Informationssäkerhetspolicy

Bakgrund

QNOVA levererar programvara till företag i olika storlekar samt företag inom olika branscher där nivåerna på informationssäkerhet kan variera mycket. Därför är det extra viktigt för oss att veta vad som gäller när kunden efterfrågar viss säkerhet eller frågar om råd kring säkerhet. Att ha en säkerhetsstandard för vår programvara och tjänster blir därför en naturlig del av vårt dagliga arbete.
Informationen som vi tillhandahåller åt våra kunder ska vara:

- Tillgänglig när behörig användare vill komma åt den.
- Riktig och skyddad mot förvanskning och obehörig hantering.
- Konfidentiell och hanterbar av behöriga användare.

Varje medarbetare på QNOVA har ett personligt ansvar att efterfölja regler och riktlinjer från QNOVAs ledningssystem för informationssäkerhet.
Regelbundna utbildningar genomförs för att samtliga medarbetar ska vara uppdaterade och medvetna kring informationssäkerhet.

Mål

Vi följer självklart alla regler, lagar, förordningar etcetera som ställs på hanteringen av informationssäkerhet. Ett exempel på detta kan vara GDPR.
Nedan kommer även några konkreta exempel på hur vi jobbar mer med de tre nyckelorden i informationssäkerhet: Tillgänglighet, riktighet och konfidentialitet.

Tillgänglighet

- Vi övervakar och gör prognoser avseende kapacitet och prestanda på våra driftmiljöer.
- Vi har reservrutiner, reservlösningar och återstartsplaner som uppfyller våra kunders krav på tillgänglighet (SLA).
- Vi garanterar 99,5% (24/7/365) tillgänglighet för vår programvara.
- Vi testar samtliga leveranser i separat testmiljö innan dem införs i driftmiljön för att skydda driftmiljön mot riskabla påfrestningar.

QNOVA
Elsa Brändströms gata 6, 582 27, Linköping
↱ +46 13 465 54 70 ↱ www.qnova.se

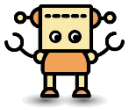
Konfidentialitet

- Vi har en policy kring hur vi jobbar på distans avseende drift, förvaltning och support av våra levererade tjänster.
- Vi har rutiner för att permanent radera information som är relaterade till programvaran.
- Vi krypterar alla lösenord.
- Vi distribuerar ej lösenord på ett sätt som gör att det kan röjas till obehöriga.
- Vi har fastställda regler för hur vi hanterar våra autentiseringsuppgifter som är relaterade till leveransen.
- Vi jobbar enligt ”minsta möjliga behörighet”-principen där endast relevanta roller har behörighet till den levererade programvaran.
- Vår leverantör för datalagring har rutiner som säkerställer att endast behörig personal har fysisk åtkomst till datahall.
- All kommunikation till och från programvaran skyddas mot obehörig åtkomst. Detta omfattar kommunikation mellan klient och server samt våra programvarukomponenter.
- Alla kunddatabaser är logiskt och/eller fysiskt separerad för att garantera att kunddata ej läcker emellan dem.
- Vi gör inga informationsutbyten med andra programvaror eller tjänster.
- Vi erbjuder att tillsammans med en utpekad roll hos kund samverka i hanteringen av sårbarheter, säkerhetshändelser eller säkerhetsincidenter.
- Vi hanterar säkerhetsincidenter enligt gällande lagar och förordningar.

Riktighet

- Vår programvara använder tidssynkronisering mot samma tidskälla.
- Vi begränsar den mjukvara som får exekveras i vår programvara.
- Vi har rutiner för återläsning av säkerhetskopior för att garantera att data som läses tillbaka är korrekt.
- All kommunikation till och från programvaran skyddas mot förvanskning. Detta omfattar kommunikation mellan klient och server samt våra programvarukomponenter.
- Alla kunddatabaser (som vi tillhandahåller) är logiskt och/eller fysiskt separerad för att garantera att inte kunddata sparas i fel databas.

Då vi har olika leveransmetoder så kan vi endast garantera vår säkerhetsstandard på de leveranser där vi tillhandahåller data



Linköping den 1 september 2022
Martin Hjelte
VD

QNOVA
Elsa Brändströms gata 6, 582 27, Linköping
↱ +46 13 465 54 70 ↱ www.qnova.se