

NIS2 Artikel 21

Tjekliste — 10 risikostyringsforanstaltninger + hændelsesrapportering

Alle krav fra NIS2 Artikel 21 med danske beskrivelser,
status-felter, ansvarlig og deadline. Klar til ledelse og revision.

■ Ikke påbegyndt	■ I gang	● Implementeret	N/A
------------------	----------	-----------------	-----

Virksomhed: _____ Dato: _____

Enhedstype: ■ Væsentlig (Annex I) ■ Vigtig (Annex II)

Udgivet af **GapGuard** — et produkt fra ITNU ApS
April 2026 · gapguard.dk

Denne tjekliste er gratis og må deles frit.
For automatiseret GAP-analyse med dashboards og mapping til CIS Controls v8:
Prøv GapGuard gratis i 7 dage →

Artikel 21 — Risikostyringsforanstaltninger

Alle 10 krav med beskrivelse, status og ansvarlig.

Artikel	Krav og beskrivelse	Status	Ansvarlig	Deadline
21(2)(a)	Politikker for risikoanalyse og informationssikkerhed Etablér formelle politikker for risikoanalyse og informationssikkerhed. Politikkerne skal godkendes af ledelsen, kommunikeres til alle relevante medarbejdere og revideres regelmæssigt.	■		
21(2)(b)	Hændeshåndtering Implementér processer for forebyggelse, detektion og håndtering af sikkerhedshændelser. Definér roller, eskaleringsprocesser og kommunikationsplaner. Test procedurene regelmæssigt.	■		
21(2)(c)	Driftskontinuitet og krisestyring Etablér beredskabsplaner for driftskontinuitet, herunder backup-strategier, disaster recovery og krisestyring. Sikr at kritiske systemer kan gendannes inden for definerede tidsrammer.	■		
21(2)(d)	Forsyningskædesikkerhed Vurdér og håndtér sikkerhedsrisici i leverandørkæden. Stil sikkerhedskrav til leverandører, monitorér deres overholdelse og etablér procedurer for leverandør-incidents.	■		
21(2)(e)	Sikkerhed ved anskaffelse, udvikling og vedligeholdelse Integrér sikkerhed i hele livscyklussen for IT-systemer: fra kravspecifikation og anskaffelse over udvikling til vedligeholdelse og udfasning. Inkludér sikkerhedstest og sårbarhedshåndtering.	■		
21(2)(f)	Vurdering af effektiviteten af foranstaltninger Mål og evaluér løbende om de implementerede sikkerhedsforanstaltninger faktisk virker. Brug KPI'er, audits og GAP-analyser til at dokumentere modenhed og fremgang over tid.	■		
21(2)(g)	Grundlæggende cyberhygiejne og awareness-træning Sikr at alle medarbejdere kender grundlæggende sikkerhedsprincipper: stærke passwords, phishing-genkendelse, sikker datahåndtering. Gennemfør regelmæssig awareness-træning og test.	■		
21(2)(h)	Politikker for kryptografi og kryptering Definér politikker for brug af kryptering til beskyttelse af data i transit og i hvile. Fastlæg standarder for nøglehåndtering, certifikater og krypteringsalgoritmer.	■		
21(2)(i)	Personalesikkerhed, adgangskontrol og asset management Dæk personalesikkerhed (baggrundstjek, onboarding/offboarding), adgangskontrol (least privilege, regelmæssige reviews, MFA) og asset management (inventar over hardware, software og data).	■		
21(2)(j)	Multifaktor-autentificering og sikker kommunikation Implementér MFA for alle kritiske systemer og fjernadgang. Brug sikre kommunikationsløsninger (krypteret e-mail, VPN, sikre videokonferencer) til følsom kommunikation.	■		

Hændelsesrapportering

NIS2 stiller krav om hurtig rapportering af væsentlige sikkerhedshændelser.

Frist	Type	Beskrivelse	Klar?
24 timer	Foreløbig underretning	Hurtig varsling til sektormyndigheden om at en væsentlig hændelse er opstået.	■
72 timer	Uddybende rapport	Vurdering af alvor, konsekvenser, kompromitteringsindikatorer og trufne foranstaltninger.	■
30 dage	Endelig rapport	Fuld årsagsanalyse, konsekvensanalyse og beskrivelse af afhjælpende foranstaltninger.	■

Artikel 20 — Ledelsens ansvar

Krav	Beskrivelse	✓
Godkendelse	Ledelsen har formelt godkendt risikostyringsforanstaltningerne	■
Overvågning	Ledelsen overvåger aktivt implementeringen af foranstaltningerne	■
Træning	Ledelsesmedlemmer har gennemgået cybersikkerhedstræning	■
Medarbejdertræning	Regelmæssig awareness-træning tilbydes alle medarbejdere	■

Træt af at udfylde tjeklisten manuelt?

GapGuard mapper automatisk fra CIS Controls v8 til NIS2 Artikel 21 med dashboards, scores og rapporter klar til ledelse og tilsyn.

→ **Prøv GapGuard gratis i 7 dage**

→ [Book en demo](#)

GapGuard — et produkt fra ITNU ApS · CVR 45557510
gapguard.dk · info@gapguard.dk