

Användnings- och säkerhetspolicy

Syfte

Denna bilaga tydliggör ansvarsfördelningen mellan **Aveki AB** och **kunden** vid användning av Avekis programvaror. Policyn kompletterar gällande **avtal** och beskriver de säkerhetsmässiga förutsättningarna för ett korrekt användande av systemen.

Avekis ansvar

Aveki ansvarar för:

- Utveckling, testning och leverans av programvaran enligt överenskommen version.
- Att informera kundens systemansvariga om relevanta versionsändringar, större fel, kända begränsningar och säkerhetsrelaterade sårbarheter som kan påverka användningen av programvaran.
- Att produkten vid leverans uppfyller de funktions- och säkerhetskrav som anges i tillhörande dokumentation, och att kommunicera uppdaterade krav och rekommendationer löpande till kundens systemansvariga.
- Att tillhandahålla support och underhåll inom ramen för gällande avtal.
- Att skydda den kundinformation som kan förekomma i Avekis egna interna system, såsom vid supportärenden, felsökning, licensadministration och versionshantering.
- Att tydligt informera kunden, när de kontaktar Aveki via supporten, om ett ärende innebär en konsultinsats som ligger utanför supportavtalet – exempelvis arbete i kundens driftsmiljö, integrationer eller andra anpassningar.
- Att använda standardiserade uppkopplingsmetoder för fjärrsupport, såsom Microsoft Teams och TeamViewer.
- Att följa tillämpliga lagar, föreskrifter och branschstandarder som gäller för utveckling, leverans och support av Avekis programvara, inklusive men inte begränsat till GDPR och NIS-direktivet.

Aveki ansvarar **inte** för drift, lagring, säkerhetskopiering, dataskydd, behörighetsstyrning eller tekniska skyddsåtgärder i kundens IT-miljö.

Kundens ansvar

Kunden ansvarar för:

- Att säkerställa att den egna driftsmiljön uppfyller Avekis dokumenterade system- och säkerhetskrav, inklusive drift, lagring, backup och behörighetsstyrning i den IT-miljö där Avekis programvara installeras.



- Att servrar, databaser, nätverk, brandväggar och säkerhetskopiering håller en säkerhetsnivå som är förenlig med branschpraxis, samt att data inte exponeras eller förloras på grund av brister i kundens infrastruktur.
- Att endast ge behöriga användare åtkomst till systemen och att administrera användarkonton på ett säkert sätt, inklusive behörighetsstyrning och åtkomstkontroll i alla system som interagerar med Avekis programvara.
- Att ansvara för säkerhet, funktion och dataskydd i externa system som integrerar med Avekis programvara.
- Att utse en eller flera systemansvariga som ansvarar för att:
 - ta del av tekniska rekommendationer, versionsinformation och säkerhetsrelaterad information från Aveki,
 - uppdatera systemet enligt rekommendationer,
 - följa Avekis allmänna försäljnings- och licensvillkor,
 - rapportera fel och förbättringsförslag.
- Att säkerställa att tekniska förutsättningar finns för fjärrsupport, inklusive att administrera och tillhandahålla alternativ åtkomst om kunden väljer andra metoder än Avekis standard (t.ex. VPN eller särskilda fjärrskrivbord).
- Att bära kostnader för extra tid som uppstår vid användning av andra uppkopplingsmetoder än Avekis standard.
- Att vid kontakt med Avekis support aktivt efterfråga förtydligande när det är oklart om ett ärende omfattas av supportavtalet eller utgör konsultation, för att undvika missförstånd kring debitering och ansvar.
- Att följa tillämpliga lagar, föreskrifter och branschrekommendationer, såsom GDPR och NIS-direktivet.

Informationssäkerhet och datahantering

Inbyggda säkerhetsfunktioner i Avekis programvara (Avekis ansvar)

Avekis programvara innehåller inbyggda skyddsåtgärder, såsom behörighetsstyrning, loggning, valideringar och andra säkerhetsfunktioner.

Aveki ansvarar för att dessa funktioner fungerar enligt specifikation vid leverans och under avtalad supportperiod.

Data som Aveki behandlar i sina interna system (Avekis ansvar)

I samband med support, testning, felsökning eller licensadministration kan viss kundinformation hanteras i Avekis interna system.

Aveki ansvarar för att denna information skyddas enligt företagets interna säkerhetsrutiner och ledningssystem för informationssäkerhet.

Data som hanteras i kundens IT-miljö eller lämnar programvaran (kundens ansvar)

När information behandlas, lagras eller överförs i kundens egna IT-miljö – eller när den exporteras, integreras med andra system, kopieras eller på annat sätt lämnar Avekis programvaras kontrollerade miljö – omfattas den inte längre av Avekis säkerhetsfunktioner.