oss att snabbt reagera på incidenter och säkerhetsfrågor. Våra anställda förstår vikten av säker hantering av information och följer företagets policies för att skydda känsliga data och system.

Sårbarhetshantering och penetrationstester
Kepler Cloud (Kepler Technologies AB) har en robust process för sårbarhetshantering som säkerställer att potentiella säkerhetshot snabbt identifieras, hanteras och åtgärdas. Vi använder automatiserade verktyg för kontinuerlig övervakning och analys av våra system för att upptäcka sårbarheter. När en sårbarhet identifieras, klassificeras den baserat på dess allvarlighetsgrad, och åtgärder vidtas omedelbart för att eliminera eller mitigera hotet. Alla kritiska sårbarheter hanteras med högsta prioritet. Regelbundna säkerhetsgranskningar och tester genomförs för att säkerställa att våra system alltid är skyddade mot nya hot.

Vi genomför även regelbundna penetrationstester där externa säkerhetsexperter testar våra system för att identifiera eventuella svagheter. Resultaten av dessa tester används för att kontinuerligt förbättra våra säkerhetsåtgärder och för att förebygga framtida säkerhetsincidenter. Dessa tester kompletterar vår interna övervakning och gör att vi snabbt kan identifiera och åtgärda eventuella sårbarheter innan det utnyttjas.