



TIL SMÅ OG MELLEMSTORE VIRKSOMHEDER I DANMARK

NIS2-tjekliste

30 ja/nej-spørgsmål, der viser, hvor jeres virksomhed står – på cirka 15 minutter.

- ✓ De 10 sikkerhedskrav i NIS2 forklaret i klart sprog
- ✓ 3 hurtige spørgsmål pr. krav
- ✓ En enkel score og hvad I bør gøre nu

polarit.dk

+45 31 67 10 87 • Support@PolarIT.dk

JUMPCLOUD MSP PARTNER

MAKE WORK HAPPEN 2026

PolarIT ApS
CVR 46412249

Er I omfattet af NIS2?

NIS2 er EU's opdaterede direktiv om cybersikkerhed. I Danmark gælder det via den danske NIS2-lov, som har været i kraft siden 1. juli 2025. Det omfatter mellemstore og store organisationer i 18 kritiske sektorer – og mange af deres leverandører mærker det også.

1 Arbejder I i en omfattet sektor?

Fx energi, transport, sundhed, digital infrastruktur, IT-serviceydelser, fremstilling, fødevarer, affald, kemikalier, post eller offentlig forvaltning.

2 Er I en mellemstor eller stor virksomhed?

Typisk 50 medarbejdere eller flere, eller en årlig omsætning over 10 mio. euro. Nogle organisationer er omfattet uanset størrelse.

3 Leverer I til en omfattet organisation?

Selv hvis I ikke selv er omfattet, skal jeres kunder styre risikoen i deres leverandørkæde – og vil i stigende grad bede jer dokumentere god sikkerhed.

Har I svaret ja til ét af spørgsmålene, er NIS2 relevant for jer. Tjeklisten er under alle omstændigheder et godt sundhedstjek.

Tre ting, enhver leder bør vide

01

Ledelsen har ansvaret

Ledelsen skal godkende sikkerhedstiltagene, føre tilsyn med dem og deltage i uddannelse – og kan holdes ansvarlig.

02

Hændelser skal indberettes hurtigt

Væsentlige hændelser: tidlig varsling inden for 24 timer, underretning inden for 72 timer og en endelig rapport inden for én måned.

03

Bøderne er betydelige

Op til 10 mio. euro eller 2 % af den globale omsætning for væsentlige enheder og op til 7 mio. euro eller 1,4 % for vigtige enheder.



Sådan bruger I tjeklisten

Svar ærligt ja eller nej til hvert spørgsmål. 'Delvist' tæller som nej. Sæt kryds ved hvert ja, og tæl jeres kryds sammen på sidste side.

De 10 sikkerhedskrav (NIS2 artikel 21)

21(a) Risikoanalyse & sikkerhedspolitikker

Kend jeres risici, og hav politikker, der styrer dem.

Vi har et skriftligt overblik over vores vigtigste systemer og data og de største risici for dem. Ja ☐

Vi har en informationssikkerhedspolitik, som ledelsen har godkendt. Ja ☐

Vi gennemgår vores risici og politik mindst én gang om året. Ja ☐

21(b) Håndtering af hændelser

Opdag, håndtér og indberet sikkerhedshændelser i tide.

Medarbejderne ved præcis, hvem de skal kontakte, hvis de har mistanke om en sikkerhedshændelse. Ja ☐

Vi har en skriftlig beredskabsplan, der også beskriver, hvem der indberetter til myndighederne inden for 24 timer. Ja ☐

Logs fra vores vigtigste systemer bliver indsamlet og gemt, så vi kan se, hvad der er sket. Ja ☐

21(c) Driftskontinuitet & backup

Hold forretningen kørende under og efter en hændelse.

Kritiske data bliver taget backup af, med mindst én kopi offline eller beskyttet mod sletning. Ja ☐

Vi har testet en gendannelse fra backup inden for de sidste 12 måneder. Ja ☐

Vi har en plan for at kunne arbejde, hvis e-mail, cloudtjenester eller kontoret ikke er tilgængelige. Ja ☐

21(d) Sikkerhed i leverandørkæden

Styr risikoen fra leverandører og tjenesteudbydere.

Vi har en liste over leverandører, der har adgang til vores systemer eller data. Ja ☐

Vores leverandørkontrakter indeholder krav til sikkerhed. Ja ☐

Leverandørers adgang er begrænset til det nødvendige og fjernes, når den ikke længere bruges. Ja ☐

21(e) Sikker anskaffelse & vedligehold

Hold systemerne sikre, når de købes, udvikles og vedligeholdes.

Styresystemer og software opdateres automatisk på alle enheder. Ja ☐

Sårbarheder på systemer, der vender ud mod internettet, bliver rettet hurtigt. Ja ☐

Vi tager stilling til sikkerhed, før vi køber eller bygger nye systemer. Ja ☐

21(f) Måling af effektivitet

Tjek, at jeres sikkerhedstiltag rent faktisk virker.

Vi tjekker jævnligt, at vores sikkerhedstiltag virker (gennemgange, test eller audits). Ja ☐

Vi kan fremvise dokumentation – rapporter eller logs – for, at vores kontroller er på plads. Ja ☐

Fund bliver fulgt op med en ansvarlig og en deadline. Ja ☐

21(g) Cyberhygiejne & uddannelse

Gode sikkerhedsvaner og awareness-træning for alle.

Alle medarbejdere har fået awareness-træning i sikkerhed inden for de sidste 12 måneder. Ja ☐

Stærke og unikke passwords er et krav – fx med en password manager. Ja ☐

Administratorrettigheder er begrænset til dem, der virkelig har brug for dem. Ja ☐

21(h) Kryptografi & kryptering

Beskyt data med kryptering, hvor det betyder noget.

Alle bærbare og mobile enheder har fuld diskkryptering slået til. Ja ☐

Data krypteres under overførsel – websites bruger HTTPS, og e-mail bruger TLS. Ja ☐

Vi har en enkel politik for kryptering og håndtering af krypteringsnøgler. Ja ☐

21(i) Personalesikkerhed, adgange & aktiver

Styr, hvem der har adgang til hvad – fra første til sidste dag.

Vi har en opdateret oversigt over enheder og brugerkonti. Ja ☐

Adgange følger princippet om mindst mulige rettigheder og gennemgås jævnligt. Ja ☐

Al adgang fjernes samme dag, som en medarbejder stopper. Ja ☐

21(j) Multifaktor-godkendelse

Brug MFA og sikker kommunikation.

MFA er påkrævet for e-mail og cloud-apps for alle brugere. Ja ☐

MFA er påkrævet for fjernadgang og alle administratorkonti. Ja ☐

Vi har en sikker måde at kommunikere på i en nødsituation, også hvis e-mail er nede. Ja ☐

Jeres score

/ 30

Tæl jeres kryds ud af 30.

● 25–30

I er godt med

I har det meste af det grundlæggende på plads. Fokusér på dokumentation – det er dét, revisorer og kunder vil spørge efter.

● 15–24

Tydelige huller

Fundamentet er der, men vigtige kontroller mangler. Prioritér MFA, adgangsstyring, backup og hændeshåndtering først.

● 0–14

Der er en del at gøre

Start med de hurtige gevinster, der fjerner mest risiko: MFA overalt, automatiske opdateringer, testet backup og offboarding samme dag.

Hurtige gevinster, der lukker flere huller på én gang

→ Slå MFA til for alle brugere og alle administratorkonti

→ Styr alle enheder centralt: opdateringer, kryptering og skærmlås håndhævet via politik

→ Én identitet til alle apps (single sign-on), så adgang fjernes ét sted

→ Test en gendannelse fra backup – og skriv ned, hvordan I gjorde

Vil I have et ekstra sæt øjne?

PolarIT hjælper danske virksomheder med at blive klar til NIS2 med én administreret platform til identitet, enheder, MFA og adgange – og dokumentationen, der beviser det.

Book en gratis snak om NIS2polarit.dk/nis2.html**Få et gratis eksternt sikkerhedstjek**polarit.dk/security-check.html

Joseph Cunningham · Grundlægger, PolarIT · +45 31 67 10 87 · Support@PolarIT.dk

Tjeklisten er generel vejledning, der kan hjælpe jer med at vurdere jeres parathed. Den er ikke juridisk rådgivning og erstatter ikke en vurdering af jeres konkrete forpligtelser efter den danske NIS2-lov.