Informationssäkerhetspolicy

Antura AB

Version 14.0

Godkänd av Anturas styrelse

2025-11-28

Antura - Informationssäkerhetspolicy

Antura anser att informationssäkerhet är viktigt för bolagets trovärdighet och kunders tillit till hur vi hanterar deras information.

> *”Informationssäkerhet är en högt prioriterad fråga för Antura och våra kunder. Vi måste kunna lita på att all information som vi hanterar internt och för våra kunders räkning alltid är tillgänglig, korrekt och skyddad från obehörig åtkomst.”*
>
> Mattias Andersson, VD

Bristande informationssäkerhet kan leda till störningar i vår och våra kunders verksamhet eller medföra bristande skydd för den personliga integriteten.

Anturas ledning har beslutat att införa ett systematiskt arbetssätt avseende hur vi jobbar med frågor och uppgifter som handlar om informationssäkerhet, ett *ledningssystem för informationssäkerhet*. Detta ledningssystem ska baseras på standarden ISO27001:2022[1] samt ett urval av de artiklar i Europaparlamentets och rådets förordning (EU) 2016/679, dvs GDPR, som berör informationssäkerhet. Det skall även möta de krav som ställs genom cybersäkerhetslagen, vilken utgår ifrån Europaparlamentets och rådets direktiv (EU) 2022/2555, dvs NIS2.

Anturas ledningssystem för informationssäkerhet ska ha en hierarkisk dokumentstruktur i tre nivåer:

- **Policyn** (detta dokument) utgör den översta nivån i styrningsdokumentationen. Policyn uttrycker Anturas ambitionsnivå, viljeinriktning samt grundläggande mål för arbetet med informationssäkerhet. Det kan finnas flera ämnesspecifika policyer parallellt med detta dokument.
- **Instruktioner** är underställda policyn och definierar de obligatoriska kraven i fråga om informations- och IT-säkerhet på en taktisk och operativ nivå i verksamheten. Efterlevnad av Anturas instruktioner är obligatoriskt. Instruktioner definierar och beskriver vad som behöver utföras med avseende på informationssäkerhet.
- **Rutiner** är underordnade instruktioner. Rutiner kan vara manuella eller automatiserade, och dess syfte är att tydligt beskriva handgrepp, moment eller tillvägagångssätt för hur en instruktion skall kunna uppfyllas.

Anturas informationssäkerhetspolicy, instruktioner och rutiner ska gälla för alla anställda, konsulter, samarbetspartners och andra underleverantörer som på något sätt är involverade i leverans, utveckling, drift, underhåll och support av Anturas produkter och tjänster. Överträdelser eller otillåtna avvikelser från denna policy och dess underordnade instruktioner och rutiner bedöms i enlighet med de instruktioner som upprättats för ändamålet och kan leda till disciplinära åtgärder och eventuellt uppsägning.

[1] ISO27001:2022 är den internationella standarden som beskriver bästa praxis för ett ledningssystem för informationssäkerhet.

Antura ska vidta minst följande åtgärder för att skydda informationstillgångar och upprätthålla en hög nivå av informationssäkerhet:

1. **Riskhantering**
   Genomföra regelbundna riskanalyser och vidta lämpliga åtgärder för att minska eller eliminera identifierade risker.
2. **Incidenthantering**
   Upprätta och tillämpa rutiner för att upptäcka, rapportera och hantera informationssäkerhetsincidenter.
3. **Kontinuitet och krishantering**
   Säkerställa att verksamheten kan upprätthållas vid störningar genom etablerade rutiner för kontinuitets- och krishantering.
4. **Leverantörs- och leveranskedjesäkerhet**
   Bedöma och hantera säkerhetsrisker hos leverantörer samt säkerställa att avtalade säkerhetskrav följs.
5. **System- och utvecklingssäkerhet**
   Integrera säkerhet i alla faser av förvärv, utveckling och underhåll av IT- och informationssystem.
6. **Kryptografi och autentisering**
   Tillämpa ändamålsenlig kryptering och autentisering för att skydda information och användaridentiteter.
7. **Åtkomstkontroll och tillgångsförvaltning**
   Hantera informationstillgångar och åtkomsträttigheter i enlighet med fastställda policyer, lagkrav och kundkrav.
8. **Ansvar och skydd av tillgångar**
   Identifiera kritiska informationstillgångar, tilldela ansvar och införa proportionerliga skyddsåtgärder.
9. **Utbildning och medvetenhet**
   Säkerställa att medarbetare och relevanta intressenter har tillräcklig kunskap och förståelse för informationssäkerhet.
10. **Tillgänglighet och informationshantering**
    Tillgodose krav på tillgänglighet, konfidentialitet, riktighet och spårbarhet av information – rätt information till rätt person vid rätt tidpunkt.

Anturas styrelse ansvarar för ytterst för bolagets ledningssystem för informationssäkerhet, medan det exekutiva ansvaret är tilldelat VD och därefter delegerat till CISO (Chief Information Security Officer). CISO ska deltaga i ledningsgruppsarbetet på Antura och därigenom hålla verkställande ledningen och styrelsen informerad om statusen för bolagets ledningssystem för informationssäkerhet.

Anturas informationssäkerhetsmål är:

- **Säker och tillgänglig SaaS-leverans**
  Säkerställa att Antura levererar sina molnbaserade tjänster som en säker SaaS-lösning med uppfyllande av avtalade **SLA:er och tillgänglighetsnivåer** (mål ≥ 99,5 % drifttid).
  Syfte: Upprätthålla kundernas förtroende och verksamhetskontinuitet.

- **Förebygga allvarliga informationssäkerhetsincidenter**
  Minimera risken för **allvarliga informationssäkerhetsincidenter** inom Anturas tjänster genom effektiva skyddsåtgärder, övervakning och snabb incidenthantering (mål: 0 allvarliga incidenter per år).
  Syfte: Skydda kundernas och Anturas egna informationstillgångar mot oavsiktlig eller avsiktlig skada.
- **Förebygga säkerhetsbrister i produkter och tjänster**
  Säkerställa att **Anturas produkter och tjänster utvecklas, testas och underhålls** enligt etablerade säkerhetskrav för att förhindra uppkomst av allvarliga sårbarheter (mål: 0 kritiska sårbarheter i produktionsmiljö).
  Syfte: Upprätthålla integritet och tillförlitlighet i Anturas lösningar.

- **Öka medvetenheten om informationssäkerhet**
  Etablera och bibehålla en hög **säkerhetsmedvetenhet** hos ledning, medarbetare och konsulter genom utbildning, kommunikation och löpande kompetenshöjning (mål: 100 % genomförd årlig utbildning).
  Syfte: Stärka säkerhetskulturen och minska den mänskliga faktorns risk.

Ett väl etablerat och certifierat ledningssystem i enlighet med ISO27001 och cybersäkerhetslagen skall bidra till uppfyllnad av ovanstående informationssäkerhetsmål.