Antura och NIS2 / cybersäkerhetslagen

Antura arbetar systematiskt med informationssäkerhet genom ett ledningssystem baserat på ISO27001:2022, GDPR och kravbilden i NIS2/cybersäkerhetslagen. Arbetet omfattar riskhantering, policyer och rutiner, säker utveckling och drift, åtkomstkontroll, kryptering, övervakning, incidenthantering, kontinuitetsplanering, leverantörsstyrning, utbildning samt löpande uppföljning och revision. Därigenom har Antura etablerade processer och kontroller som stödjer kunder som behöver bedöma leverantörer utifrån kraven i NIS2 och cybersäkerhetslagen.

Vad NIS2 och cybersäkerhetslagen innebär

NIS2 är EU:s reglering för en hög gemensam nivå av cybersäkerhet inom unionen. I Sverige har direktivet genomförts genom cybersäkerhetslagen, som trädde i kraft den 15 januari 2026. Regelverket omfattar verksamhetsutövare inom utpekade sektorer och ställer krav på ett systematiskt och riskbaserat cybersäkerhetsarbete. För verksamheter som omfattas är de centrala skyldigheterna att:

1. bedöma om verksamheten omfattas och anmäla sig enligt gällande regler,
2. vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska säkerhetsåtgärder,
3. rapportera betydande incidenter enligt regelverkets krav.

Anturas säkerhetsarbete i korthet

Anturas informationssäkerhetsarbete är en integrerad del av hur bolaget styr, utvecklar och levererar sina tjänster. Arbetet omfattar hela organisationen - från styrelse och ledning till utveckling, drift, support och kundnära funktioner.

Ledning och styrning

Ledningssystem för informationssäkerhet baserat på ISO27001:2022, GDPR och kravbilden i NIS2/cybersäkerhetslagen. Styrelse, VD och CISO har tydliga roller.

Riskbaserat arbetssätt

Regelbundna riskanalyser utifrån konfidentialitet, riktighet och tillgänglighet. Säkerhetsåtgärder dokumenteras och följs upp genom Statement of Applicability.

Säker utveckling och drift

Security by design och security by default i produktlivscykeln. Åtskilda utvecklings- och produktionsmiljöer, godkända versioner, loggning, övervakning och kryptering.

Åtkomst och dataskydd

Principen om least privilege, stöd för extern autentisering och rutiner för personuppgiftshantering, gallring, pseudonymisering samt privacy by design/default.

Incident och kontinuitet

Dokumenterade rutiner för klassificering, hantering och rapportering av incidenter samt kontinuitetsplanering med identifierade scenarier, övning och uppdatering.

Uppföljning och förbättring

KPI:er, regelbundna penetrationstester av tredje part, internrevisioner, extern revision och löpande rapportering från CISO till ledning.