Pejlemærker og observationspunkter til NIS2 compliance

1. Risikostyring

NIS2-krav	Pejlemærker og observationspunkter
Direktion og bestyrelse skal 1. godkende virksomhedens foranstaltninger til styring af cybersikkerhedsrisici 2. føre tilsyn med deres gennemførelse 3. kunne gøres ansvarlige for virksomhedens overtrædelser af minimumsforanstaltninger (jf. nedenfor).	• Rammesætning af ledelsens cybersikkerhedsstrategi og fastlæggelse af risikoappetit. • Fastlæggelse af indhold, kvalitet og frekvens af rapporter og risikovurderinger til ledelsen. • Identifikation af konkrete kontrolpunkter (teknisk, operationelt og organisatorisk), herunder ift. tests og leverandører. • Fastlæggelse af (omfanget af) anvendelsen af anerkendte standarder som ISO 27001, NIST og CIS-kontroller.
Bestyrelse og direktion er forpligtet til at følge cybersikkerhedsrelaterede kurser og skal få medarbejdere til at gøre det samme.	• Gennemførelse af løbende cybersikkerhedskurser. • Udvikling af tilpassede uddannelses- og træningsprogrammer. • Forædling af virksomhedens cybersikkerhedskultur.

2. Minimumsforanstaltninger

NIS2-krav	Pejlemærker og observationspunkter
Politikker for risikoanalyse og informationssystemsikkerhed.	• Fastlæggelse af samlet risikotilgang, herunder risikoforståelse, risikovurdering og risikokvantificering.
Planer for håndtering af hændelser (incidents).	• Etablering af bistand fra leverandører og plan for involvering af eksterne eksperter.
Procedurer for driftskontinuitet og krisestyring.	• Indførelse af krav til og test af offline og/eller eksterne back-up services.
Forsyningskædesikkerhed (leverandørsikkerhed).	• Identifikation og risikovurdering af kritiske primært digitale leverandører. • Indførelse af krav til sikkerhed, rapportering, dokumentation og audit i leverandørkontrakter. • Fastlæggelse af risiko- og ansvarsfordeling i kontrakter og forsikringspolicer. • Etablering af sammenhæng med virksomhedens håndtering af persondata (GDPR og databehandleraftaler).
Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer.	• Anvendelse af due diligence og request lists i forbindelse med kontraktindgåelser, herunder køb og salg af virksomheder. • Indførelse af designkrav og brug af standarder. • Understøttelse af pligt til offentliggørelse af sårbarheder.
Politikker og procedurer til vurdering af effektivitet af foranstaltninger til styring af cybersikkerhedsrisici.	• Indførelse af krav til kontroller, test, rapportering og audit - både internt og eksternt, herunder i leverandørkontrakter.
Basal cyberhygiejne og -uddannelse.	• Indførelse af basal cyberhygiejne, herunder oversigter, multi-faktor, patching, antivirus, backup, overvågning, logging, adgangsbegrænsning, AD-beskyttelse, segmentering, OT-systemer, VPN og awareness.
Politikker og procedurer om kryptografi og kryptering.	• Identifikation af omfang og lokationer hvor data er "i bevægelse". • Valg af krypteringsmodel til forebyggelse, detektion og genetablering.
Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.	• Etablering af CMDB og Asset registre samt dokumentation herfor. • Styring af bruger- og adgangsrettigheder, herunder brugere med administrative eller eksterne adgange.
Multifaktorautentificering og sikker kommunikation, herunder et "nødkommunikationssystem".	• Etablering af multifaktor brugervalidering på alle fjernadgange. • Sikring af kommunikationslinje(r) til en krisesituation (hvor outlook for eksempel er utilgængelig).

3. Rapporteringsforpligtelser

NIS2-krav	Pejlemærker og observationspunkter
Tre-trinsunderretning af tilsyn ved væsentlige hændelser. Frist: • 24 timer (tidlig varsling) • 72 timer (indledende vurdering) • Èn måned (endelig rapport).	• Forberedelse af gennemførelse af væsentligheds- og sandsynligheds-vurdering og kriterier. Herunder om en hændelse aktuelt er eller poten-tielt kan være væsentlig og have grænseoverskridende virkninger. • Opdatering af processer for hændelseshåndtering, herunder alarmer, roller og leverandørkrav. • Etablering af processer, templates og ansvarlige for underretning af myndigheder indenfor henholdsvis 24-72 timer og en måned. • Forberedelse af ekstern bistand til vurderinger og rapportering.
Underretning af kunder ved væsentlige hændelser. Frist: Uden unødigt ophold.	• Forberedelse af gennemførelse af væsentligheds- og sandsynligheds-vurdering og kriterier herfor, herunder om en hændelse aktuelt er eller potentielt kan være væsentlig og sandsynligvis påvirker services til kunden. • Opdatering af processer for hændelseshåndtering, herunder alarmer, roller og leverandørkrav. • Etablering af processer, templates og ansvarlige for underretning af kunderne, herunder om (i) evt. foranstaltninger eller modforholdsregler, som kunden kan træffe, og (ii) hvor relevant selve cybertruslen. • Forberedelse af ekstern bistand til vurderinger og rapportering.
Pligt til offentliggørelse af væsentlige hændelser.	• Betydning for bestyrelsens og direktionens fastlæggelse af risikoappetit indenfor cybersikkerhed, herunder i hvilket omfang offentliggørelsespligt eventuelt påvirker kommercielle interesser og fortrolighed.

4. Standarder

NIS2-krav	Pejlemærker og observationspunkter
Tilskyndelse til brug af standarder og tekniske specifikationer.	• Overvejelse om anvendelse af standarder m.v. ISO 27001/2 vil være en god basis for arbejdet med kravene i NIS2-direktivet. Samtidig vil NIST-rammeværket og CIS-kontrollerne vil være en god baseline for best practices. • Den danske mærkningsordning, D-mærket, kan overvejes i SMV-segmentet.

5. Tilsyn, håndhævelse og ansvar

NIS2-krav		Pejlemærker og observationspunkter
Væsentlige enheder (*Omfattende forudgående og efterfølgende tilsynsordning*).	Niveau 1 • Kontroller, sikkerheds-audits og sikkerheds-scanninger. • Oplysninger, data og dokumenter. • Advarsler, instrukser, påbud og forbud. • Indsættelse af en over-vågningsansvarlig. • Offentliggørelse af over-trædelser. • Administrative bøder. (maksimum mindst 10 mio. euro mindst 2 % af den samlede globale årsomsætning i det fore-gående regnskabsår).	Forberedelse til håndtering af tilsynsordning. Dokumentation bliver væsentlig for at reducere risikoen for sanktioner. Omfatter blandt andet dokumentation af: 1. cybersikkerhedspolitikker og gennemførelsen heraf 2. risikovurderinger 3. håndtering af identificerede risici 4. resultater af tests og audits samt 5. implementering af krav til og risikofordeling af leverandørsikkerhed i kontrakter.
	Niveau 2 • Midlertidig suspension af services. • Midlertidigt forbud mod ledelsesfunktioner (direk-tionsniveau).	• Forberedelse til håndtering af tilsynsordning. Bringes først i spil, hvis (i) én eller flere sanktioner nævnt ovenfor har været anvendt men har vist sig virkningsløse, og (ii) der ikke er sket afhjælpning indenfor en given frist.
Vigtige enheder (*Lettere efter-følgende tilsyns-ordning*).	• Kontroller, sikkerheds-audits og sikkerheds-scanninger. • Oplysninger, data og dokumenter. • Advarsler, instrukser, påbud og forbud. • Pligt til underretning af kunder om væsentlig cybertrusler. • Gennemføre anbefalinger fra en sikkerhedsaudit • Offentliggørelse af over-trædelser. • Administrative bøder (maksimum mindst 7 mio. euro eller mindst 1,4 % af den samlede globale årsomsætning i det fore-gående regnskabsår).	• Forberedelse til håndtering af tilsynsordning. Dokumentation er til-svarende vigtigt som hos væsentlige enheder, men uden samme høje krav til løbende og systematisk dokumentation af overholdelse af for-anstaltninger til styring af cybersikkerhedsrisici. • Efterfølgende tilsyn kan udløses af dokumentation eller oplysninger, som tilsynet gøres opmærksom på, og som tyder på potentielle overtræ-delser, herunder oplysninger fra myndigheder, borgere, medier, kunder eller andre kilder.
Ledelsesansvar.	• Ledelsesansvarlige skal kunne drages til ansvar for overtrædelse af deres forpligtelse til at sikre overholdelse af NIS2.	• Sikring af, at medlemmer af bestyrelse og direktion dels er bekendte med både NIS2's krav og den samlede risikostyring, som virksomheden har im-plementeret (herunder om den opfylder kravene), dels fører kontrol hermed. • Civilretligt erstatningsansvar kan udløses (som det primære ansvar). • Bredt forretningsmæssigt skøn tilladt forudsat at beslutninger træffes på et oplyst grundlag (business judgment rule).