ANTURA

# Informationssäkerhet på Antura

Ett dokument som beskriver arbetet med informationssäkerhet på Antura.

# Ledningssystem för informationssäkerhet

Anturas tillämpar ett systematiskt arbetssätt för informationssäkerhet.
Detta arbetssätt är väl etablerat och bygger på ett regelverk baserat på standarden ISO27001:2022 samt ett urval av artiklarna i Europaparlamentets och rådets förordning (EU) 2016/679, dvs. GDPR som berör informationssäkerhet. Ett regelverk som styr arbetet med informationssäkerhet kallas ofta för ett Ledningssystem för Informationssäkerhet (LIS). På engelska används ibland ordet Information Security Management System (ISMS).

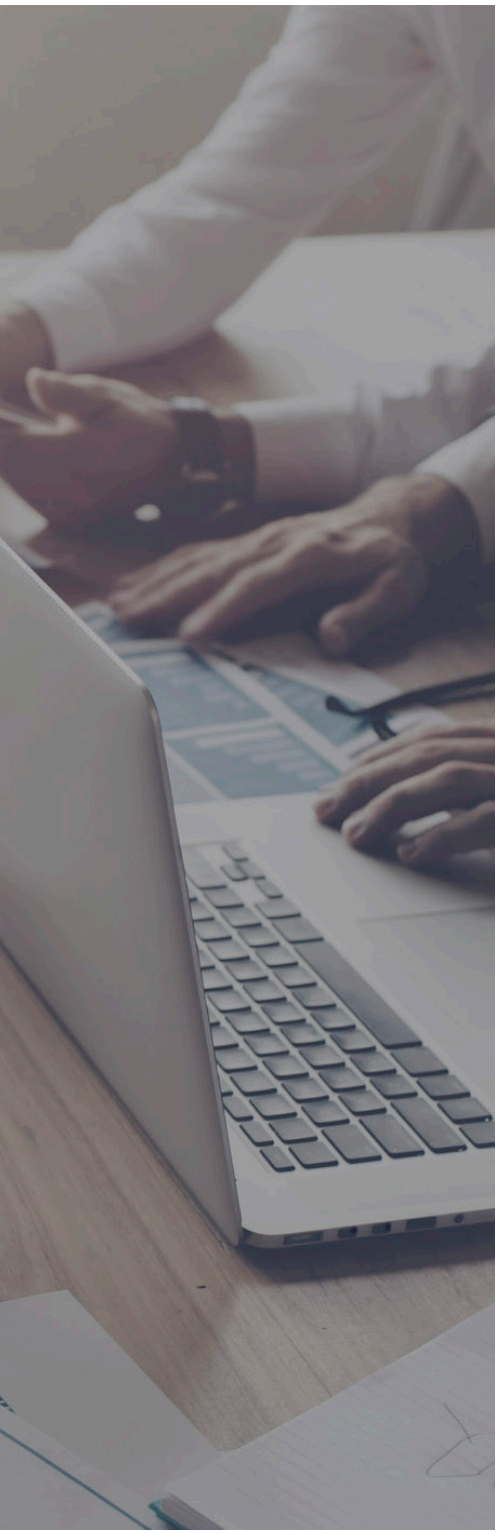
Anturas verksamhet bedöms även falla under NIS2-direktivet (Direktiv (EU) 2022/2555), vilket syftar till att stärka nätverks- och informationssystemens säkerhet inom EU. Detta genom att ställa krav på säkerhetsåtgärder för operatörer av essentiella tjänster och leverantörer av digitala tjänster:

- Genomföra riskhantering och bedömning av säkerhetsnivåer.
- Implementera säkerhetsåtgärder för att skydda nätverks- och informations-system.
- Genomföra incidentrapportering och hantering.
- Säkerställa kontinuitet i verksamheten.

Arbetet med Informationssäkerhet inom Antura LIS utgår ifrån identifierade verksamhets- och informationssäkerhetsrisker samt tillämpliga lagar och förordningar. Riskerna kartläggs utifrån ett integritets-, sekretess- och tillgänglighetsperspektiv (CIA). Även hantering av personuppgifter inkluderas i riskanalysens omfattning. Riskanalys genomförs regelbundet och följer en fastställd rutin.

Målen för informationssäkerhet (Security Objectives) utgår från de förutsättningar och den omfattning som är definierad för informations- säkerhetsarbetet (Information Security Scope).

Anturas ambition, målsättning och riktlinjer för informationssäkerhets-arbetet dokumenteras och kommuniceras genom flera olika policyer.



# Hur säkrar vi våra kunders data och information?

Antura har som mål att förhindra stöld, röjande eller förvanskning av de informationstillgångar vi ansvarar för. Målet uppnås genom vårt ISMS, som är uppbyggt av en kombination av interna rutiner och teknisk infrastruktur.

Antura analyserar såväl de risker som de åtgärder (Security Controls) som avser att hantera de aktuella riskerna i syfte att säkerställa att de tänkta kontrollerna verkligen uppnår den effekt som är tänkt. Analysen resulterar i en s.k. Statement of Applicability (SoA). I SoA beskrivs vilka åtgärder Antura har beslutat att implementera i sin organisation, Dessa åtgärder kan grupperas i fyra olika kategorier, vilka presenteras nedan. Dessutom finns ett antal säkerhetsåtgärder i syfte att skydda personuppgifter implementerade.

## Organisatoriska säkerhetsåtgärder

Organisatoriska säkerhetsåtgärder omfattar 37 olika säkerhetsåtgärder inom olika områden.

Huvudprincipen för tilldelning av åtkomst och behörigheter på Antura är att eftersträva s.k. least privilege, dvs. man skall bara ha åtkomst till den information man behöver för att kunna utföra sitt arbete på ett effektivt sätt. Genom rutiner och tekniskt stöd för autentisering säkerställer Antura att enbart personer med rätt behörighet kan ta del av t.ex. kunders information. Antura erbjuder även stöd för extern autentisering via t.ex. AD, ADFS eller Azure AD.

De leverantörsrelationer som Antura ingår övervägs och granskas noggrant. Varje ny relation genomgår en riskanalys och leverantörerna granskas regelbundet i syfte att säkerställa att de krav som Antura ställer också uppfylls.

Antura tillämpar dokumenterade rutiner för att hantera incidenter oavsett om det handlar om en informationssäkerhets-, personuppgifts eller produktrelaterad incident. Alla incidenter klassificeras efter en allvarlighetsmatris som avgör hur den fortsatta hanteringen ser ut. Antura har även rutiner för incidentrapportering till olika myndigheter i enlighet med kraven i NIS2.

Antura säkerställer genom kontinuitetsplanering (Business Continuity Plan) att bolagets viktigaste verksamhetsprocesser skall kunna upprätthållas även under olika former av störningar. Utifrån den risk och sårbarhetsanalys som genomförts regelbundet, identifieras ett antal tänkbara scenarion, vilka innebär olika typer av störningar i Anturas verksamhet. Planerna övas och uppdateras regelbundet i enlighet med fastställda rutiner. Att säkerställa kontinuitet i verksamheten är också ett krav enligt NIS2.

Antura eftersträvar att uppfylla lagar och kontrakt som t.ex. ingångna servicenivåavtal (SLA), licensvillkor, svenska lagar, tillämpliga förordningar, sekretess och dataskydd.

Antura har ett flertal rutiner till att stödja regelverket kring hantering av personuppgifter (GDPR). Antura har bl.a. en rutin för att kunna rapportera personuppgiftsincidenter till berörda myndigheter inom de tidsramar som lagar och förordningar stipulerar, samt rutiner för hur gallring av personuppgifter skall genomföras. Antura eftersträvar att så långt som möjligt tillämpa privacy by design och privacy by default.

## Personrelaterade säkerhetsåtgärder

Personrelaterade säkerhetsåtgärder omfattar 8 olika säkerhetsåtgärder.

Antura har som mål att säkerställa att all personal, underkonsulter och andra relevanta externa är medvetna om och uppfyller sitt ansvar för informationssäkerhet. Antura uppnår målen genom att följa ett antal rutiner som handlar om rekrytering, kompetensutveckling, medvetandeträning samt checklistor och rutiner vid inledande och avslutande av anställning ochuppdrag. Alla medarbetare och andra berörda individer undertecknar NDA.

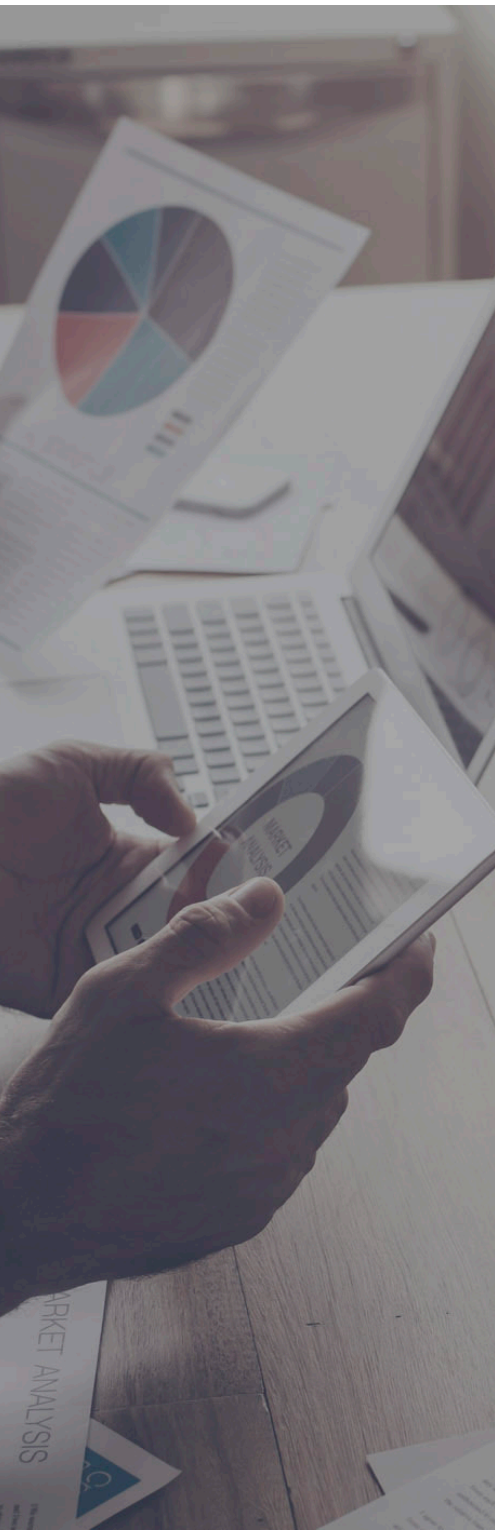
## Fysiska säkerhetsåtgärder

Fysiska säkerhetsåtgärder omfattar 14 olika säkerhetsåtgärder.

Anturas eftersträvar en hög fysisk säkerhet genom att i huvudsak bedriva det dagliga arbetet i ändamålsenliga lokaler, där arbetsytorna är indelade i grön, gul eller röd zon utifrån hur hårt ställda informationssäkerhetskraven är ställda på det arbete som utförs.

Kraven på fysiska säkerhetsåtgärder gäller även för Anturas viktiga underleverantörer av infrastrukturtjänster. T.ex. ställer Antura krav på att dessa underleverantörer också skall vara ISO27001-certifierade.

Såväl kontorslokaler som datahallar är således utrustade med ändamålsenlig teknisk utrustning i form av passerkontroll, larm, brandskydd och reservkraft i enlighet med direktiv från t.ex. MSB.



## Tekniska säkerhetsåtgärder

Tekniska säkerhetsåtgärder omfattar 34 olika säkerhetsåtgärder.

Anturas produkter och tjänster utformas enligt principerna security by design och security by default. All produktutveckling sker i enlighet med en fastställd process, som sträcker sig från kravanalys till kvalitetssäkring. Informationssäkerhet utgör en integrerad del av livscykeln för produkten
Antura.

Produktutveckling sker i nätverk och miljöer som är tekniskt helt åtskilda från kundernas produktionsmiljöer och dess kunddata. Implementerade säkerhetsåtgärder för att skydda nätverks- och informationssystem är också ett krav enligt NIS2.

Endast verifierade och godkända versioner av Antura tillåts installeras i kundernas produktionsmiljöer.
Antura samarbetar sedan många år med etablerade partners för datadrift och vi tillämpar höga krav på driftsäkerhet i form av tillgänglighet, skydd mot cyberhot, säker dataöverföring och spårbarhet i form av loggning.

Kundmiljöer övervakas dygnet runt där kapacitetsutnyttjande och potentiella sårbarheter analyseras regelbundet i syfte att optimera tillgänglighet och prestanda. Antura har flera olika loggar för att spara och följa upp olika typer av fel, intrångsförsök, förändringar och andra viktiga händelser som sker i systemet.

Antura tillämpar den senaste teknologin inom kryptering i syfte skydda kunddata från stöld eller förvanskning. Vidare erbjuder Antura ett flertal funktioner som möjliggör pseudonymisering eller gallring av personuppgifter.

## Hantering av personuppgifter

Antura har ett flertal rutiner till att stödja regelverket kring GDPR. Antura har bl.a. en rutin för att kunna rapportera personuppgiftsincidenter till berörda myndigheter inom de tidsramar som lagar och förordningar stipulerar, samt rutiner för hur gallring av personuppgifter skall genomföras. Antura eftersträvar att så långt som möjligt tillämpa privacy by design och privacy by default.

# Uppföljning och övervakning av Anturas verksamhet

Antura genomför regelbundet uppföljningar, analyser och utvärderingar av effektiviteten i arbetet med informationssäkerhet. Exempel på etablerade rutiner och åtgärder är:

- Kontinuerlig rapportering av KPI:er som mäter effektiviteten i rutiner och automatiserade åtgärder sker regelbundet, typiskt månadsvis
- Penetrationstester av Antura görs regelbundet av tredje part.
- Internrevisioner i syfte att granska efterlevnaden av de informationssäkerhetskrav Antura ställer på sin organisation genomförs flera gånger per år. Ev. avvikelser återrapporteras, planeras in för åtgärd och följs därefter upp.
- Antura genomgår årligen en externrevision där representanter från ett ackrediteringsorgan går igenom Anturas LIS och kontrollerar vår efterlevnad.
- Anturas Chief Information Security Officer (CISO) rapporterar löpande för Anturas ledningsgrupp hur det kontinuerliga informationssäkerhetsarbetet fortlöper samt hur de ställda målen kan uppnås.

# Antura ger stöd och resurser till den egna organisationen

Antura avdelar varje år resurser till organisationen i syfte att bibehålla och vidareutveckla den nivå av informationssäkerhet som etablerats. Dessa resurser omsätts till bl.a.:

## Kompetensutveckling

Antura säkerställer att alla anställda på Antura har rätt kompetens för att utföra sina uppgifter i förhållande till LIS och informationssäkerhetskraven. Utbildning och fortbildning genomförs i enlighet med gällande regler för anställning och introduktion av nyanställda eller vid tillträdandet av nya roller.

## Säkerhetsmedvetande

Antura säkerställer att personalen besitter ett högt säkerhetsmedvetande. Informationssäkerhet är en återkommande punkt på alla interna större möten och datorbaserade utbildningar genomförs regelbundet.

## Kommunikation kring informationssäkerhet

I de fall att osäkerheter råder beslutar CISO och VD kring vilken kommunikationskanal och vilket budskap som ska förmedlas.

## Projekt- och uppdragsledning

Informationssäkerhet beaktas inom projekt- och uppdragsledning i form av checklistor och metodstöd.

## Dokumentation av LIS

Antura dokumenterar och följer upp allt informationssäkerhetsarbete i Antura!

# Upprätthållande av informationssäkerheten på Antura

Det operativa arbetet med informationssäkerhet pågår ständigt på Antura. Implementationen av tekniska och organisatoriska åtgärder innebär att rutiner, checklistor, anvisningar och rent automatiserade åtgärder tillämpas dagligen. Upprätthållandet säkerställs genom att:

- Anturas personal tillämpar och efterlever fastslagna rutiner
- Löpande underhåll och förbättringar av åtgärder sker regelbundet
- Ledningen genomför mätning och uppföljning och av åtgärdernas effektivitet

Antura eftersträvar att hela tiden bli mer effektiva i informationssäkerhetsarbetet!

Genom ett målmedvetet, fokuserat och systematiskt angreppssätt säkerställer Antura att en hög informationssäkerhet kan upprätthållas. Därigenom bibehålles bolagets trovärdighet och kunders tillit till hur vi hanterar deras data och information.

---

**Antura har ett väl utvecklat och implementerat ISMS, där Anturas ISO 27001-certifiering är resultatet av bolagets medvetna och framgångsrika satsningar inom informationssäkerhet.**

- Berndt Roslund, Lead auditor, Intertek -

---

intertek
Total Quality. Assured.

# CERTIFICATE OF REGISTRATION

**This is to certify that the management system of:**

ANTURA

## Antura AB

Main site: Västra Hamngatan 13 A, SE-411 17 Gothenburg, Sweden

Additional site: Vasagatan 40, SE-111 20 Stockholm, Sweden

**has been registered by Intertek as conforming to the requirements of:**

## ISO/IEC 27001:2022

**The management system is applicable to:**

Development, maintenance, management, operations, and support of all products, solutions and services delivered by Antura.

This is in accordance with the statement of applicability Version 8. Date 13 September 2024.

**Certificate Number:**
0054823

**Initial Certification Date:**
07 October 2016

**Date of Certification Decision:**
25 September 2024

**Issuing Date:**
03 October 2024

**Valid Until:**
06 October 2025

ISO 27001:2022 CERTIFICATION
intertek
UKAS MANAGEMENT SYSTEMS
014

**Calin Moldovean**
President, Business Assurance

Intertek Certification Limited, 10A Victory Park, Victory Road, Derby DE24 8ZF, United Kingdom

Intertek Certification Limited is a UKAS accredited body under schedule of accreditation no. 014.

In the issuance of this certificate, Intertek assumes no liability to any party other than to the Client, and then only in accordance with the agreed upon Certification Agreement. This certificate's validity is subject to the organisation maintaining their system in accordance with Intertek's requirements for systems certification. Validity may be confirmed via email at certificate.validation@intertek.com or by scanning the code to the right with a smartphone. The certificate remains the property of Intertek, to whom it must be returned upon request.
CT_ ISO/IEC_27001:2022-UKAS-EN-A4-31.jul.23