



Antura SaaS

● Antura SaaS Dokumentation	3
● Infrastruktur och Teknologi	3
● Fysisk Säkerhet	3
● Teknisk Arkitektur	3
● Molnsäkerhet	4
● Säkerhetsrevisioner	4
● Förändrings-, Incident- och Problemhantering	4
● Åtkomst och Administration	5
● Säker Åtkomst med VPN och MFA	5
● Tidsbegränsad Åtkomst	5
● Backup	6

Antura SaaS Dokumentation

Antura SaaS – Software as a Service – är placerad i moderna datacenter belägna inom Sverige, kända för sina stränga säkerhetsåtgärder. Vår IaaS-leverantör hanterar och driver dessa datacenter, men de har inte auktoriserad åtkomst till Antura SaaS-resurser. Den virtualiseringsteknik som driver plattformen är Hosted VMware.

Infrastruktur och Teknologi

Vår plattform förlitar sig på pålitlig och väletablerad hårdvaru- och programvaruteknik, vilket garanterar optimal prestanda och tillförlitlighet. Med en robust nätverksinfrastruktur som sträcker sig över både Sverige och internationella platser levererar vi en sömlös tjänst till våra användare.

De grundläggande teknikerna som driver Antura är .NET Framework och .NET (tidigare känt som .NET Core), tillsammans med Microsoft SQL Server. Följaktligen är en betydande del av vår tekniska plattform baserad på Microsoft-teknologier.

Vår åtagande för säkerhet sträcker sig till både vår fysiska och virtuella infrastruktur, som följer ISO 27001-normer för efterlevnad. Både Antura och vår datacenterleverantör innehar ISO 27001-certifieringar, vilket ytterligare visar vårt engagemang för att skydda dina data.

Fysisk Säkerhet

För att upprätthålla högsta säkerhetsnivå avstår vi från att avslöja den exakta geografiska platsen för våra datacenter. De har en klassificering som "Skyddsobjekt" enligt svensk lag 2010:305 ([Länk](#)), vilket betonar deras kritiska säkerhetsstatus.

Våra datacenter övervakas ständigt av utbildad säkerhetspersonal, vilket garanterar omfattande skydd.

Teknisk Arkitektur

Arkitektonisk design av Antura SaaS prioriterar säkerhet, underhållbarhet och skalbarhet.

Trots delade beräkningsresurser förblir varje kundinstans logiskt isolerad från andra. Denna separation säkerställer integriteten för dina data och operationer.

Produktionszoner är strikt avskilda från icke-produktionsområden, såsom test- eller utbildningsmiljöer. Denna isolering innebär att resurser i en produktionszon inte kan kommunicera med dem i en testzon.

Antura Cloud har utformats noggrant för att följa Antura AB:s ISO 27001-certifiering, vilket garanterar robusta säkerhetspraxis.

Molnsäkerhet

Vår molnsäkerhetsstrategi omfattar kantskydd, nätverkssegmentering, antivirusåtgärder, mikrosegmentering, strikt autentisering, privilegiehantering, åtkomstkontroller, säkra kryptografiska tekniker och säkerhetsförfaranden i enlighet med ISO 27001-standards.

Vi genomför regelbundet externa och interna säkerhetsrevisioner för att upprätthålla högsta säkerhetsstandards.

Antura SaaS är fullt GDPR-kompatibelt. All data och plattformen själv är exklusivt placerade inom Sverige, med vår infrastrukturleverantör som är ett svenskt företag. Anturas personal är svenska medborgare.

Säkerhetsrevisioner

Vi tar säkerheten på allvar och genomför regelbundna säkerhetsrevisioner av Antura SaaS. Dessa revisioner utförs av en extern part med expertis inom säkerhetsområdet för att säkerställa att vår plattform uppfyller de högsta säkerhetsstandarderna. Genom att använda externa säkerhetsrevisioner kan vi identifiera och hantera potentiella sårbarheter och risker i vår tjänst.

Säkerhetsrevisionerna är en integrerad del av vårt åtagande att skydda dina data och säkerställa att Antura SaaS förblir en pålitlig och säker plattform för våra användare.

Förändrings-, Incident- och Problemhantering

För att förbättra kvaliteten och stabiliteten i våra tjänster automatiserar vi kontinuerligt administrativa och underhållsuppgifter.

Våra förändringshanteringsprocesser säkerställer att alla förändringar genomgår noggrann förberedelse, granskning, godkännande och genomförande, vilket överensstämmer med Anturas ISMS och ISO 27001-certifiering.

Vi har implementerat processer och rutiner för hantering av incidenter, förändringar och problem som följer ISO 27001-standarder, vilket garanterar snabba och effektiva svar på eventuella problem.

Åtkomst och Administration

Administrativa åtkomsträttigheter till resurser inom Antura SaaS är strikt begränsade till Anturas Operations team, som ansvarar för plattformens dagliga drift, säkerhet och underhåll. Vi tar åtkomstkontroll och säkerhet på allvar och implementerar flera skyddsnivåer.

Säker Åtkomst med VPN och MFA

För att säkerställa hög säkerhetsnivå ansluter medlemmar i Operations teamet till Antura SaaS-plattformen med hjälp av ett Virtual Private Network (VPN). Denna VPN-anslutning upprättar en säker och krypterad tunnel mellan vårt teams enheter och vårt datacenter, vilket ger ett extra säkerhetslager.

Utöver VPN tvingar vi flerfaktorsautentisering (MFA) för all administrativ åtkomst. MFA kräver att teammedlemmarna tillhandahåller flera former av verifiering innan de får åtkomst, vanligtvis något de vet (lösenord) och något de har (t.ex. en mobilapp-genererad kod). Denna extra autentisering stärker betydligt säkerheten för administrativ åtkomst.

Tidsbegränsad Åtkomst

För att ytterligare förstärka säkerheten och kontrollen är åtkomsten för vårt Operations-team tidsbegränsad. Varje session har en fördefinierad varaktighet, och vid utgången måste teammedlemmarna autentisera sig på nytt för att förnya sin åtkomst. Denna tidsbegränsade metod minimerar risken för obehörig åtkomst, även i fall där autentiseringsuppgifter kan ha blivit komprometterade.

Varje åtkomsthändelse, inklusive inloggningsförsök, sessionstider och vidtagna åtgärder, loggas och övervakas noggrant för att säkerställa öppenhet och ansvarsskyldighet. Vårt åtagande för säkerhet sträcker sig till varje aspekt av åtkomst och administration.

Backup

Våra backuprutiner innefattar dagliga säkerhetskopieringar med en retentionspolicy på 7 dagar. Dessa säkerhetskopior lagras i ett separat datacenter, fysiskt isolerat från det datacenter där data härstammar från.

Alla säkerhetskopior är krypterade både under överföring och i vila, vilket säkerställer högsta säkerhet för dina data. Vid behov kan en säkerhetskopia återställas på kundens begäran genom att kontakta Antura Support eller din Key Account Manager (KAM).