NIS 2-direktivet

Foranstaltninger til sikring af et højt cybersikkerhedsniveau

Den 20. februar 2025

MOLT | WENGEL

Agenda

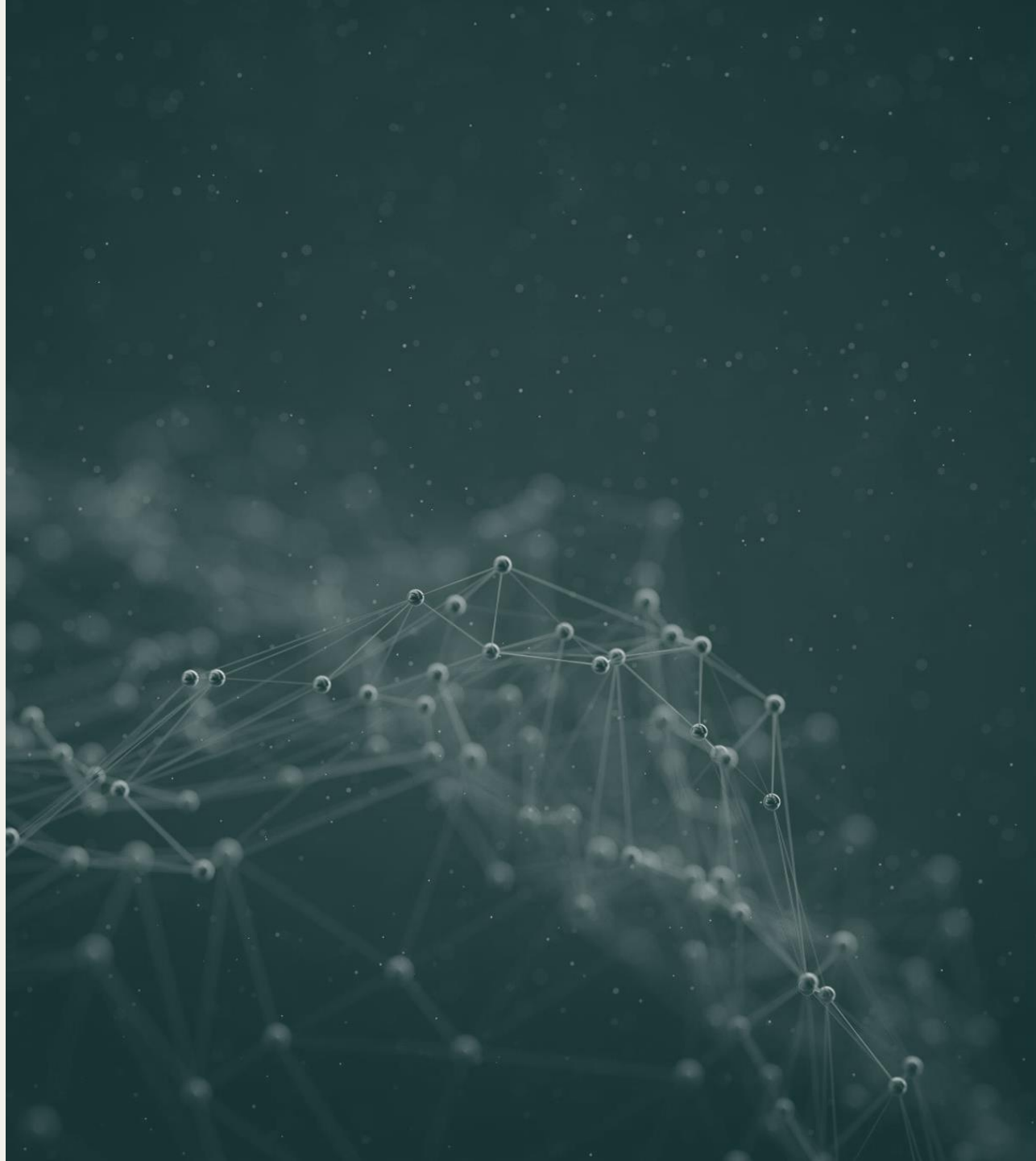
01 Tidslinje & anvendelsesområde

02 Væsentlig eller vigtig enhed

03 Forpligtelser

04 Tilsyn og håndhævelse

05 NIS 2 i byggeriet og eksempler



Hvem er jeg?

Kathrine Ahrenholt er specialiseret i udbudsret og særligt i IT-udbud. Kathrine rådgiver både offentlige myndigheder og private IT-leverandører om udbud, herunder udarbejdelse af tilbud, strategi i forbindelse med tilrettelæggelse og gennemførelse af IT-udbud samt kontraktforhandlinger.

Kathrine har stor erfaring med at udarbejde strategi for gennemførelse af udbud, kvalitetssikring af udbudsmateriale samt bistand med forberedelse og deltagelse i kontraktforhandlinger.

Derudover har Kathrine stor erfaring med at føre sager ved Klagenævnet for Udbud og tilhørende processtrategisk rådgivning. Kathrine underviser eller optræder som indlægsholder på forskellige kurser og konferencer om udbuds- og IT-regler.

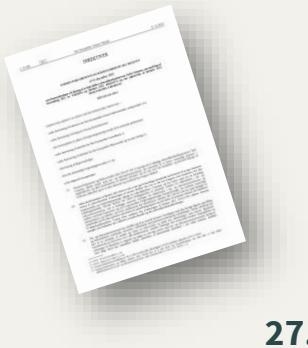
Kathrine Ahrenholt
Advokat. Procurement & Technology Lead
Molt Wengel
Tlf: 5180 8078
ka@mowe.dk

MOLT | WENGEL

Tidslinje

For implementering af NIS 2

MOLT | WENGEL



6. juli 2016
NIS 1 direktivet vedtaget i EU

27. december 2022
NIS 2 direktivet vedtaget i EU

5. juli 2024
Lovforslag sendt i høring

17. oktober 2024
Gennemførelsesforordning vedtaget vedr. foranstaltninger til styring af cybersikkerhedsrisici og væsentlige hændelser

6. februar 2025
Lovforslag fremsat i DK:
1) NIS 2 - Cybersikkerhed
2) Kritiske enheders modstandsdygtighed
3) Sikkerhed og beredskab i telesektoren

1. juli 2025
Forventet ikrafttræden i DK

Oktober 2025
Seneste NIS 2 ikrafttræden i DK
(oprindeligt i oktober 2024, og traktatbrudssag mod Danmark blev indledt den 28. november 2024)

Lovens formål

MOLT | WENGEL

Styrkelse af cybersikkerhed og risikostyring

Direktivet skærper kravene til virksomheder og organisationer inden for kritiske sektorer for at sikre, at de har passende cyber-sikkerhedsforanstaltninger og risikostyring på plads.

Udvidelse af dækningsområdet

NIS 2 udvider listen over sektorer og enheder ift. NIS 1, der er omfattet af reglerne, så flere virksomheder, der leverer essentielle og vigtige tjenester (f.eks. energi, transport, sundhed og digitale tjenester), nu skal leve op til sikkerhedskravene.

Forbedre samarbejde og rapporteringspligt

Direktivet skal styrke samarbejdet mellem EU og etablere en fælles ramme for informationsdeling om cybertrusler og hændelser. Det skærper også kravene til rapporte-ring af sikkerhedshændelser, så myndigheder kan reagere på trusler.

Kort sagt har NIS 2 til formål:

- at **øge** den generelle cybersikkerhed i EU,
- gøre flere organisationer **ansvarlige** for at beskytte deres systemer, og
- **forbedre** det internationale samarbejde mod cyberangreb.

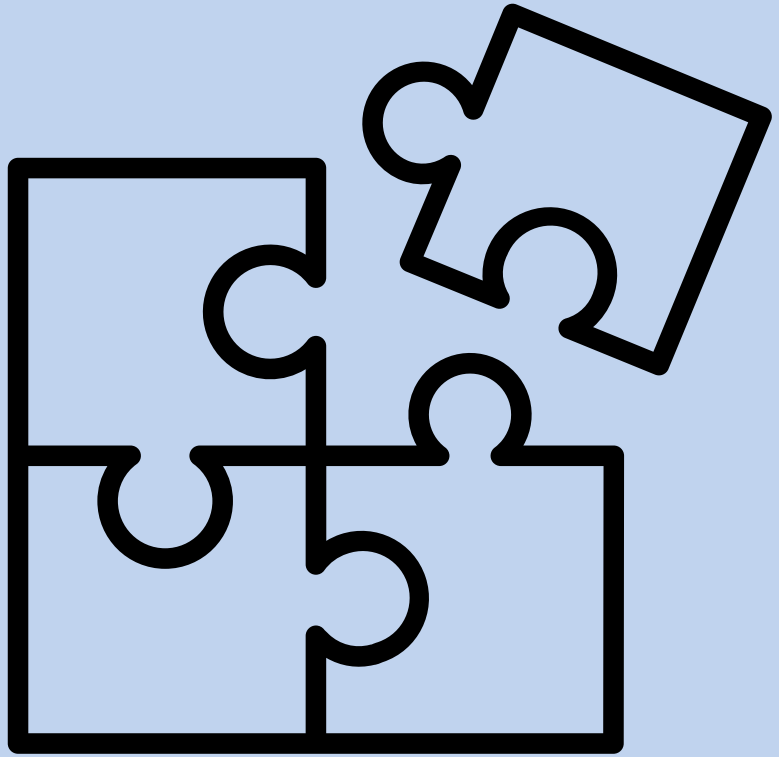
MOLT | WENGEL

Anvendelsesområde

Anvendelsesområde

- Loven finder anvendelse på **offentlige og private enheder**, der er omfattet af sektorerne der er oplistet lovens **bilag 1 og bilag 2**, jf. § 1, stk. 1
  - Dog ikke på enheder, der er omfattet af:
    - Lov om styrket beredskab i energisektoren
    - Lov om sikkerhed og beredskab i telesektoren
    - Lov om finansiel virksomhed

- I udgangspunktet udgør sektorerne brancher, som i større eller mindre grad er **kritiske for samfundets drift**



Bilag 1 – Sektorer

	Sektor		
	Transport		Digital infrastruktur
	Energi		Forvaltning af IKT-tjenester
	Drikke- og spildevand		Statslig og regional forvaltning
	Sundhed		Rummet
	Bankvirksomhed og finansielle markedsinfrastruktur		

Energisektoren

MOLT | WENGEL

Sektor	Delsektor	Type sektor
Energi	**Elektricitet**	Elektricitetsvirksomheder
		Distributionssystemoperatører
		Transmissionssystemoperatører
		Udpegede elektricitetsmarkedsoperatører,
		Markedsdeltagere, der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring Operatører af ladestationer
	Fjernvarme	Operatører af fjernvarme eller fjernkøling
	Olie	Olierørledningsoperatører
		Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission
		Centrale lagerenheder
	Gas	Forsyningsvirksomheder
		Distributionssystemoperatører
		Transmissionssystemoperatører
		Lagersystemoperatører
		LNG-systemoperatører
		Naturgasvirksomheder
		Operatører af naturgasraffinaderier og -behandlingsanlæg
	Brint	Operatører inden for brintproduktion, - lagring og -transmission

Bilag 2 – Sektorer

	Sektor		
	Post- og kurertjenester		Affaldshåndtering
	Kemikalier		Fødevarevirksomheder
	Digitale serviceudbydere		Forskning
	Produktionsvirksomheder af særlig vigtigt udstyr		

Kommunerne

MOLT | WENGEL

Er kommunerne omfattet af loven?

- Kommunerne er omfattet af loven i det omfang, de udfører opgaver i en af sektorerne i bilag 1 eller 2
  - I udgangspunktet omfattet af **sundhedssektoren** i bilag 1:
    - *"en fysisk eller juridisk person eller anden enhed, der lovligt leverer sundhedsydelser på en medlemsstats område"*

- Ministeren kan herudover fastsætte regler om, at loven finder anvendelse for **kommunerne** og uddannelsesinstitutioner, jf. § 1, stk. 6
  - Uddannelsesinstitutionerne er ikke omfattet af forskningssektoren, men forventes at blive særskilt nævnt

Forventning:

- Bestemmelsen efter § 1, stk. 6, er pt. **ikke udnyttet** i lovforslaget

- Ministeriet for Samfundssikkerhed og Beredskab er i dialog med KL og relevante myndigheder om, hvorvidt bestemmelsen i § 1, stk. 6, skal udnyttes

- Det forventes, at Ministeriet for Samfundssikkerhed og Beredskab udnytter § 1, stk. 6, til direkte at nævne/opliste **kommunerne** og universiteterne, der beskæftiger sig med forskning

Kommunerne

Ministeriet for Samfundssikkerhed og Beredskab blev stillet følgende spørgsmål inden lovforslaget blev fremsat:

- *"Kan ministeren redegøre for, hvorfor muligheden i EU-direktivet for at omfatte kommuner som lokale eller regionale myndigheder **ikke er blevet udnyttet** i lovforslaget for NIS2, fremlagt den 5. juli 2024?"*

Ministeriet svarede blandt andet følgende:

- *"[…]* kunne blive omfattet af lovens anvendelsesområde, selvom bemyndigelsen i den foreslåede § 1, stk. 7, ikke var udnyttet. Dette ville eksempelvis kunne være tilfældet i en situation, hvor en **kommune agerer som sundhedstjenesteyder** i overensstemmelse med NIS 2-direktivets bilag. I denne **situation ville kommunen kunne være omfattet af lovens anvendelsesområde på baggrund af disse aktiviteter.**
- *[…] det til at fremgå af udkastet til NIS 2-lovforslag, som forventes fremsat den 6. februar 2025, at **kommunerne** – på lige fod med andre enheder, der er omfattet af lovens anvendelsesområde – **ikke alene vil skulle træffe passende og forholdsmæssige foranstaltninger** for at styre risiciene for sikkerheden i net- og informationssystemer vedrørende de aktiviteter, der er oplistet i direktivets bilag, **men for samtlige af de net- og informationssystemer, som de anvender til deres operationer, eller til at levere deres tjenester."***

MOLT | WENGEL

Efter lovforslaget af 6. februar, er §1, stk. 7 ændret til § 1, stk. 6

MOLT | WENGEL

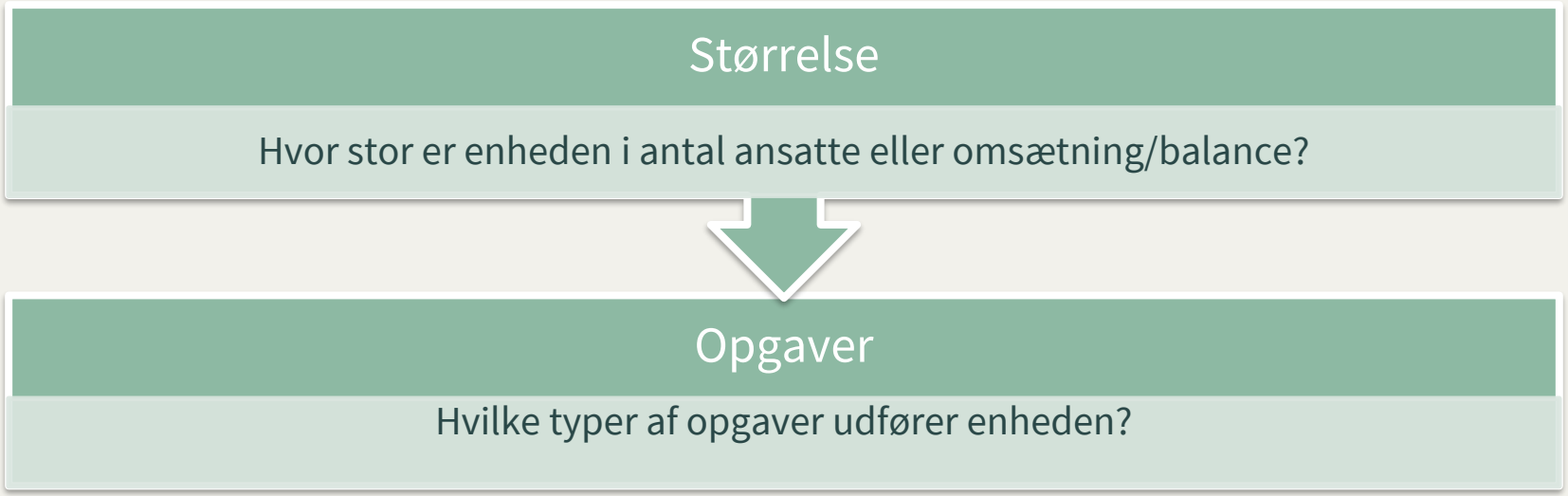
Væsentlig eller vigtig enhed

Væsentlig eller vigtig enhed

Der sondres mellem væsentlige enheder (§ 4) og vigtige enheder (§ 5) i lovforslaget

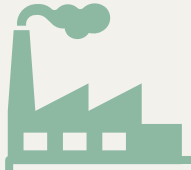
- Sondringen har betydning for **tilsynet** og **håndhævelsen** af de forpligtelser, der pålægges enheden
  - Væsentlige enheder pålægges flere forpligtelser, idet de udfører opgaver i sektorer, der er mere kritiske

- Afhænger af enhedens opgaver og størrelse



Enhedens størrelse

- Det skal først og fremmest fastslås, hvilken størrelse enheden har
- Enhedernes størrelse defineres enten ud fra antallet af deres ansatte (årsværk) eller ud fra den årlige omsætning/balancepost, jf. 2003/361/EF
  - Kun den ene betingelse skal være opfyldt

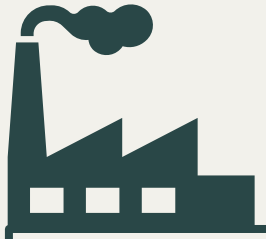


Vigtig enhed § 5, stk. 1

Mere end 50 ansatte

eller

Årlig omsætning på over 10 mio. EUR **og** en årlig samlet balance på over 10 mio. EUR



Væsentlig enhed § 4, stk. 1

Mere end 250 ansatte

eller

Årlig omsætning på over 50 mio. EUR **og** en årlig samlet balance på over 43 mio. EUR

Enhedens opgaver

	Sektor		
	Transport		Digital infrastruktur
	Energi		Forvaltning af IKT-tjenester
	Drikke- og spildevand		Statslig og regional forvaltning
	Sundhed		Rummet
	Bankvirksomhed og finansielle markedsinfrastruktur		

Væsentlig enhed efter lovforslagets § 4

- Lovforslaget oplister en række tilfælde, hvormed en virksomhed udgør en ***væsentlig enhed***. Bl.a. vil følgende enheder være væsentlige enheder:
  - Enhed, der er omfattet af bilag 1 og har enten mere end 250 ansatte **eller** en årlig omsætning på over 50 mio. EUR og en årlig samlet balance på over 43 mio. EUR, jf. stk. 1
  - Kommune eller region, der med **kommercielt formål** udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester og er en mellemstor virksomhed, jf. stk. 2
  - Uanset deres størrelse anses følgende enheder for at være væsentlige enheder, jf. stk. 3, nr. 1 - 5 (eksempler):
    - Staten og statslige organer, jf. stk. 3, nr. 2
    - Enhed, der er defineret som kritisk enhed i henhold til lov om kritiske enheders modstandsdygtighed, jf. stk. 3, nr. 3
    - Enhed, der er omfattet af bilag 1 eller 2, og:
      - hvor enheden er eneste udbyder af tjenesten i Danmark, som er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, jf. stk. 3, nr. 5, litra a, eller
      - hvor forstyrrelse af den tjeneste, som enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden, jf. stk. 3, nr. 5, litra b

Enhedens opgaver

	Sektor		
	Post- og kurertjenester		Affaldshåndtering
	Kemikalier		Fødevarevirksomheder
	Digitale serviceudbydere		Forskning
	Produktionsvirksomheder af særlig vigtigt udstyr		

Vigtig enhed efter lovforslagets § 5

- Lovforslaget anfører, at følgende enheder vil udgøre en ***vigtig enhed***:
  - Enhed, der er omfattet af bilag 1 eller 2,
    - men som ikke opfylder kriterierne for at være en væsentlig enhed efter § 4,
    - og som har mere end 50 ansatte **eller** en årlig omsætning på over 10 mio. EUR og en årlig samlet balance på over 10 mio. EUR
  - Den kompetente myndighed kan træffe afgørelse om, at en enhed uanset størrelse, er en vigtig enhed.
    - Det betyder, at **mikro- og små virksomheder** (< 50 ansatte eller 10 mio. EUR i omsætning/balancepost), som udfører opgaver i sektorerne oplistet i bilag 1 eller 2, men som ikke er nævnt særskilt i § 4, i udgangspunktet ikke er omfattet af loven

Enhedens opgaver

	Sektor		
	Transport		Digital infrastruktur
	Energi		Forvaltning af IKT-tjenester
	Drikke- og spildevand		Statslig og regional forvaltning
	Sundhed		Rummet
	Bankvirksomhed og finansielle markedsinfrastruktur		
	Post- og kurertjenester		Affaldshåndtering
	Kemikalier		Fødevarevirksomheder
	Digitale serviceudbydere		Forskning
	Produktionsvirksomheder af særlig vigtigt udstyr		

Enheder, der er omfattet af både bilag 1 og bilag 2, flere sektorer og love

- Opfylder en enhed både betingelserne for at være en væsentlig og vigtig enhed, eksempelvis fordi enheden både opererer i bilag 1 og 2, udgør enheden en **væsentlig enhed** (§ 4)
- NIS 2 finder ikke anvendelse i det omfang, enheden er:
  - Underlagt lov om styrket beredskab i energisektoren
  - Underlagt lov om sikkerhed og beredskab i telesektoren
  - Underlagt lov om finansiel virksomhed
    - → medmindre enheden er en **kommune** eller **region**, som med **kommercielt formål** stiller offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester til rådighed, og enheden enten har mere end 50 ansatte, eller mere end 50 ansatte **eller** en årlig omsætning på over 10 mio. EUR og en årlig samlet balance på over 10 mio. EUR .
  - Underlagt lov om finansiel virksomhed

MOLT | WENGEL

Forpligtelser

§ 6 **Væsentlige og vigtige enheder** skal **træffe passende** og forholdsmæssige **tekniske, operationelle og organisatoriske** foranstaltninger for at styre **risiciene** for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at **forhindre** hændelser eller **minimere** deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Foranstaltninger

MOLT | WENGEL

Foranstaltningerne skal <u>minimum</u> omfatte:

1) Politikker for risikoanalyse og informationssystemsikkerhed
   - Enheden skal udarbejde en politik, hvor den overordnede ramme for implementering af foranstaltningerne fastlægges
   - Metoder til at identificere og adressere evt. risici
2) Håndtering af hændelser
   - Procedure for håndtering af hændelser
   - Implementere logning og monitering af uregelmæssigheder i enhedens net- og informationssystemer. Logdata skal beskyttes mod uautoriseret adgang
3) Driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring
   - Procedure for backupstyring og gendannelse af data
   - Beredskabsplan for krisestyring og reetablering efter katastrofer
   - Etablere redundans, nødstrømsforsyning, understøttende forsyning mv.
4) Forsyningskædesikkerhed, sikkerhedsrelaterede aspekter
   - Procedure for leverandørstyring og sikre passende forsyningskæder
   - Sikre kontraktregulering af leverandører (og evt. andet led)

Foranstaltninger fortsat

MOLT | WENGEL

5) Sikkerhed ved erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

- Procedure for erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer
- Procedure for håndtering af offentliggørelse af sårbarheder

6) Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

- Procedure for tekniske test for sårbarheder

7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

- Procedure for cyberhygiejnepraksisser (brug af passwords og sikker e-mails)
- Procedure for uddannelse af medarbejdere til håndtering af IT-sikkerhed

8) Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

- Procedure for brug af kryptografi og evt. kryptering

9) Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

- Politik for adgangskontrol og adgangsrettigheder til IT-systemer
- Foranstaltninger vedrørende informationssikkerhed – ”*sikre at den enkelte medarbejder forstår, udviser og forpligter sig til at leve op til deres ansvar til informationssikkerhed*”
- Fastlægge hvordan enheden vil forvalte aktiver, der vil kunne påvirke sikkerheden i enhedens net- og informationssystemer

10) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant

- Foranstaltninger vedrørende multifaktorautentificering eller kontinuerlig autentificering
- Anvende sikret tale-, video- og tekstkommunikation (også i nødsituationer)

Foranstaltninger

MOLT WENGEL

Bemyndigelse

§ 6, stk. 3. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab **fastsætte nærmere regler** om foranstaltninger efter stk. 1.

Sektorspecifikke hensyn

Bemærkningerne: *"De ansvarlige ressortministre bør bemyndiges til at konkretisere lovens generelle krav om foranstaltninger, såfremt **særlige sektorspecifikke** hensyn tilsiger dette. "*

Dynamisk formål

*"En sådan konkretisering bør ske i bekendtgørelsesform med henblik på at sikre, at der **løbende og smidigt kan ske en tilpasning** af kravene i takt med den teknologiske udvikling og udviklingen i trusselsbilledet."*

Foranstaltninger fortsat

MOLT | WENGEL

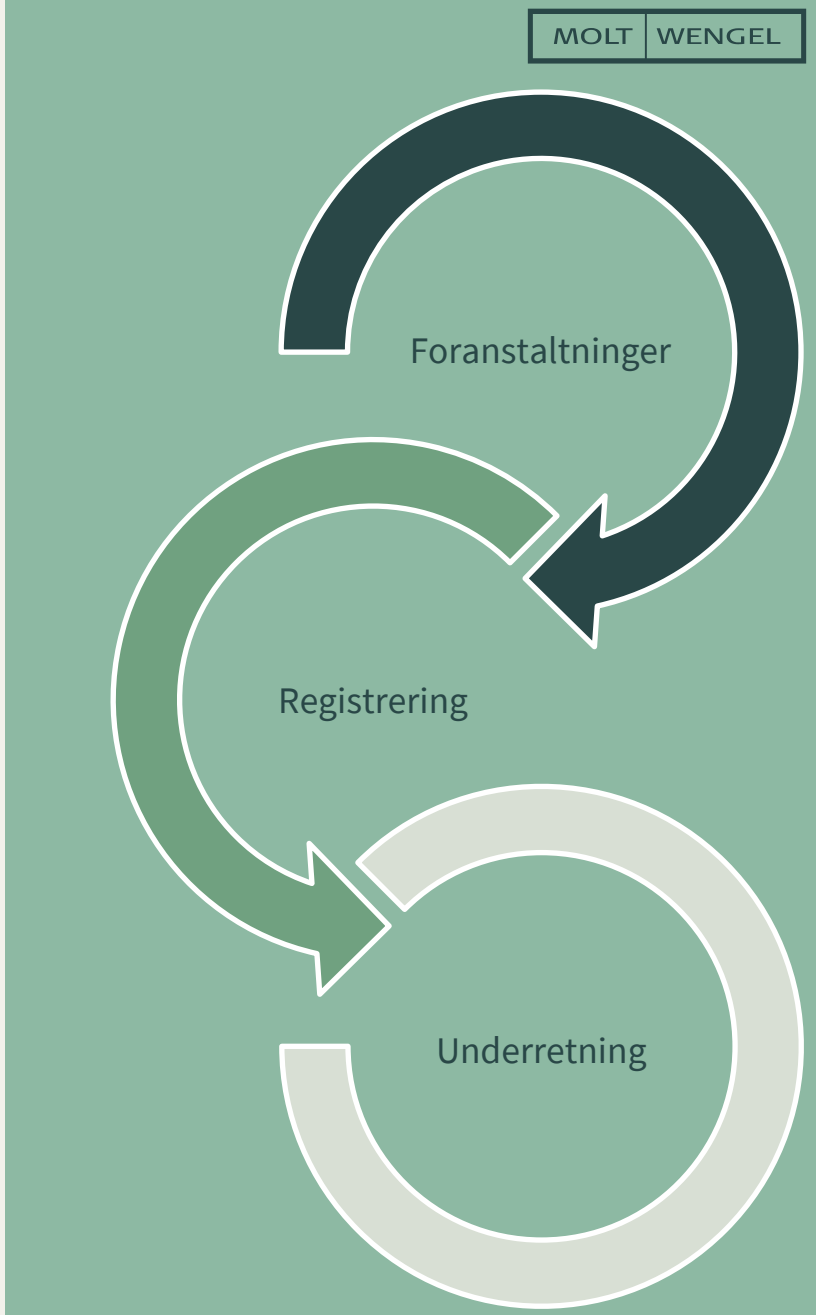
Ledelsen har følgende opgaver:

§ 7. De foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af § 6, stk. 1 og 2, samt regler fastsat i medfør af § 6, stk. 3, skal være ***godkendt*** *af* ***enhedens ledelsesorgan****. Ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse.*

Stk. 2. Medlemmerne af en væsentlig eller vigtig enheds ***ledelsesorgan skal deltage i relevante kurser om styring af cybersikkerhedsrisici*** *og tilskynde til at tilsvarende kurser tilbydes til enheden øvrige ansatte.*

Forpligtelser

- Rapporteringsforpligtelser, *registrering og underretning,* skal ske til den nationale CSIRT (Computer Security Incident Response Team)
  - I Danmark fungerer Styrelsen for Samfundssikkerhed *(tidligere Center for Cybersikkerhed)* som national CSIRT
- Det forventes, at enhederne skal rapportere via virk.dk



§ 10 **Væsentlige og vigtige enheder** samt enheder, der leverer domænenavns-registreringstjenester, skal **registrere** sig hos den relevante kompetente myndighed

Registrering

MOLT | WENGEL

- Der skal oplyses følgende oplysninger:
  - Enhedens navn
  - Adresse og ajourførte kontaktoplysninger, herunder emailadresser, IP-intervaller og telefonnumre.
  - Den relevante sektor og delsektor, som enheden er omfattet af, jf. loven bilag 1 eller 2
  - En liste over de øvrige medlemsstater i Den Europæiske Union, hvor enheden leverer tjenester (dog ikke Grønland og Færøerne)

- Oplysningerne skal være indsendt senest to uger efter enheden omfattes af loven
  - Dog tidligst 1. oktober 2025, jf. § 33, stk. 3
- Ændringer i oplysningerne skal ligeledes indsendes inden to uger efter ændringen.

§12 **Væsentlige og vigtige enheder** skal **underrette** den relevante kompetente myndighed og Computer Security Incident Response Team (CSIRT) om enhver **væsentlig hændelse**. En underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Underretning til CSIRT

MOLT | WENGEL

- En hændelse anses for at være **væsentlig**, hvis:
  - Hændelsen har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller
  - Hændelsen har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke-fysisk skade
- Når en enhed har **underrettet** om en væsentlig hændelse, sikrer CSIRT uden unødigt ophold og inden 24 timer efter modtagelsen, at der gives et svar og indledende tilbagemeldinger
  - Enheden kan i samme ombæring anmode CSIRT om at **yde vejledning, operativ rådgivning** om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand
- Offentlige og private enheder, der ikke er omfattet af loven, kan på samme vis underrette om hændelser
  - Sådanne underretninger vil være undtaget fra aktindsigt

Underretning til CSIRT

MOLT | WENGEL

Bemyndigelse

§ 12, stk. 3. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab **fastsætte nærmere regler** om, hvornår en hændelse kan anses for at være væsentlig.

Sektorspecifikke hensyn

Bemærkningerne: *" Henset til kriteriernes generelle udformning finder Ministeriet for Samfundssikkerhed det hensigtsmæssigt, at der gives mulighed for, at der **sektorvist kan fastsættes nærmere regler** om, hvornår en hændelse anses for at være væsentlig.*

Ved fastsættelsen af regler

*"Det forudsættes, at de kompetente myndigheder i relevant omfang vil være særligt opmærksomme på at **yde vejledning** til enheder, der omfattes af særlige sektorspecifikke krav om væsentlige hændelser."*

Underretning til CSIRT

Underretninger om væsentlige hændelser skal ske inden for følgende frister:

Tidlig varsling
Angivelse af om hændelsen mistænkes at være forårsaget af ulovlige eller ondsindede handlinger eller grænseoverskridende virkning

Hændelsesunderretning
Ajourføring af tidlige varsling med indledende vurdering af dens alvor og indvirkning samt kompromitteringsindikatorerne

Foreløbig rapport
Rapport med relevante statusopdateringer

Endelig rapport
Detaljeret beskrivelse af hændelsens alvor, indvirkning, truslen, årsag og grænseoverskridende virkninger

Pågår hændelsen stadig en måned efter? Endelig rapport en måned efter hændelsen er håndteret.

Underretninger til modtagere

MOLT | WENGEL

Udover underretning til CSIRT skal modtagerne også underrettes (§15)

- Væsentlige og vigtige enheder skal uden unødigt ophold underrette **modtagerne af tjenesterne**, såfremt hændelserne **sandsynligvis vil påvirke leveringen af modtagernes tjenester negativt**
- Endvidere skal væsentlige og vigtige enheder uden unødigt ophold **oplyse modtagerne**, som potentielt er berørt af en væsentlig cybertrussel, om **eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion herpå**
  - Samt hvor relevant, **informere** om den væsentlige cybertrussel

MOLT | WENGEL

Tilsyn og håndhævelse

Tilsyn

- Ministeriet for Samfundssikkerhed og Beredskab fører tilsyn med enhedernes overholdelse af loven.
  - Væsentlige enheder: Rutine kontroller
  - Vigtige enheder: Kun ved indikationer på manglende overholdelse
- Der anvendes følgende tilsynsforanstaltninger:
  - **Kontrol på stedet** og eksternt tilsyn (samt stikprøvekontroller) – uden retskendelse
  - **Sikkerhedsaudits** (systematisk gennemgang), herunder regelmæssige og målrettede sikkerhedsaudits, eller stille krav om et uafhængigt organ skal foretage disse audits
  - **Sikkerhedsscanninger** (automatisk teknisk analyse af it-systemer)
  - Kræve **udlevering** af nødvendige **oplysninger** vedrørende foranstaltningerne
  - Kræve **adgang** til **data, dokumenter og oplysningerne**, der er nødvendige for udførslen af tilsynsopgaven
  - Kræve udlevering af **dokumentation** for gennemførelsen af cybersikkerhedspolitikker

Når ministeriet kræver udlevering eller adgang til oplysninger mm., skal de angives et **formål** hermed, samt en **præcisering** af hvilke oplysninger, der ønskes, og i hvilket **format**.

Håndhævelse

- Ministeriet for Samfundssikkerhed og Beredskab kan anvende følgende håndhævelsesforanstaltninger over for **væsentlige** enheder:
  - Påbud om at træffe foranstaltninger, der forhindrer eller afhjælper
  - Udpege en person med ansvar for i en periode at føre tilsyn med enhedens overholdelse af foranstaltningerne og underretningerne
- Herudover kan ministeriet anvende følgende håndhævelsesforanstaltninger over for både **væsentlige** og **vigtige** enheder:
  - Udstede advarsler
  - Udstede bindende instrukser vedrørende for forhindre eller afhjælpe hændelser, herunder frister for gennemførelse og rapportering herom samt pålæg om afhjælpning
  - Meddele påbud og forbud for sikre overholdelse af loven
  - Påbyde enheden at underrette fysiske eller juridiske personer, til hvilke enheden leverer tjenester eller udfører aktiviteter, hvis de er berørte
  - Påbyde gennemførelse af anbefalinger en sikkerhedsaudit har medført
  - Påbyde enheden i ikke anonymiseret form at offentliggøre påbudte håndhævelsesforanstaltninger, domme eller bøder

MOLT | WENGEL

Ministeriet vil altid fortage en **høring** af enheden forinden håndhævelsesforanstaltninger anvendes (§16 og §26)

Bøder

- Enheder straffes med bøde, såfremt de:
  - Overtræder deres forpligtelser til varetage sine foranstaltninger, registreringer eller underretninger,
  - Undlader at efterkomme forbud, påbud eller afgørelser, eller
  - Hindrer myndighederne i at føre tilsyn

- For manglende varetagelse af foranstaltninger eller manglende indsendelse af underretninger idømmes op mod følgende bødestørrelser:
  - Væsentlige enheder: Maksimalt 10.000.000 euro eller 2 % af enhedens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvad der er højest.
  - Vigtige enheder: Maksimalt 7.000.000 euro eller 1,4 % af enhedens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvad der er højest.

MOLT | WENGEL

Idømmelse af bøder:

- Bøderne kan ikke pålægges administrativt
- Bøder udstedes og udmåles i det almindelige straffeprocessuelle system

MOLT | WENGEL

NIS 2 i byggeriet

ITK og NIS 2

MOLT | WENGEL

	Sektor		
	Transport		Digital infrastruktur
	Energi		Forvaltning af IKT-tjenester
	Drikke- og spildevand		Statslig og regional forvaltning
	Sundhed		Rummet
	Bankvirksomhed og finansielle markedsinfrastruktur		
	Post- og kurertjenester		Affaldshåndtering
	Kemikalier		Fødevarevirksomheder
	Digitale serviceudbydere		Forskning
	Produktionsvirksomheder af særlig vigtigt udstyr		

Entreprenører og underleverandører kan ***indirekte*** falde under lovens anvendelsesområde, såfremt de leverer ydelser til kritiske bygninger eller infrastrukturer, idet **enhederne skal sikre forsyningskædesikkerheden**, eksempelvis:

- **Entreprenører**, der opfører kritiske bygninger til brug for offentlig forvaltning,
- **Teknologileverandører til byggeriet**, der udvikler software til kritisk infrastruktur, og
- **Rådgivere og ingeniører**, der designer eller rådgiver om digitalt byggeri til brug for offentlig forvaltning

- ITK-bekendtgørelsen i offentligt byggeri fastlægger krav til anvendelse af digitale løsninger i byggeriet
  - ITK-bekendtgørelsen skal derfor spille sammen med NIS 2

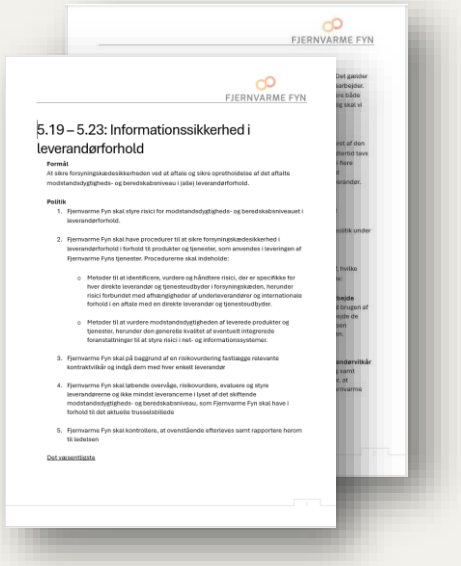
- Enhederne skal udarbejde procedurer for deres leverandørstyring samt undersøge eventuelle sårbarheder i forbindelse hermed
  - På denne vis omfattes leverandører af bygge- eller rådgivningsydelser til sektorerne af NIS 2. Det kan eksempelvis være
    - Statslige og regionale bygninger og andre bygninger, der håndterer kritisk infrastruktur (kemi- og fødevarevirksomheder (engros og industriel))

- Med NIS 2 loven skal aktører i byggeriet, sikre, at:
  - deres IT-systemer overholder forpligtelserne, således de lever op til kundernes politikker, og
  - tænke cybersikkerhed ind i designet af deres digitale løsninger

Eksempler på foranstaltninger

MOLT | WENGEL

Foranstaltning nr. 1 (Politik)


FJERNVARME FYN

FJERNVARME FYN

5.19 – 5.23: Informationssikkerhed i leverandørforhold

Formål

At sikre forsyningskædesikkerheden ved at aftale og sikre opretholdelse af det aftalte modstandsdygtigheds- og beredskabsniveau i (alle) leverandørforhold.

Politik

1. Fjernvarme Fyn skal styre risici for modstandsdygtigheds- og beredskabsniveauet i leverandørforhold.
2. Fjernvarme Fyn skal have procedurer til at sikre forsyningskædesikkerhed i leverandørforhold i forhold til produkter og tjenester, som anvendes i leveringen af Fjernvarme Fyns tjenester. Procedurerne skal indeholde:
   - Metoder til at identificere, vurdere og håndtere risici, der er specifikke for hver direkte leverandør og tjenesteudbyder i forsyningskæden, herunder risici forbundet med afhængigheder af underleverandører og internationale forhold i en aftale med en direkte leverandør og tjenesteudbyder.
   - Metoder til at vurdere modstandsdygtigheden af leverede produkter og tjenester, herunder den generelle kvalitet af eventuelt integrerede foranstaltninger til at styre risici i net- og informationssystemer.
3. Fjernvarme Fyn skal på baggrund af en risikovurdering fastlægge relevante kontraktvilkår og indgå dem med hver enkelt leverandør
4. Fjernvarme Fyn skal løbende overvåge, risikovurdere, evaluere og styre leverandørerne og ikke mindst leverancerne i lyset af det skiftende modstandsdygtigheds- og beredskabsniveau, som Fjernvarme Fyn skal have i forhold til det aktuelle trusselsbillede
5. Fjernvarme Fyn skal kontrollere, at ovenstående efterleves samt rapportere herom til ledelsen

Det væsentligste

Foranstaltning nr. 3 (Back-up)

Kravkategori:	K	Opfyldt:	
Kundens krav:	**Krav-id 10-3 Sikkerhedskopiering** Det er et Krav, at Løsningen og dens data sikkerhedskopieres af Leverandøren, således at seneste kopi altid dækker mindst indtil foregående Arbejdsdag. Herudover er det et krav, at Løsningen, giver mulighed for restore af enkeltelementer eller af hele Løsningen. *Leverandøren bedes beskrive det tilbudte.*		
Leverandørens svar:	*[Indsæt besvarelse her, eller umiddelbart under kravboksen]*		

Eksempler på foranstaltninger

MOLT | WENGEL

Foranstaltning nr. 4 (Forsyningskædesikkerhed)

- Fra SKI 02.22 IT Drift, bilag 14 - Sikkerhed

Punkt 2.2 Leverandørens efterlevelse af kundens sikkerhedskrav

"Leverandøren skal efterleve Kundens interne politikker og it-sikkerhedsregler. Hvis Leverandøren på enkelte områder ikke kan efterleve Kundens interne politikker og it-sikkerhedsregler, skal Leverandøren kunne påvise, at Leverandøren efterlever alternative politikker, der er egnede til at tilvejebringe et tilsvarende sikkerhedsniveau."

Foranstaltning nr. 6 (Procedure for måling af effektiviteten)

- Fra SKI 02.22 IT Drift, bilag 14 - Sikkerhed

Punkt 2.1 Risikostyring

"Leverandørens risikostyring af informationssikkerheden i forhold til Leverandørens opfyldelse af Leveringskontrakten skal baseres på en dokumenteret og regelmæssigt opdateret risikovurdering.

Risikovurderingen skal omfatte de Ydelser og de dele af Leverandørens virksomhed, som kan have konsekvenser for informationssikkerheden i Systemerne. Leverandøren skal herunder inddrage alle relevante forhold og Kundens egne erfaringer fra øvelser og hændelser samt eventuelle trusselsvurderinger fra Center for Cybersikkerhed, såfremt disse eksisterer."

Eksempler på foranstaltninger

MOLT | WENGEL

Foranstaltning nr. 8 (Kryptografi)

- Fra SKI 02.22 IT Drift, bilag 14 - Sikkerhed

Punkt 2.7 Kryptografi

"Leverandøren skal sikre korrekt og effektiv brug af kryptografi for at beskytte Kundens informationer mod brud på fortrolighed, autenticitet eller integritet.

Leverandøren skal implementere formelle procedurer for sikring og håndtering af krypteringsnøgler, herunder certifikater gennem hele deres levetid.

Eventuelle Øvrige Leverandører må ikke opnå adgang til krypteringsnøgler, herunder certifikater, der benyttes til kryptering, medmindre Kunden vurderer, at der foreligger et forretningsmæssigt behov herfor."

Foranstaltning nr. 9 & 10 (Adgangskontrolpolitikker og multifaktorautentificering)

- Fra SKI 02.22 IT Drift, bilag 14 - Sikkerhed

Punkt 2.4 Adgangskontrol

"Leverandøren skal sikre alle logiske adgange til Kundens informationer, data og Systemerne, herunder foranledige adgang for autoriserede Brugere og forhindre uautoriseret adgang.

Følgende generelle principper skal overholdes i forbindelse med Leverandørens varetagelse af adgangskontrol til Systemerne:

a. Leverandøren skal sikre sporbarhed og logning af alle hændelser samt følge op herpå.

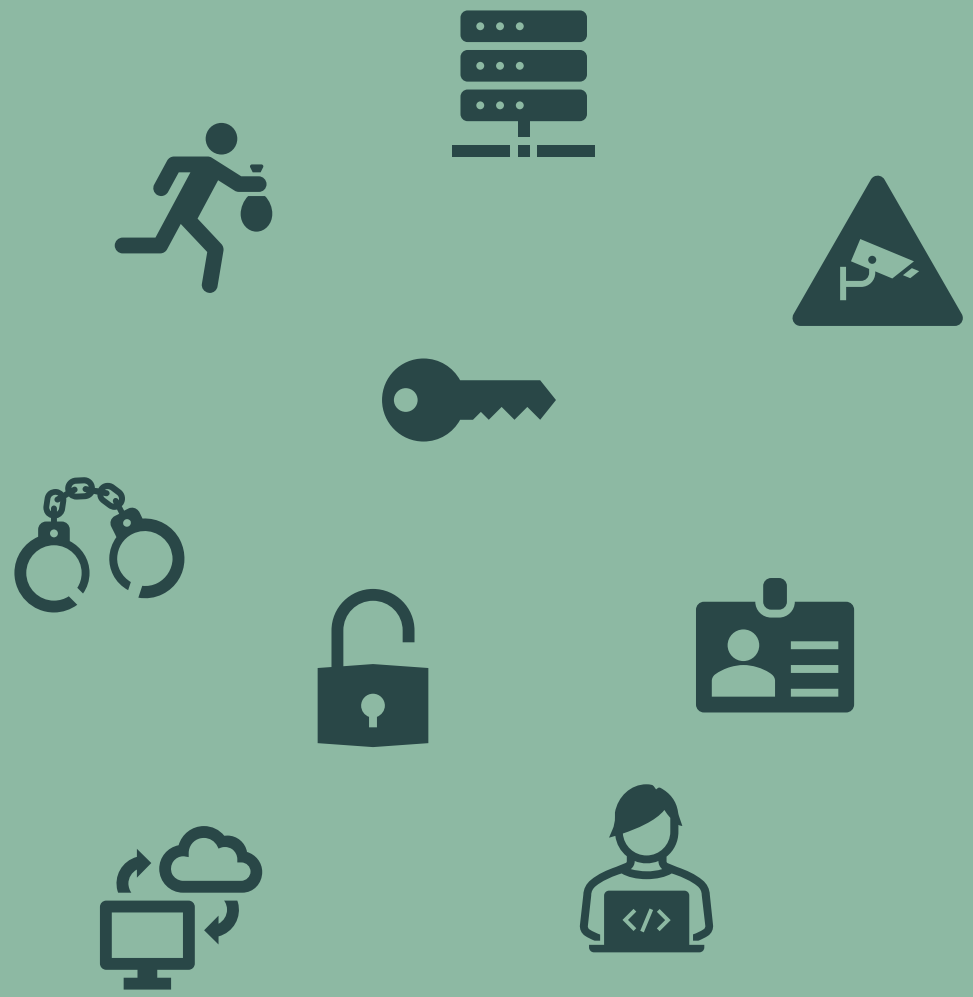
b. Alle eksterne adgange til Systemerne skal ske gennem brug af multifaktorgodkendelse.

c. Leverandøren skal sikre, at kun behørigt autoriserede medarbejdere kan få adgang til Kundens informationer, data og Systemerne.

d. Adgange og rettigheder skal være begrænset til et "need to know"-grundlag."

MOLT | WENGEL

Hvad betyder cybersikkerhed for jer i jeres daglige arbejde?



Opsummering

MOLT | WENGEL

Ledelsesorganets forpligtelser

- Foranstaltningerne skal være godkendt af enhedens ledelsesorgan
- Ledelsesorganet skal føre tilsyn med gennemførelsen
- Medlemmer af ledelsesorganet skal deltage i relevante kurser om styring af cybersikkerhedsrisici
  - Samt tilskynde tilsvarende kurser udbydes til enhedens øvrige ansatte

Foranstaltninger, enheder som minimum skal have foretaget inden 1. juli 2025:

- **Politik** for risikoanalyse og informationssystemsikkerhed
- **Politik** for kryptografi (*beskyttelse af data*) og - hvis relevant - kryptering *(gøre data ulæsbar og kun tilgængelig med nøgle/dekryptering)*
- **Politik og procedure** for måling af foranstaltningernes effektivitet
- **Procedure** for sikkerhed i forbindelse erhvervelse, udvikling og vedligeholdelse af IT-systemer, samt for håndtering af sårbarheder i IT-systemer
- **Procedure** for håndtering af hændelser
- **Sikre driftskontinuitet** *(ved backup-styring samt kunne reetablere til tidligere versioner)*
- **Sikre forsyningskædesikkerhed** *(Undersøge sine direkte leverandørers og tjenesteudbyderes sårbarheder, samt sikre deres generelle kvalitet af produkter og cybersikkerhedspraksis)*
- Grundlæggende **cyberhygiejnepraksisser** og **cybersikkerhedsuddannelse** *(brug af passwords og sikker mail mm., samt uddannelse af relevante medarbejdere)*
- **Sikre** personalesikkerhed *(sikre medarbejdere forstår og forpligter sig til leve op til ansvaret for sikkerheden),* adgangskontrolpolitikker *(sikre kun relevante medarbejdere får adgang)* og forvaltning af aktiver *(sikre forvaltningen hvis de kan påvirke sikkerheden)*.
- **Multifaktorautentificering** for adgang til systemer eller kontinuerlig autentificering, samt **sikre** tale-, video- og tekstkommunikation

Rapporteringer, enheder som minimum skal have foretaget inden 1. oktober 2025:

- **Indsende** enhedens registreringsoplysninger gennem virk.dk

Opsummering

MOLT | WENGEL

Tjekliste vedrørende enhedens forpligtelser ved væsentlige hændelser:

- **Tidlig varsling** ved mistanke om ulovlige eller ondsindede handlinger *(inden 24 timer)*
- **Hændelsesunderretning** vedrørende dens alvor og indvirkning samt kompromitteringsindikatorerne *(inden 72 timer)*
- **Underretning** til modtagere af tjenester, hvis negativ påvirkning af levering af tjenester og hvis modtageren potentielt er/bliver berørt af hændelsen, herunder eventuelle modforanstaltninger modtageren kan foretage *(uden unødigt ophold – formentlig maksimalt 72 timer)*
- **Foreløbig rapport** med statusopdatinger *(efter CSIRT's anmodning)*
- **Endelig rapport** med detaljeret beskrivelse af hændelsen og truslen eller årsagen, der sandsynligvis har udløst hændelsen, samt eventuelle grænseoverskridende virkninger af hændelsen. Herunder anvendte eller igangværende afbødende foranstaltninger *(en måned efter den væsentlige hændelse – hvis afsluttet – og ellers en måned efter hændelsen er håndteret)*
- Eventuelt **pressehåndtering,** såfremt myndighed træffer afgørelse om at informere offentligheden om den væsentlige hændelse

MOLT WENGEL

Spørgsmål?

En mærkbar forskel i byggeriet

www.mowe.dk