

Sektorspecifik vejledning
til NIS 2-loven

Offentlige forvaltnings- enheder under den centrale forvaltning



Styrelsen for
Samfundssikkerhed

Denne vejledning er udarbejdet af Styrelsen for Samfundssikkerhed.
Vejledningen er sektorspecifik og henvender sig til offentlige
forvaltningsenheder under den centrale forvaltning.

Datavej 20
3460 Birkerød
Telefon: +45 4516 1666
E-mail: tilsyn@samsik.dk

1. udgave oktober 2026.

INDHOLD

ORDLISTE	4
1. FORMÅL MED VEJLEDNINGEN	6
Målgruppe	6
Læsevejledning	6
2. ANVENDELSESOMRÅDET	7
Hvad er en offentlig forvaltningsenhed under den centrale forvaltning?.....	7
Undtagelse af specifikke offentlige forvaltningsenheder	9
Registrering	9
3. LEDELSE.....	10
4. FORANSTALTNINGER.....	10
ISO 27001 og tekniske minimumskrav i relation til NIS 2-tilsynet	10
Opgaver varetaget af og løsninger driftet hos andre myndigheder.....	12
5. HÆNDELSESUNDERRETNING.....	13
6. TILSYN OG HÅNDHÆVELSE	14
Det proaktive tilsyns tilrettelæggelse	14
Det reaktive tilsyn	16
Håndhævelse.....	16
BILAG 1: SAMMENHÆNG MELLEM TEKNISKE MINIMUMSKRAV OG NIS 2-LOVENS CYBERSIKKERHEDSFORANSTALTNINGER	17

ORDLISTE

CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM)

En national eller sektorbaseret enhed, udpeget eller oprettet af en medlemsstat i EU i henhold til artikel 10 i NIS 2-direktivet, med ansvar for at forebygge, detektere og håndtere cybersikkerhedshændelser. I Danmark er CSIRT en national enhed. CSIRT's opgaver omfatter bl.a. hændelseshåndtering, varsling og koordinering med relevante myndigheder og private aktører. CSIRT er en central aktør i både den nationale cybersikkerhedsstruktur og i det europæiske CSIRT-netværk, jf. artikel 15 i NIS 2-direktivet med fokus på samarbejde og informationsdeling på tværs af medlemsstaterne

CYBERHYGIEJNE

Cyberhygiejne dækker i NIS 2-loven over de grundlæggende foranstaltninger og daglige sikkerhedsvaner, praksisser og procedurer, som beskytter netværk, systemer og data mod almindelige trusler. Det omfatter f.eks. brug af stærke passwords, regelmæssig opdatering af software, sikkerhedskopiering, brug af antivirus samt opmærksomhed på phishing og andre digitale angreb.

CYBERSIKKERHED

De aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler.

DIREKTE LEVERANDØR

En leverandør, der har en direkte aftale med en NIS 2-omfattet enhed, og som leverer produkter eller tjenester, der påvirker enhedens net- og informationssystemer.

DOKUMENTATION

Dokumentation er nedskrevne politikker og procedurer, som alle relevante medarbejdere i enhederne har adgang til. Det kan eksempelvis være i form af papirdokumenter, sider på enhedernes intranet eller i en vidensdatabase. Enhederne kan benytte sig af den metode og form, de i forvejen anvender til at opbevare og formidle deres procedurer og lignende. I forbindelse med tilsyn kan dokumentation også antage andre former, som eksempelvis netværksovervågnings-logs, udskrift af adgangstilladelse, referater m.v.

Dokumentationen skal under alle omstændigheder kunne gøres tilgængelig for tilsynet, der har behov for adgang til data, dokumenter og oplysninger, som er nødvendige for udførelsen af tilsynsopgaven.

ENHED

I NIS 2-loven defineres en enhed som en fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale ret på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser. En enhed kan – udover at være en fysisk person – anses for at være virksomheder, foreninger, organisationer og offentlige myndigheder mv. (juridiske personer), der er tildelt et CVR-nummer. Et selskab med et underliggende datterselskab vil således være at anse for to separate enheder, forudsat at de har fået tildelt hver deres CVR-nummer.

CYBERSIKKERHEDSFORANSTALTNINGER

Tiltag, der fremmer sikkerhed, som både omfatter tekniske, operationelle og organisatoriske foranstaltninger, der fastholder og/eller ændrer en risiko. Der er oplyst ti minimumskrav til foranstaltninger i NIS 2-lovens § 6, stk. 1, nr. 1–10.

HÆNDELSE

En begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare (NIS 2-lovens § 3, nr. 12). På engelsk ofte benævnt "incident".

NET- OG INFORMATIONSSYSTEM

Et net- og informationssystem er i NIS 2-loven defineret som:

- Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabel-systemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.
- Enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data.
- Digitale data som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.

Eksempler på dette kan være it-systemer, OT-systemer, IoT-enheder og it infrastrukturkomponenter.

OFFENTLIGE FORVALTNINGSENHEDER UNDER DEN CENTRALE FORVALTNING

Enhedstype under sektor 10 "Offentlig forvaltning" opført i bilag 1 (sektorer af særlig kritisk betydning) til NIS 2-loven. Se afsnit 2 for en nærmere gennemgang heraf.

SEKTORANSVARLIGE MYNDIGHEDER

Begrebet beskriver den myndighed, der har ansvaret for at sikre, at enheder i specifikke sektorer overholder lovens forpligtelser. De sektoransvarlige myndigheder udpeges af ministeren for samfundssikkerhed og beredskab efter forhandling med de relevante ressortministre. Udpegningen sker ved bekendtgørelse forud for NIS 2-lovens ikrafttræden. I NIS 2-direktivet, NIS 2-loven og bekendtgørelsen anvendes begrebet "kompetente myndigheder".

VÆSENTLIG HÆNDELSE

En hændelse anses i henhold til NIS 2-loven for at være væsentlig, hvis en af følgende betingelser er opfyldt:

Hændelsen har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed.

Hændelsen har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikkefysisk skade

1. FORMÅL MED VEJLEDNINGEN

Formålet med vejledningen er at uddybe de dele af lov nr. 434 af 6. maj 2025 om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven), der kan være særlige for offentlige forvaltningsenheder under den centrale forvaltning.

Denne vejledning skal hjælpe enheder med viden om, hvilke parametre der skal lægges vægt på, når det skal vurderes, om en enhed er omfattet af NIS 2-loven som en offentlig forvaltningsenhed under den centrale forvaltning, hvem "ledelsen" hos sådanne enheder er, samt forholdet mellem NIS 2-loven og henholdsvis de tekniske minimumskrav for statslige myndigheder og ISO27001. Vejledningen vil også give viden om underretningspligten, og hvordan tilsyn og opfølgning vil fungere.

MÅLGRUPPE

Vejledningens målgruppe er enheder, som er omfattet af NIS 2-loven som offentlige forvaltningsenheder under den centrale forvaltning. Læs nærmere om anvendelsesområdet i afsnit 2.

LÆSEVEJLEDNING

Styrelsen for Samfundssikkerhed har som koordinerende myndighed til opgave at facilitere et tæt samarbejde mellem de sektoransvarlige myndigheder. I kraft heraf har Styrelsen for Samfundssikkerhed publiceret en række tværgående vejledninger, der beskriver de centrale og tværgående begreber og krav i NIS 2.

Derudover har Styrelsen for Samfundssikkerhed som sektoransvarlig myndighed for kommunerne, jf. bekendtgørelse nr. 620 af 2. juni 2025, udstedt en sektorspecifik vejledning til kommuner om NIS 2-loven.

Styrelsen for Samfundssikkerhed er ligeledes sektoransvarlig myndighed for offentlige forvaltningsenheder under den centrale forvaltning, jf. bekendtgørelse nr. 620 af 2. juni 2025. Nærværende vejledning udgør Styrelsen for Samfundssikkerheds sektorspecifikke vejledning for offentlige forvaltningsenheder under den centrale forvaltning.

Vejledningen beskriver og uddyber centrale dele af NIS 2-loven med fokus på særlige forhold for offentlige forvaltningsenheder under den centrale forvaltning. Vejledningen beskæftiger sig derfor ikke med generelle forhold, der er beskrevet i andre vejledninger.

Eksempelvis vil det for en uddybning af de generelle krav til foranstaltninger, der følger af NIS 2-loven, være relevant at orientere sig i den tværgående vejledning om cybersikkerhedsforanstaltninger og derefter i nærværende vejledning for så vidt angår særlige forhold, der gør sig gældende for offentlige forvaltningsenheder under den centrale forvaltning.

Det bemærkes, at Sundhedsdatastyrelsen, jf. bekendtgørelse nr. 620 af 2. juni 2025, er sektoransvarlig myndighed for regionerne, hvorfor spørgsmål i relation til NIS 2-loven vedrørende regionerne skal rettes til Sundhedsdatastyrelsen.

2. ANVENDELSESOMRÅDET

Det siger NIS 2-loven:

§ 4, stk. 3, nr. 2 *Uanset deres størrelse anses følgende enheder for at være væsentlige enheder:*
 (...)

2) Offentlige forvaltningsenheder under den centrale forvaltning

(...)

HVAD ER EN OFFENTLIG FORVALTNINGSENHED UNDER DEN CENTRALE FORVALTNING?

I bemærkningerne til NIS 2-loven er der opsat en række kriterier, som kan anvendes til at fastlægge, hvornår der er tale om en offentlig forvaltningsenhed under den centrale forvaltning. Lovbemærkningerne afspejler bl.a. de kriterier, der opstilles i NIS 2-direktivets artikel 6, nr. 35.

For det første skal enheden være anerkendt som en offentlig forvaltningsenhed efter national ret.

Ved vurderingen af hvorvidt en enhed udgør en offentlig forvaltningsenhed efter dansk ret, kan der ifølge lovbemærkningerne lægges vægt på følgende væsentlige kriterier:

- Om enheden er oprettet ved lov eller på privat initiativ.
- Om enheden er placeret i et over-/underordningsforhold til en forvaltningsmyndighed.
- Om enhedens drift finansieres ved offentlig bevilling eller private midler.
- Om der ved lov er fastsat regler med hensyn til anvendelsen af de bevilgede midler.

Der er ikke tale om kumulative kriterier, som alle skal være opfyldt, men en konkret helhedsvurdering. I tvivlstilfælde vil der også kunne lægges vægt på, om enheden udøver offentligretlige funktioner.

Enhedens eventuelle benævnelse som "råd", "institut" eller lignende vil ikke være afgørende for, om det omfattes af begrebet den offentlige forvaltning og de fire love (forvaltningsloven, offentlighedsloven, retssikkerhedsloven og ombudsmandsloven).

For det andet oplystes i NIS 2-direktivet følgende kriterier for, hvornår en offentlig forvaltningsenhed er omfattet af direktivets anvendelsesområde:

- a) Enheden er oprettet med henblik på at opfylde almennyttige formål og har ikke industriel eller kommerciel karakter.
- b) Enheden har status som juridisk person eller er ved lov berettiget til at handle på vegne af en anden enhed med status som juridisk person.
- c) Enheden finansieres overvejende af staten, regionale myndigheder eller af andre offentligretlige organer, er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer, eller har et administrations-, ledelses- eller tilsynsorgan, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale myndigheder eller andre offentligretlige organer.
- d) Enheden har beføjelse til at rette administrative eller lovgivningsmæssige afgørelser til fysiske eller juridiske personer, der påvirker deres rettigheder i forbindelse med grænseoverskridende bevægelse for personer, varer, tjenester eller kapital.

Der er her tale om kumulative kriterier. Kriterie c) indeholder en række betingelser. Her skal man være opmærksom på, at det er tilstrækkeligt at opfylde én af betingelserne. Med andre ord er kriterierne a)-d) obligatoriske dog således, at kriterie c) indeholder tre alternative kriterier, hvoraf mindst ét skal være opfyldt.

I henhold til ovenstående vil myndigheder som departementer, styrelser og institutioner, som f.eks. Udbetaling Danmark være omfattet af NIS 2-loven som offentlige forvaltningsenheder under den centrale forvaltning. Selvstændige offentlige virksomheder vil også kunne være omfattet af NIS 2-loven som offentlige forvaltningsenheder under den centrale forvaltning. Statslige institutioner, der er organiseret i selskabsform, vil dog ikke umiddelbart være en del af den centrale offentlige forvaltning i henhold til NIS 2-loven.

Folketinget og visse organer med organisatorisk tilknytning til Folketinget, Rigsrevisionen, Folketingets Ombudsmand, domstolene, udenlandske myndigheder og internationale organisationer falder uden for den forvaltningsretlige definition af "den offentlige forvaltning". Disse organer udgør derfor ikke "offentlige forvaltningsenheder under den centrale forvaltning" i NIS 2-lovens forstand.

Der henvises i øvrigt til Styrelsen for Samfundssikkerheds generelle vejledning til NIS 2-loven om "Anvendelsesområdet".

UNDTAGELSE AF SPECIFIKKE OFFENTLIGE FORVALTNINGSENHEDER

I medfør af § 1, stk. 4, finder loven ikke anvendelse på offentlige forvaltningsenheder, som udfører deres aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger. Det følger dog af NIS 2-direktivets præambelbetragtning nr. 8, at offentlige forvaltningsenheder, hvis aktiviteter kun er marginalt forbundet med disse områder, ikke bør undtages fra anvendelsesområdet.

Det følger desuden af NIS 2-direktivets præambelbetragtning nr. 8, at offentlige forvaltningsenheder, der er etableret i fællesskab med et tredjeland i overensstemmelse med en international aftale, er udelukket fra NIS 2-direktivets anvendelsesområde. Det følger videre af samme præambelbetragtning, at direktivet ikke finder anvendelse på medlemsstaternes diplomatiske og konsulære missioner i tredjelande eller på deres net- og informationssystemer, for så vidt sådanne systemer befinder sig i missionens lokaler eller drives for brugere i et tredjeland.

REGISTRERING

Offentlige forvaltningsenheder under den centrale forvaltning er uanset størrelse *væsentlige* enheder og skal registrere sig som sådanne via Virk.dk.

En offentlig forvaltningsenhed under den centrale forvaltning skal også registrere sig i andre sektorer som nævnt i lovens bilag 1 og 2, hvis enheden også har aktiviteter, der gør, at den bliver omfattet af disse andre sektorer. F.eks. vil en offentlig forvaltningsenhed under den centrale forvaltning, som også er udbyder af datacentertjenester, jf. NIS 2-lovens bilag 1, sektor 8, også skulle registrere sig som udbyder af datacentertjenester i sektoren Digital Infrastruktur.

Offentlige forvaltningsenheder under den centrale forvaltning vil i denne sammenhæng uanset eventuelle aktiviteter i andre sektorer alene være underlagt tilsyn fra Styrelsen for Samfundssikkerhed, der er den sektoransvarlige myndighed for offentlige forvaltningsenheder under den centrale forvaltning. For mere herom henvises til afsnit 6 om tilsyn.

3. LEDELSE

Det siger NIS 2-loven:

§ 3 nr. 20, litra c) *For offentlige myndigheder er ledelsesorganet den øverste administrative ledelse i myndigheden.*

I offentlige forvaltningsenheder under den centrale forvaltning vil ledelsesorganet typisk være en direktion, hvis myndigheden har en direktion. I offentlige myndigheder, der ikke har en direktion, vil ledelsesorganet være et andet ledelsesorgan på tilsvarende niveau. I et departement, som ikke har en direktion, vil ledelsesorganet således være departementschefen og vicedirektører eller afdelingschefer. I en styrelse vil ledelsesorganet være direktionen.

For mere viden henvises til Styrelsen for Samfundssikkerheds generelle vejledning til NIS 2-loven om "*Ledelsens rolle og opgaver*".

4. FORANSTALTNINGER

Offentlige forvaltningsenheder under den centrale forvaltning er omfattet af NIS 2-loven i deres helhed. Det betyder ikke, at alle systemer og aktiviteter nødvendigvis skal have samme niveau af sikkerhed, men det betyder, at alle systemer og aktiviteter skal indgå i enhedens arbejde med cyber- og informationssikkerhed. Læs mere herom i Styrelsen for Samfundssikkerheds generelle vejledning til NIS 2-loven om "*Implementering af cybersikkerhedsforanstaltninger*".

Det gælder for de forvaltningsenheder, der også er omfattet gennemførelsesforordning (EU) 2024/2690 (f.eks. som udbydere af cloudcomputingtjenester, tillidstjenester eller datacenter), at de tværgående, udspecifiserede metodologiske og teknologiske krav, som følger af gennemførelsesforordningen, gælder for hele enheden, med mindre det i den enkelte bestemmelse i gennemførelsesforordningen er specifikt angivet, at bestemmelsen kun angår en bestemt type af roller, udbyder eller på anden måde eksplicit afgrænset del af forretningen.

ISO 27001 OG TEKNISKE MINIMUMSKRAV I RELATION TIL NIS 2-TILSYNET
ISO 27001 har igennem en årrække været anvendt i staten med henblik på sikring af informationssikkerheden i staten, ligesom de tekniske minimumskrav har været anvendt med det formål at sikre et højt fælles minimumsniveau af teknisk sikkerhed på tværs af enhederne uafhængigt af individuelle risikovurderinger.

ISO 27001 er en international ledelsesstandard for informationssikkerhed. ISO 27001 opstiller blandt andet krav til risikostyring, dokumentation af processer samt fordeling af roller og ansvar for informationssikkerhed.

De tekniske minimumskrav er en række tekniske krav rettet mod statslige myndigheder inden for kategorierne klienter/PC'er, mail, autentifikation, password, mobile enheder, logning, domænesikkerhed, netværk, internetvendte tjenester og interne it-systemer, som har til formål at sikre et fælles højt sikkerhedsniveau i staten. De tekniske minimumskrav udarbejdes af Styrelsen for Samfundssikkerhed.

Med NIS 2-loven indføres et lovgrundlag til sikring af et højere og mere ensartet cybersikkerhedsniveau. Loven indfører krav til cybersikkerhedsforanstaltninger underlagt tilsyns-, kontrol- og håndhævelsesforanstaltninger.

NIS 2-loven stiller krav om, at enheder omfattet af loven skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger til styring af cybersikkerhedsrisici. Disse skal som minimum omfatte de foranstaltninger, som fremgår af lovens § 6, stk. 1, nr. 1-10.

For offentlige forvaltningsenheder under den centrale forvaltning kan anvendelsen af ISO 27001 samt efterlevelse af de tekniske minimumskrav i høj grad bidrage til at overholde foranstaltningskravene i NIS 2-loven. Omvendt er anvendelse af ISO 27001-standarden og efterlevelse af de tekniske minimumskrav ikke nødvendigvis tilstrækkelig i sig selv til at sikre overholdelse af foranstaltningskravene i NIS 2-loven.

ISO 27001 kan fortsat anvendes til at give en fælles struktur og sprog for sikkerhedsarbejdet blandt de offentlige forvaltningsenheder under den centrale forvaltning. Alternativt kan en anden international anerkendt standard anvendes.

Henset til de fordele der er ved genkendeligheden, tilrettelægger Styrelsen for Samfundssikkerhed tilsynet med de offentlige forvaltningsenheder under den centrale forvaltning under hensyntagen til de statslige myndigheders erfaringer med ISO-standarden, se nærmere herom i denne vejlednings afsnit 6 om tilsyn og håndhævelse. De tekniske minimumskrav vil desuden indgå som en integreret del af tilsynet og vurderingen af, om de omfattede enheder har truffet passende og forholdsmæssige tekniske foranstaltninger i henhold til NIS 2-loven, jf. denne vejlednings afsnit 6.

I Styrelsen for Samfundssikkerheds generelle vejledning til NIS 2-loven om *"Implementering af cybersikkerhedsforanstaltninger"* er de enkelte foranstaltninger kortlagt op mod de tilsvarende ISO 27001-foranstaltninger. De tekniske minimumskrav er tilsvarende kortlagt op mod de enkelte NIS 2 cybersikkerhedsforanstaltninger i bilaget til denne vejledning. Eventuelle justeringer af de tekniske minimumskrav vil fra Styrelsen for Samfundssikkerhed blive udmeldt med behørigt varsel, så der er tid til implementering hos enhederne.

OPGAVER VARETAGET AF OG LØSNINGER DRIFTET HOS ANDRE MYNDIGHEDER
Der anvendes i staten en række tekniske løsninger, som er påkrævet ved lov, regeringsbeslutning eller lignende. Endvidere stilles fællesstatslige løsninger til rådighed, som anvendes af en række andre myndigheder og institutioner. Dette gælder f.eks. standardløsninger og basal it-drift hos Statens IT, fællesstatslige administrative løsninger udbudt af Økonomistyrelsen og fællesoffentlige løsninger som MitID og Digital Post hos Digitaliseringsstyrelsen.

Driftsmyndighederne, der driver de fællesstatslige løsninger mv. (Økonomistyrelsen, Digitaliseringsstyrelsen og Statens IT), er i sig selv offentlige forvaltningsenheder under den centrale forvaltning, og de er derfor selvstændigt omfattet af NIS 2-loven som væsentlige enheder. Dette betyder, at de er forpligtede til at efterleve NIS 2-loven for så vidt angår de systemer de drifter og udbyder, ligesom de også skal underrette om væsentlige hændelser, når sådanne indtræder. Styrelsen for Samfundssikkerhed fører tilsyn med Digitaliseringsstyrelsens, Økonomistyrelsens og Statens IT's efterlevelse af bestemmelserne i NIS 2-loven.

I henhold til NIS 2-reguleringen er det væsentligt at bemærke, at offentlige forvaltningsenheder under den centrale forvaltning, der som aftagere eller kunder, frivilligt eller pligtigt anvender de fællesstatslige løsninger mv., også er selvstændigt omfattet af NIS 2-reguleringen som væsentlige enheder. I denne sammenhæng er de nævnte driftsmyndigheder i forhold til kunderne at betragte som leverandører og/eller tjenesteudbydere.

Det påhviler alle enheder, der er omfattet af NIS 2-loven, at tage højde for sikkerheden i alle anvendte net- og informationssystemer – og herunder også tage højde for effekten af eventuelle hændelser på deres eget brug af den pågældende løsning. Dette skal f.eks. ske i enhedernes egne procedurer til sikring af driftskontinuitet, foranstaltninger i forhold til forsyningskædesikkerhed og processer for krisestyring mv.

Omfattede enheder skal derfor, i fornødent omfang og under hensyntagen til, at der fsva. Digitaliseringsstyrelsen, Økonomistyrelsen og Statens IT ikke er tale om ordinære aftale- og leverandørforhold, være med til at sikre, at driftsmyndighederne, som leverandører og/eller tjenesteudbydere stiller relevant dokumentation til rådighed, således at de omfattede enheder på et så kvalificeret grundlag som muligt kan træffe evt. interne mitigerende foranstaltninger samt udarbejde egne risikovurderinger og beredskabsplaner i

tilfælde af manglende adgang til eller anden kompromittering af de pågældende systemer.

For så vidt angår systemer leveret af Økonomistyrelsen og Statens It bidrages til dette via Finansministeriets tilsyn med systemerne på vegne af kunderne (se *Vejledning om tilsynet med Statens It (2025)* og *Vejledning om tilsynet med Økonomistyrelsens fællesstatslige systemer (2019)*). Statens IT stiller herudover bl.a. et hjælpeark til rådighed for kunderne, som præciserer det indbyrdes ansvar mellem kunder og Statens IT, i forhold til håndtering af tekniske minimumskrav i de driftede løsninger. Digitaliseringsstyrelsen vil i relevant omfang få udarbejdet NIS 2-ledelseserklæringer, som kunder vil kunne rekvirere på digst.dk.

5. HÆNDELSESUNDERRETNING

Det påhviler altid den enkelte enhed at foretage underretning om væsentlige hændelser, hvis den væsentlige hændelse kan føre til alvorlig driftsforstyrrelse af enhedens tjenester, betydelig økonomisk skade for enheden eller betydelig skade for tredjepart. Dette gælder, uanset om den væsentlige hændelse vedrører net- og informationssystemer, der administreres af enheden selv, eller om driften er outsourcet til en ekstern leverandør.

En enhed kan dog indgå en aftale om, at den virksomhed, der f.eks. driver enhedens net- og informationssystemer, kan foretage underretninger på vegne af enheden. Ansvar for, at der sker en rettidig hændelsesunderretning, påhviler dog altid enheden, ligesom det altid er enhedens ansvar at sikre, at hændelsesunderretningen er fyldestgørende og korrekt.

Hændelsesunderretninger sendes til CSIRT samt Styrelsen for Samfundssikkerhed, der er sektoransvarlig myndighed. CSIRT giver en tilbagemelding om hændelsen, og Styrelsen for Samfundssikkerhed kan herudover som sektoransvarlig myndighed eventuelt også foretage en opfølgning i forhold til hændelsen i form af et reaktivt tilsyn.

For fællesstatslige løsninger mv. gælder det, at den ansvarlige driftsmyndighed kan indberette evt. hændelser på vegne af alle tilsluttede aftagere, således at aftagerne ikke alle skal indberette den samme hændelse. I praksis kan dette lettest ske i forbindelse med 24-timers underretningen, idet senere underretninger kræver nøje kendskab til hændelsens konsekvenser, som typisk vil variere mellem brugerne. En forudsætning for indberetning på vegne af alle tilsluttede aftagere er, at driftsmyndighederne og aftagerne forudgående for hvert enkelt system, der anvendes, afklarer og aftaler skriftligt, hvem der er ansvarlig for at indberette hændelser, således at både driftsmyndigheder og aftagere har et klart overblik over deres respektive ansvar for hændelsesindberetning og -håndtering. Ansvar for, at der sker en rettidig hændelsesunderretning, påhviler altid de enkelte enheder.

For en gennemgang af den generelle regler omkring underretning om væsentlige hændelser henvises til Styrelsen for Samfundssikkerheds generelle vejledning til NIS 2-loven "*Hændelsesunderretning*".

6. TILSYN OG HÅNDHÆVELSE

Styrelsen for Samfundssikkerhed fører tilsyn med overholdelse af NIS 2-loven for offentlige forvaltningsenheder under den centrale forvaltning. Dette følger af § 1, nr. 2, i bekendtgørelse nr. 620 af 2. juni 2025 om udpegning af kompetente myndigheder og digital kommunikation omfattet af NIS 2-loven.

Offentlige forvaltningsenheder under den centrale forvaltning er per definition og uanset størrelse, jf. NIS 2-lovens § 4, stk. 3, nr. 2, omfattet som væsentlige enheder, hvilket vil sige, at der skal føres proaktivt tilsyn med disse.

Tilsynet har til formål at følge op på enhedernes efterlevelse af NIS 2-lovens bestemmelser, herunder særligt implementeringen og efterlevelsen af foranstaltninger til styring af cybersikkerhedsrisici, jf. §§ 6 og 7, samt efterlevelse af underretningspligterne, jf. §§ 12 og 13.

For de offentlige forvaltningsenheder under den centrale forvaltning, der også er omfattet af sektoren Digital infrastruktur og derfor omfattet af gennemførelsesordningen (EU) 2024/2690 (f.eks. som tillidstjenesteudbydere), føres tilsyn i henhold til de udspecificerede krav, der fremgår heraf.

Tilsynet foretages i overensstemmelse med lovens tilsyns- og kontrolforanstaltninger for væsentlige enheder, jf. NIS 2-lovens § 21, som bl.a. rummer adgang til at gennemføre kontrolbesøg, stille krav om audits, foretage sikkerhedsscanninger samt kræve at få udleveret oplysninger til vurdering af foranstaltninger og få udleveret dokumentation for gennemførelsen af cybersikkerhedspolitikken.

DET PROAKTIVE TILSYNS TILRETTELÆGGELSE

Tilsynet med NIS 2-loven tilrettelægges risikobaseret og ud fra en cyklus, hvor det sikres, at der føres tilsyn med alle omfattede væsentlige enheder inden for en fastsat årrække. Frekvensen for tilsynet med den enkelte enhed vil variere afhængigt af bl.a. enhedens kritikalitet, viden om trusler og sårbarheder, tilsyns- og hændelseshistorik. Alle enheder bliver dermed ikke underlagt lige meget tilsyn.

I 2026 og 2027 gennemføres det proaktive tilsyn to-delt, dvs. i to runder.

I første runde gennemføres et bredt surveybaseret tilsyn, der omfatter alle de offentlige forvaltningsenheder under den centrale forvaltning. Tilsynet vil

basere sig på selvevaluering fra enhedernes side. Alle enheder vil modtage en individuel tilbagemelding.

Spørgerammen i det surveybaserede tilsyn vil basere sig på Styrelsen for Samfundssikkerheds generelle vejledning til NIS 2-loven "*Implementering af cybersikkerhedsforanstaltninger*" og vil herudover også indeholde spørgsmål om opfyldelse af tekniske minimumskrav. Det bemærkes, at spørgsmål om opfyldelse af tekniske minimumskrav i det surveybaserede tilsyn vil optræde samlet i en separat sektion af hensyn til genkendelighed og for at lette enhedernes interne arbejdsprocesser.

I forhold til de offentlige forvaltningsenheder under den centrale forvaltning, som ikke tidligere har været omfattet af de tekniske minimumskrav, vil tilsynet fokusere på enhedernes arbejde med at implementere disse krav. For udvalgte af de statslige myndigheder, som tidligere har været omfattet af de tekniske minimumskrav, men som ikke er omfattet af NIS 2-loven, forventer Styrelsen for Samfundssikkerhed at stille en mulighed for frivillig rapportering til rådighed.

I anden runde udvælges en række enheder til dybdegående tilsyn centreret om mere afgrænsede temaer som f.eks. forsyningskædesikkerhed, dokumentation for efterlevelsen af udvalgte tekniske minimumskrav, driftskontinuitet eller hændeshåndtering. Udvælgelsen af, hvilke enheder der underlægges dybdegående tilsyn, vil basere sig på det surveybaserede tilsyn samt faktorer som enhedens kritikalitet, sårbarheder og hændeshistorik.

Styrelsen for Samfundssikkerheds plan for NIS 2-tilsyn offentliggøres så vidt muligt, inden årets tilsynsaktiviteter igangsættes. Ligeledes offentliggøres tilsynsspørgerammer med henblik på, at andre enheder end dem, som er omfattet af det konkrete tilsyn, kan få indsigt i kravene. Ultimo 2027 evalueres effekten af såvel de surveybaserede som de dybdegående tilsyn som led i tilrettelæggelsen af tilsynsplan for 2028.

Det bemærkes i forhold til de opfølgninger, som de statslige myndigheder tidligere har været underlagt, at tilsyn igangsættes via brev med digital post til CVR-nummeret for den enkelte offentlige forvaltningsenhed under den centrale forvaltning.

Der lægges vægt på, at tilsynet og dialogen med myndigheden er værdiskabende for myndighedens arbejde med cybersikkerhed, og det er hensigten at gennemføre tilsynet effektivt med henblik på at mindske den administrative byrde knyttet til tilsyn.

DET REAKTIVE TILSYN

Der kan føres reaktivt tilsyn på baggrund af konkrete hændelser eller andre oplysninger, der kommer til Styrelsen for Samfundssikkerheds kendskab, f.eks. via medierne. Styrelsen for Samfundssikkerhed har således mulighed for at foretage tilsyn hos en omfattet enhed når som helst og på eget initiativ.

HÅNDHÆVELSE

I forbindelse med tilsyn med de offentlige forvaltningsenheder under den centrale forvaltning kan Styrelsen for Samfundssikkerhed gøre brug af lovens håndhævelsesforanstaltninger, jf. NIS 2-lovens §§ 22 og 23, der bl.a. indeholder adgang til at udstede advarsler, bindende instrukser, påbud og forbud.

Det bemærkes, at offentlige forvaltningsenheder under den centrale forvaltning kun kan straffes med bøde for overtrædelse af NIS 2-loven og regler udstedt i medfør af loven, hvis deres aktiviteter ikke har karakter af myndighedsudøvelse. Det kan for eksempel være, hvis de leverer tjenester eller udøver virksomhed, der i øvrigt måtte være omfattet af direktivet, eksempelvis inden for sundhedssektoren eller spildevandshåndtering.

BILAG 1: SAMMENHÆNG MELLEM TEKNISKE MINIMUMSKRAV OG NIS 2-LOVENS CYBERSIKKERHEDSFORANSTALTNINGER

Nedenfor følger mapning af de tekniske minimumskrav og NIS 2-lovens cybersikkerhedsforanstaltninger. Opfyldelse af de tekniske minimumskrav bidrager til efterlevelse af NIS 2-lovens foranstaltninger, men der er ikke tale om, at efterlevelse af NIS 2-lovens foranstaltninger alene kan ske gennem opfyldelse af de tekniske minimumskrav. De angivne tekniske minimumskrav er gældende pr. 1. juli 2026. Ved senere opdateringer af tekniske minimumskrav vil nærværende bilag blive opdateret.

Klienter/PC'er: Kravene angår alle de stationære, bærbare og virtuelle klienter, som har adgang til myndighedens interne systemer:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
1	Der skal implementeres firewall på klienterne.	Formålet med kravet er at sikre myndighedens klienter mod utilsigtet netværksadgang. Klientbaserede firewalls reducerer risikoen for, at en kompromitteret klient kan bruges til at kompromittere andre klienter.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse
2	Klienter skal benytte Always On VPN fra eksterne netværk.	Formålet med kravet er at modvirke man-in-the-middle angreb og sikre, at klientens trafik er omfattet af myndighedens øvrige sikkerhedstiltag. Ved brug af Always On VPN sikres det, at al internettrafik ledes gennem myndighedens egen it-infrastruktur.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 8 Kryptografi Nr. 10 Multifaktor-autentificering og nødkommunikationssystemer
3	Fysiske klienters harddiske skal krypteres.	Formålet med kravet er at undgå kompromittering af data i forbindelse med tab eller tyveri af en klient. Fuld diskkryptering af det lokale faste lager på klienten reducerer risikoen for brud på fortroligheden af data.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 8 Kryptografi
4	Der skal implementeres endpoint-beskyttelse på klienter.	Formålet med kravet er at opdage og forhindre, at vira og malware mv. afvikles på klienten.	Nr. 5 Erhvervelse, udvikling og vedligeholdelse Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse
5	Klienters OS og applikationer på klienten skal holdes sikkerhedsopdateret.	Formålet med kravet er at lukke kendte sårbarheder på klienterne.	Nr. 5 Erhvervelse, udvikling og vedligeholdelse Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse

6	Almindelige brugerkonti må ikke tildeles administrative rettigheder til klienter.	Formålet med kravet er at reducere risikoen for installation af malware eller anden kompromittering. Da størstedelen af malware kræver administrative rettigheder på klienten for at blive installeret eller afviklet, må administrative rettigheder ikke tildeles konti, der anvendes til andre aktiviteter.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 9 Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
7	Klienter skal anvende det nyeste operativsystem.	Formålet med kravet er at sikre, at myndighedens klienter får gavn af de nyeste sikkerhedsfeatures. Da nyere operativsystemer ofte har et højere sikkerhedsniveau end ældre versioner, skal myndigheden anvende det nyeste operativsystem på de omfattede klienter.	Nr. 5 Erhvervelse, udvikling og vedligeholdelse Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse

Mail: kravene angår mailkommunikation til og fra enhederne:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
8	Der må kun anvendes godkendte mail-relays med autentifikation.	Formålet med kravet er at reducere risikoen for misbrug af mail-servere til spredning af malware og spam. Der må derfor kun anvendes mail-relays med autentifikation, som myndigheden har godkendt.	Nr. 9 Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
9	Kommunikation med mail-protokoller skal krypteres og anvende minimum TLS 1.2.	Formålet med kravet er at kryptere mailtrafikken med henblik på at sikre dataintegritet og fortrolighed. Med anvendelse af TLS 1.2 reduceres risikoen for, at mail-kommunikation bliver aflyttet undervejs i transmissionen over internettet.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 8 Kryptografi
10	Afsenders DMARC-politik skal overholdes ved modtagelse.	Formålet med kravet er at reducere antallet af forfalskede mails, der modtages af en slutbruger, ved at sikre, at afsenderdomænets eventuelle DMARC-politik overholdes.	Nr. 8 Kryptografi

Autentifikation: Kravet angår de af myndighedens it-systemer, som kan tilgås fra internettet, og hvor der logges på med myndighedens brugerkonti:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
11	Autentifikation til myndighedens systemer over internettet skal anvende flerfaktor-autentificering.	Formålet med kravet er at reducere risikoen for, at kompromitterede login-oplysninger kan anvendes af andre til at tilgå myndighedens it-systemer og data.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 10 Multifaktorautentificering og nødkommunikationssystemer

Password: Kravet angår alle myndighedens brugerkonti, herunder konti udstedt til administratorer, it-systemer og services i centrale brugerdata-baser/autentifikationstjenester:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
12	Myndigheden skal sikre, at der ikke anvendes tidligere lækede og/eller svage passwords.	Formålet med kravet er at sikre, at uvedkommende ikke nemt kan kompromittere konti, fordi der anvendes svage passwords.	Nr. 6 Effektivitet af foranstaltninger Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse

Mobile enheder: Kravene angår mobiltelefoner og tablets med app-baseret adgang til myndighedens data:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
13	Anvend numerisk adgangskode på minimum seks cifre eller biometrisk identifikation.	Kravet er opfyldt, hvis der anvendes numerisk adgangskode på minimum seks cifre eller biometrisk identifikation for at få adgang til den mobile enhed.	Nr. 6 Effektivitet af foranstaltninger Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse
14	MDM (Mobile Device Management) skal implementeres på alle mobile enheder.	Formålet med kravet er at beskytte myndighedens data på mobile enheder med særlige sikkerhedstiltag.	Nr. 5 Erhvervelse, udvikling og vedligeholdelse Nr. 6 Effektivitet af foranstaltninger Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse
15	Operativsystem og apps på mobile enheder skal holdes sikkerhedsopdateret	Formålet med kravet er at sikre, at kendte sikkerhedshuller lukkes hurtigst muligt. Regelmæssig opdatering sikrer også, at myndighedens mobile enheder får gavn af de nyeste sikkerhedsfeatures.	Nr. 5 Erhvervelse, udvikling og vedligeholdelse Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse

Logning: Kravet angår alle internetvendte tjenester og centrale interne it-systemer:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
16	Logning skal foretages på internetvendte tjenester og centrale interne it-systemer	Formålet med kravet er at sikre de bedste forudsætninger for opdagelse og efterforskning af sikkerhedshændelser. Logningen skal ikke implementeres med formål om at monitorere brugeradfærd.	Nr. 2 Håndtering af hændelser

Domænesikkerhed: Kravene angår myndighedens egne domæner og sikring i forbindelse med myndighedens navneforespørgsler:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
17	Internetvendte tjenester tilhørende myndigheden skal registreres under .dk-domæner.	Formålet med kravet er at sikre genkendelighed for borgere, myndigheder og virksomheder i Danmark, og at statslige domæner er under national kontrol via Punktum dk. Dette sikrer eksempelvis, at ondsindede .dk-domæner, der bruges til phishing, hurtigt kan nedtages.	Nr. 4 Forsyningskædesikkerhed
18	DNSSEC skal tilknyttes alle domænenavne tilhørende myndigheden.	Formålet med kravet er at sikre, at domæne-forespørgsler besvares af domæneeejeren, og at svar ikke er manipuleret undervejs. Ved brug af DNSSEC kan klienter kryptografisk stole på, at de tilgår de rette systemer og tjenester hos myndigheden.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 8 Kryptografi
19	Det skal sikres, at indgående mailgateways ligger i DNSSEC-signerede domæner.	Kravet er opfyldt, hvis alle indgående mailgateways, der håndterer mails for myndigheden, ligger i DNSSEC-signerede domæner.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 8 Kryptografi
20	Der skal anvendes DANE for alle indgående mailgateways.	Formålet med kravet er at tydeliggøre over for afsenderen, at myndigheden understøtter kryptering med henblik på at reducere risikoen for, at mails sendes ukrypteret.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 8 Kryptografi

21	Der skal foretages validering af DNSSEC-signerede svar på navneopslag.	Formålet med kravet er at forhindre, at myndighedens ansatte eksempelvis sendes videre til falske hjemme-sider. Ved at foretage DNSSEC-validering sikres det, at svar på navneopslag kommer fra domæneejeren og ikke er manipuleret undervejs.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse Nr. 8 Kryptografi
22	Myndigheden skal anvende en sikker DNS-tjeneste eller implementere anden løsning til beskyttelse mod adgang til kendte skadelige domæner.	Formålet med kravet er at beskytte enheder på netværket mod at tilgå eksempelvis kendte phishing-sider og hjemme-sider med malware. Ved brug af en sikker DNS-tjeneste filtreres navne-forespørgsler på baggrund af automatisk opdaterede lister over domæner, der vurderes at være skadelige.	Nr. 5 Erhvervelse, udvikling og vedligeholdelse
23	DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden.	Formålet med kravet er at give mailmodtagere mulighed for at opdage forsøg på email-spoofing, hvor en afsender udgiver sig for at være en anden. Ved at implementere DMARC på alle domæner reduceres risikoen for, at myndighedens domænenavne kan misbruges til udsendelse af phishing- eller spam-mails.	Nr. 8 Kryptografi

Netværk: Kravene angår myndighedens trådede og trådløse netværk:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
24	Myndighedens WiFi-netværk skal være krypteret med minimum WPA2	Formålet med kravet er at forhindre misbrug og aflytning af trafikken på myndighedens WiFi-netværk.	Nr. 8 Kryptografi
25	Gæstenetværk skal holdes adskilt fra myndighedens interne netværk	Formålet med kravet er at sikre, at trafik fra gæstenetværket ikke omgår eksisterende sikringstiltag, og at eventuel uønsket internettrafik fra gæstenetværket ikke påvirker myndighedens omdømme.	Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse

Internetvendte tjenester: Kravene angår de af myndighedens it-systemer, som kan tilgås fra internettet:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
26	Software på myndighedens internetvendte tjenester skal holdes sikkerhedsopdateret.	Formålet med kravet er, at kendte sårbarheder, der kan udnyttes over eller fra internettet, bliver lukket hurtigst muligt. Derfor skal al software, der anvendes på myndighedens internetvendte tjenester, være omfattet af aktiv support og regelmæssige sikkerhedsopdateringer.	Nr. 5 Erhvervelse, udvikling og vedligeholdelse Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse
27	Adgang til myndighedens internetvendte tjenester skal ske over en krypteret forbindelse.	Formålet med kravet er at sikre dataintegritet og fortrolighed samt forebyggelse af man-in-the-middle angreb.	Nr. 6 Effektivitet af foranstaltninger Nr. 8 Kryptografi
28	Internettilgængelige IP-adresser, som myndigheden har brugsret over, skal scannes for tjenester.	Formålet med kravet er at sikre, at kun det nødvendige og forventede er tilgængeligt over internettet.	Nr. 6 Effektivitet af foranstaltninger Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse

Interne it-systemer: Kravet angår specifikke interne infrastruktur-enheder og tjenester:

Nr.	Krav	Beskrivelse	NIS 2-lovens § 6, stk. 1
29	Software på specifikke interne infrastruktur-enheder og -tjenester skal holdes sikkerhedsopdateret.	Formålet med kravet er, at kendte sårbarheder bliver lukket hurtigst muligt. Derfor skal software, der anvendes på omfattede infrastruktur-enheder og -tjenester være omfattet af regelmæssig sikkerhedsopdatering.	Nr. 5 Erhvervelse, udvikling og vedligeholdelse Nr. 7 Cyberhygiejne og cybersikkerhedsuddannelse