SKABELON FOR IT-TILSTANDSRAPPORT & SIKKERHEDSSTRATEGI

Følgende dokument er en skabelon til udarbejdelse af en tilstandsrapport, der beskriver din virksomheds overordnede tilstand ift. it-sikkerhed, cybersikkerhed og persondatasikkerhed, samt evt. andre sikkerhedsområder relevant for din virksomhed. Tilstandsrapporten giver et overblik over organisationens status for IT/OT, implementerede procedurer og tekniske sikkerhedsforanstaltninger ift. relevant lovgivning, for med den viden at kunne planlægge en realistisk og risikobaseret plan for fremtidige tiltag, ændringer og indkøb. Dokumentet kan dels bruges internt, som en støtte i det videre arbejde, og dels som dokumentation over for leverandører og samarbejdspartnere til underbyggelse af drift, vedligehold, monitorering og videreudvikling.

Dokumentet er én af flere skabelon-dokumenter, som indgår i det IT-sikkerhedsmateriale, som alle organisationer bør have ift. overholdelse af NIS2. Skabelonen er opdateret således at den understøtter ”Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren”.

Vi har i Lakeside lavet en række skabeloner, som du er velkommen til at bruge. Skabelonerne er tiltænkt SMV’er med produktion, men kan sagtens bruges af organisationer uden produktion (OT). Skabelonerne er udarbejdet med udgangspunkt i små og mellemstore forsyningsselskaber.

* IT-sikkerhedspolitik
* Nærværende IT-sikkerhedshåndbog
* IT/OT-leverandør sikkerhedspolitik
* IT/OT-leverandør tjekliste
* Risikostyringspolitik og Risikolog
* Hændelseshåndteringsprocedure og Hændelseslog
* Kriseberedskabspolitik, -planer og -skabeloner

Skabelonerne for de øvrige dokumenterne kan findes og downloades på [www.lakeside.dk/publikationer](http://www.lakeside.dk/publikationer)

**Sådan bruger du skabelonen**

* Tekster med gråt og i firkantede klammer er vejledningstekster, som slettes ved endt redigering.
* <organisation> er en dokument-egenskab. Den kan rettes under Filer / Egenskaber / Brugerdefineret (nederste tekstboks) og derefter opdatere alle felter i hele dokumentet (vælg alt og højreklik).
* Alle tekster kan ændres efter behov og som tilpasning til din organisation. Alle tekster med gult bør du ændre eller som minimum forholde dig til.
* Kontaktinformation og organisation skal opdateres i sidehoved og sidefod. OBS! Organisation og logo på forsiden er også i en sidefod.

**Versions historik for skabelon:**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer |
| 1.0 | 03.02.2025 | MTH | Oprettet første version |
| 1.1 |  | MTH | Opdateret jf. bekendtgørelse til energisektoren som implementerer NIS2 og CER. |

DATO | VERSION X.X

TILSTANDSRAPPORT

KONTAKTPERSONER

|  |  |
| --- | --- |
| Fornavn Efternavn (initialer)Skriv din titel her, fx konsulentTlf.: +45 xxxx xxxxxxx@xxxx.dk<Organisation> | Fornavn Efternavn (initialer)Skriv din titel her, fx konsulentTlf.: +45 xxxx xxxxxxx@xxx.dk<Organisation> |

VERSIONS- OG GODKENDELSESHISTORIK

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer | Godkendt |
| [0.0.] | [dd.mm.yy] | [initialer] | [beskrivelse af ændring] | [dato/navn] |

TERMER

[Vejledning: Nedenstående liste indeholder nogle termer som ofte benyttes til beskrivelse af IT/OT. De termer I ikke benytter slettes, og evt. nye tilføjes efter behov.]

| Forkortelse i teksten | Beskrivelse |
| --- | --- |
| AD | Står for Active Directory. Active Directory er egentligt et produktnavn, men er blevet et synonym med en rolle-rettighedsløsning, som styrer brugeradgange. |
| CFCS | Center For Cyber Sikkerhed |
| EMM | Står for Enterprise Mobility Management og dækker over:* Mobilenhedsadministration (MDM)
* Mobilapplikationsadministration (MAM)
* Mobilindholdsadministration (MCM)
* Mobilidentitetsadministration (MIM)

Enterprise Mobility Management (EMM) er en kombination af politikker, teknologier, processer og værktøjer, der hjælper organisationer med at sikre virksomhedsdata, der tilgås fra virksomhedens og personligt ejede enheder.Organisationer kan anvende EMM-software for at sikre, at alle de krævede sikkerhedspolitikker er på plads for at give medarbejderne sikker adgang til de krævede virksomhedsdata overalt. Enterprise Mobility Management lader IT-administratorer eksternt konfigurere de apps og data, som deres ansatte kræver. |
| IT | Informations Teknologi.  |
| MFA | Står for Multi Factor Authentication – eller flerfaktor-autentifikation på dansk. En faktor er noget i kategorien: ”noget jeg ved”, ”noget jeg har” eller ”noget jeg er”.I praksis betyder det at man ud over brugernavn og kodeord skal have endnu en faktor som fx en nøglechip, en indrulleret telefon eller lignende. |
| OT | Operational Technology. Det IT der bruges til understøttelse af produktion; fx SCADA, PLC’er etc. |
| RDP | Står for Remote Desktop Protocol. RDP er en proprietær protokol udviklet af Microsoft Corporation, som giver en bruger et grafisk interface til at oprette forbindelse til en anden computer via en netværksforbindelse. Brugeren anvender RDP-klientsoftware til dette formål, mens den anden computer skal køre RDP-serversoftware. |
| VPN | Står for Virtual Private Network, på dansk "Virtuelt Privat Netværk", er betegnelsen på en teknik, som anvendes for at skabe krypterede punkt til punkt-forbindelser, såkaldte "tunneler", gennem et andet datanet. |

INDHOLDSFORTEGNELSE

[1 Indledning 5](#_Toc191991794)

[1.1 Kort Gennemgang 6](#_Toc191991795)

[2 Rammesætning 8](#_Toc191991796)

[2.1 Lovgivning & rammeværker 8](#_Toc191991797)

[2.1.1 GDPR – Databeskyttelsesloven 8](#_Toc191991798)

[2.1.2 Lov om styrket beredskab i energisektoren (NIS2 & CER) 9](#_Toc191991799)

[2.1.3 ISO 27000 10](#_Toc191991800)

[2.1.4 D-mærket 11](#_Toc191991801)

[3 Generelt 13](#_Toc191991802)

[3.1 Politikker 13](#_Toc191991803)

[3.2 Procedurer 14](#_Toc191991804)

[3.3 Opfølgning 17](#_Toc191991805)

[3.4 Awareness & uddannelse 18](#_Toc191991806)

[3.5 Fysisk sikkerhed 20](#_Toc191991807)

[3.6 Enheder og andet på IT-netværket 21](#_Toc191991808)

[4 Netværk 21](#_Toc191991809)

[4.1 Netværk-navn 22](#_Toc191991810)

[4.2 leverandører til netværk 23](#_Toc191991811)

[4.2.1 Leverandør - navn 23](#_Toc191991812)

[5 Produktion (OT) 24](#_Toc191991813)

[5.1 Produktionsanlæg/Lastniveau 24](#_Toc191991814)

[5.2 Underleverandører til produktionen 25](#_Toc191991815)

[5.2.1 Navn 25](#_Toc191991816)

[5.3 OT-Beredskab 26](#_Toc191991817)

[5.3.1 Eksisterende nøddriftsprocedurer 26](#_Toc191991818)

[5.3.2 Backup & recovery 27](#_Toc191991819)

[6 IT 27](#_Toc191991820)

[6.1 Forretningsproces 27](#_Toc191991821)

[6.1.1 Systemnavn – kort formål (fx økonomisystem) 28](#_Toc191991822)

[6.2 leverandører Af IT 28](#_Toc191991823)

[6.2.1 Navn 29](#_Toc191991824)

# Indledning

[Vejledning: Start med en kort beskrivelse af jeres virksomhed og baggrund for den udarbejdede tilstandsrapport. Nedenfor er der givet et eksempel.]

<Organisation> er et demokratisk ejet anpartsselskab, dvs. kundeejet selskab, som non-profit sørger for, at størstedelen af … altid har varme i radiatoren og varmt vand i hanen. Det er vores erklærede mål at levere den bedste og billigste varme til vores forbrugere.

Det frygtes nationalt og i EU at et cyberangreb kan efterlade store dele af samfundet uden varme, og den største trussel er mod IT og OT-systemerne. Derfor skal fjernvarmeselskaberne mere end før være opmærksomme og implementere IT-sikkerhedsforanstaltninger til beskyttelse af deres IT og OT.

IT/OT-anvendelsen i <Organisation> har til formål at understøtte selskabets overordnede forretnings-formål om at levere stabil og prisbillig varmeforsyning.

For <Organisation> er OT de kritiske systemer, da det er disse der styrer fjernvarmeproduktionen. IT er administrative systemer og understøtter løn-, personale- og kundeadministration, hvilket alle er vigtige funktioner, men den primære proces er og bliver fjernvarmeproduktionen.

For at lave en effektiv implementering af sikkerhedsforanstaltninger, har vi valgt at få udarbejdet denne tilstandsrapport som beskriver udgangspunktet for arbejdet. Dvs. at vi i <Organisation> har kortlagt vores eksisterende politikker & procedurer, fysisk sikkerhed, netværk, produktions- og IT-løsninger. Herigennem er leverandører, hardware (komponenter) og dataflows kortlagt, sammen med eksisterende sikkerhedstiltag og evt. sårbarheder og mangler, samt forslag til forbedringer.

Denne rapport er udarbejdet på vegne af ledelsen i <Organisation>, ved hjælp af …, og godkendt af bestyrelsen jf. historikken først i dokumentet. Rapporten er blevet til via inddragelse af <Organisation>s medarbejdere og IT/OT-leverandører.

[Vejledning: fremhæv i kassen de vigtigste punkter. Her er der givet et bud]

|  |
| --- |
| Status: <Organisation> er godt med ift. netværkssikkerhed og OT-sikkerhed. De største mangler findes ift.:1. politikker, procedurer og vejledninger, inkl.
2. awareness træning og uddannelse af medarbejdere.
3. leverandørstyring
 |

## Kort Gennemgang

[Vejledning: Herunder fremhæves de overordnede nedslagspunkter. Dette opsummerer resten af rapporten, og laves bedst som det sidste afsnit.]

**Niveauplacering & anlægs klassificering**

[Vejledning: Her kan man angive det niveau som virksomheden indplaceres på. Denne placering ligger grundlaget for det resterende arbejde ift. lovgivning. For virksomheder indplaceret på niveau 2 og over skal man have vurderet og klassificeret sine anlæg. Anlæg kan ikke klassificeres jf. Bekendtgørelsens bilag til en højere klasse end virksomhedens niveauplacering. Det er vigtigt at holde i mente at Energistyrelsen har mandat til både at hæve virksomhedens niveauplacering og klassen for specifikke anlæg, hvis de vurderer at der er særlige omstændigheder ift. kritisk infrastruktur i andre sektorer, men som udgangspunkt vil de fleste indplaceres jf. Bekendtgørelsen.]

Jf. Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren (herefter Bekendtgørelsen) Bilag 1 vil <Organisation> niveauplaceres på niveau X, og jf. Bekendtgørelsens Bilag 2 er anlæg A, B, C indplaceret i klasse Y.

**Politikker og procedurer**

<Organisation> har sideløbende med udarbejdelsen af denne tilstandsrapport igangsat arbejdet med udarbejdelsen og opdatering af politikker som definerer rammerne og organiseringen af sikkerheds- og beredskabsarbejdet.

**Beredskab**

[Vejledning: På niveau 1 er der krav om at man kan sende sin beredskabsplan ind til Energistyrelsen, hvis de beder om den. På niveau 2 og over er der krav om at man selv sender den ind. For fjernvarmeselskaber er deadline for første indsendelse 1. oktober 2025, og herefter hvert 3. år.]

<Organisation> skal sikre at der er implementeret et beredskab jf. Bekendtgørelsen, og kunne indsende sin beredskabsplan til Energistyrelsen, hvis denne bliver efterspurgt.

**Risiko og håndtering af risiko**

[Vejledning: Der er ikke krav om risikostyring på niveau 1. På niveau 2 og over er der krav om at man sender sin risiko- og sårbarhedsvurdering ind til Energistyrelsen. Deadline for første indsendelse 1. oktober 2025, og herefter hvert 3. år. Desuden er der krav til risikostyring i projekter og indberetning til Energistyrelsen for større projekter der fx kan have indvirkning på virksomhedens niveau eller anlægs klasse.]

<Organisation> er i gang med at udarbejde en risikostyringspolitik. Risikostyringspolitikken vil definere risikovurderingsprocessen og -organisationen, samt de risikoniveauer som benyttes på tværs af organisationen med det formål at alle forstår risiko på den samme måde. Resultatet af risikostyringen vil være en handlingsplan for mitigerende tiltag, som vil sikre at handlingsplanen fordeler og prioriterer ressourcer på et oplyst grundlag.

<Organisation> har implementeret risikostyring på projektniveau.

**Leverandører**

For <Organisation> leverandører er der udarbejdet en vurdering af den enkelte leverandørs indflydelse på <Organisation> IT- og OT-sikkerhed og beredskab. De mest kritiske leverandører er X og Y:

1. Leverandør X er ansvarlig for vedligehold af <Organisation>s netværk og kontrolstyring for OT, og indgår dermed som en vigtig samarbejdspartner i <Organisation>s beredskab.
2. Leverandør Y er en SaaS-leverandør vis tjenester <Organisation> gør brug af til understøttelse af økonomi, selvbetjeningsløsninger til forbrugere, ledelsesunderstøttelse etc.

Denne vurdering genbesøges årligt, samtidig med at det sikres at der er indgået de nødvendige aftaler til understøttelse af <Organisation>s behov, og at disse aftaler efterleves.

**Fysiske sikkerhedsforanstaltninger**

[Vejledning: Der er ikke krav til implementering af specifikke fysiske sikkerhedsforanstaltninger på niveau 1. På niveau 2 og over gælder Bekendtgørelsens kapitel 10 for alle anlæg på klasse 2 og over. Her beskrives kort hvorvidt man overholder Bekendtgørelsens krav til fysisk sikring:

* modstandsdygtighed og genoprettelse af de fysiske anlæg,
* adgangskontrol, overvågning af adgang til bygninger og alarmer

Der er stor differentiering i krav til de forskellige klasser anlæg.]

**Tekniske sikkerhedsforanstaltninger**

[Vejledning: Der er ikke krav til implementering af specifikke tekniske sikkerhedsforanstaltninger på niveau 1. På niveau 2 og over gælder Bekendtgørelsens kapitel 11 for netværk og IT/OT. Det er her der kommer krav til logning, adgangskontrol (til systemer og fjernadgang), backup, kryptering, netværkssegmentering etc.]

**Rapportering**

<Organisation> følger op på tilstanden for IT-sikkerhed i organisationen og afrapporterer status løbende til bestyrelsen, samt fremlæggelse af en opsummeret rapport en gang årligt.

# Rammesætning

Først fastsættes rammerne for arbejdet med IT-sikkerhed i <Organisation> identifikation af den relevante lovgivning.

Tilsynsrapporten er blevet til med vejledning fra Center for Cybersikkerheds: ”Håndtering af industri- og kontrolsystemer”: <https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-vejledning-haandtering-af-industrikontrolsystemer-2020.pdf>

## Lovgivning & rammeværker

I dette afsnit beskrives kort den lovgivning og de rammeværker ud fra hvilke IT-miljøets tilstand er vurderet.

[Vejledning: Slet de afsnit der ikke er vurderet relevant på nuværende tidspunkt for den pågældende organisation]

### GDPR – Databeskyttelsesloven

[Vejledning: Afsnittet er obligatorisk, da alle virksomheder i Danmark skal overholde GDPR]

|  |  |
| --- | --- |
| Navn | Kært barn har mange navne; GDPR, [Databeskyttelsesforordningen](https://gdpr.dk/databeskyttelsesforordningen/) og [Persondataforordningen](https://gdpr.dk/persondataforordningen/) er det samme. GDPR står for General Data Protection Regulation, og er en lovgivning, som er indført af EU. Danske organisationer skal overholde den danske implementation af dette: Databeskyttelsesloven. |
| Formål | Helt konkret handler Databeskyttelsesloven om, at du skal have styr på sikkerheden om de personoplysninger, som din virksomhed behandler. Du skal altså blive bedre til at passe på personoplysninger. |
| Ikrafttrædelses dato | 25. maj 2018 |
| Gældende for | Alle virksomheder |
| Risikovurdering | Virksomheden skal lave en vurdering af risici for de registrerede. Dvs. at en GDPR-risikovurdering ikke omhandler virksomhedens risici, men de risici som de registrerede har ved virksomhedens behandling af data. |
| Myndighed | **Datatilsynet*** Datatilsynet har ret til at komme på tilsyn i din virksomhed.
* I har pligt til at anmelde ”sikkerhedsbrud” til Datatilsynet.
* Kunder kan anmelde din virksomhed til Datatilsynet.
 |

### Lov om styrket beredskab i energisektoren (NIS2 & CER)

|  |  |
| --- | --- |
| Navn | Net- og Informationssikkerhedsdirektiv (NIS2-direktivet) [EU-direktiv (EU) 2022/2555](https://eur-lex.europa.eu/eli/dir/2022/2555/oj).Kritiske enheders modstandsdygtighed (CER-direktivet) EU direktiv (EU) 2022/2557.NIS2 og CER implementeres for danske fjernvarmeselskaber i ”Lov om styrket beredskab i energisektoren”, som udmøntes i ”Bekendtgørelse om modstandstandsdygtighed og beredskab i energisektoren”. Til dagligt omtales alt dette blot som ”Bekendtgørelsen”. |
| Formål | Formålet med direktiverne, lovforslaget og bekendtgørelsen er at styrke energisektorens beredskab med henblik på at forebygge og modstå hændelser, som truer energiforsyningen. |
| Ikrafttrædelses dato | 7. marts 2025 |
| Gældende for | Sektor: Energi Delsektor: Elektricitet, fjernvarme og fjernkøling, Olie, Gas og BrintAlle selskaber i de nævnte delsektorer inddeles i niveauer. For fjernvarmeselskaber er disse niveauer baseret på tærskelværdier for distribution og transmission af fjernvarme; dog kan nogle selskaber også blive indplaceret baseret på deres elforbrug i fjernvarmeproduktionen. <Organisation> forventes indplaceret på niveau X jf. Bilag 1 i Bekendtgørelsen[[1]](#footnote-2).  |
| Risikovurdering | Omfattede organisationer skal lave en vurdering af risici for organisationens tjenester. Dvs. risiko for at hændelser har en negativ effekt på levering af organisationens tjenester - primært levering af fjernvarme. |
| Myndighed | **Energistyrelsen**[[2]](#footnote-3)* For alle organisationer i energisektoren er der er krav til indrapportering til Energistyrelsen ift. indplacering på niveau
* Niveau 1 virksomheder, skal kunne indsende en beredskabsplan ved efterspørgsel. Niveau 2 virksomheder og over skal indsende beredskabsplan og sårbarhedsvurdering hvert 3. år. Første gang 1. oktober 2025
* Energistyrelsen har ret til at komme på tilsyn i din virksomhed
* Energistyrelsen har ret til at lave sårbarhedsscanning af din virksomhed.
 |

### ISO 27000

[Vejledning: Optionel standard som kan bruges til at standardisere og understøtte implementation af de nødvendige foranstaltninger, som virksomheden skal implementere for at beskytte egne aktiver, samt overholde forskellig lovgivning]

|  |  |
| --- | --- |
| Navn | ISO 27000. Dækker i dagligomtale en række standarder 27000, 27001, 27002, 27005 etc. Fælles for dem er at der er tale om standarder for informationssikkerhedsledelsessystemer (ISMS) |
| Formål | Formålet med standard(erne) er at specificere kravene til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for informationssikkerhed (ISMS) inden for organisationens rammer og vilkår.  |
| Gældende for | Optionel standard for private virksomheder. Standarden er meget brugt i offentlige virksomheder og organisationer, og et krav i nogle. |
| Risikovurdering | Virksomheden skal lave en vurdering af risici for virksomheden.  |
| Certificering | Man kan vælge at betale en it-revisor for at lave en revision eller en certificering af sit ISMS. Revision og certificering skal vedligeholdes med jævne mellemrum; typisk årligt eller ved større ændringer.  |

### D-mærket

[Vejledning: Optionel standard som kan bruges til at standardisere og understøtte implementering af de nødvendige foranstaltninger som virksomheden skal implementere for at beskytte egne aktiver, samt overholde forskellig lovgivning]

|  |  |
| --- | --- |
| Navn | D-mærket. En mærkningsordning udarbejdet i samarbejde mellem bl.a. Digitaliseringsstyrelsen, Dansk Erhverv, Dansk Industri, SMVdanmark og Forbrugerrådet Tænk. |
| Formål | Mærkningsordningen fortæller at en virksomhed har styr på it-sikkerhed og ansvarlig dataanvendelse efter internationale standarder. D-mærket er din vej til at forsikre forbrugere, kunder og partnere om, at de og deres data er i sikre hænder hos din virksomhed – nu og i fremtiden.Med en D-mærkning viser en virksomhed at de overholder krav fra GDPR, NIS2, ISO 27000 og har lavet dataetiske overvejelser i forbindelse med deres indsamling og brug af data. |
| Gældende for | Optionel mærkning for private virksomheder.  |
| Mærkning | Det er gratis og uforpligtende at komme i gang. Din virksomhed betaler først, når I ansøger om tilsyn for at få tildelt D-mærket. Betalingen er baseret på virksomhedens størrelse og kategori.  |

Overblik



I nedenstående afsnit gives et overblik over vores eksisterende IT- og OT-systemer, samt de organisatoriske tiltag der er implementeret i <Organisation>. For hvert afsnit beskrives den nuværende tilstand, og der gives forslag til mulige forbedringstiltag.

Vi har valgt at gruppere overblikket under fire overskrifter:

1. Generelt – som gennemgår eksisterende politikker og procedurer, inkl. retningslinjer og tiltag målrettet medarbejderne
2. Netværk – som gennemgår netværkets opbygning
3. OT – som gennemgår OT til understøttelsen af varmeproduktionen
4. IT – som gennemgår IT til understøttelsen af administration og støttesystemer til driften for <Organisation>, inkl. understøttelse af forbrugerne og forbrugerafregning.

# Generelt

|  |  |
| --- | --- |
|  | I dette afsnit beskrives alle de it-sikkerhedstiltag, politikker, procedurer, planer etc. som går på tværs i virksomheden, inkl. alle de medarbejderrettede procedurer som understøtter virksomhedens it-sikkerhed og fysiske sikkerhedstiltag.Med begrebet ”medarbejder” menes i denne sammenhæng også konsulenter og underleverandører med adgang til virksomhedens it-miljøer. |

## Politikker

[Vejledning: Politikkerne sætter rammerne og lægger strategien for virksomheden indenfor specifikke områder. Politikker skal godkendes af det øverste ledelsesniveau fx bestyrelsen, hvis virksomheden har en sådan.]

Politikker gives en status fra 0-4 baseret på følgende skala:

|  |  |
| --- | --- |
| 1. Mangler
 |  |
| 1. Planlagt
 |  |
| 1. Findes
 |  |
| 1. Godkendt
 |  |
| 1. Gennemgår årligt review
 |  |

[Vejledning: Tanken er, at der sættes en værdi i tabellens ’status’ kolonne, og cellen farvemarkres jf. ovenstående skala. Tabellens rækker er udfyldt ift. de politikker og procedurer som er påkrævet af GDPR og Bekendtgørelsen (eller anden ramme), hvilket fremgår af kolonne ’Ramme’.]

| Politik  | Status | Note | Ramme |
| --- | --- | --- | --- |
| IT-sikkerhedspolitik inkl. persondatapolitik, netværkspolitik og logpolitik | 2 - Findes | [Vejledning: IT-sikkerhedspolitikken skal sætte rammerne for IT-sikkerhedsarbejdet, inkl. organisering og ansvarsplacering. ] | Bekendtgørelsen |
| Beredskabspolitik | 1 - Planlagt | [Vejledning: Beredskabspolitikken skal sætte rammerne for beredskabsplanlægning, inkl. organisering og ansvarsplacering. Beredskabsplanlægningen skal både dække IT og OT, krisehåndtering, forretningskontinuitet og genskabelsesstrategi/-plan, og test af beredskab.] | Bekendtgørelsen |
| Privatlivspolitikker | 3 - Godkendt | [Vejledning: Privatlivspolitikken fortæller hvordan virksomheden behandler persondata. Man kan have forskellige privatlivspolitikker målrettet forskellige modtagere fx medarbejdere, kunder og ansøgere, samt en cookiepolitik målrettet brugere af deres hjemmeside.] | GDPR |

|  |  |
| --- | --- |
| Kendte sårbarheder  | Mulige forbedringstiltag |
|  |  |

## Procedurer

Procedurer gives en status fra 0-4 baseret på følgende skala:

|  |  |
| --- | --- |
| 1. Mangler
 |  |
| 1. Planlagt
 |  |
| 1. Findes
 |  |
| 1. Implementeret
 |  |
| 1. Gennemgår årligt review
 |  |

[Vejledning: Tanken er at der sættes en værdi i tabellens ’status’ kolonne, og cellen farvemarkres jf. ovenstående skala. Tabellens rækker er udfyldt ift. de politikker og procedurer som er påkrævet af GDPR og NIS2, hvilket fremgår af kolonne ’Ramme’. ]

| Procedure | Status | Note | Ramme |
| --- | --- | --- | --- |
| IT-sikkerhedshånd-bog | 3 - Implementeret | [Vejledning: IT-sikkerhedshåndbogen kan have mange navne. Det vigtige er at den indeholder medarbejdernære sikkerhedsretningslinjer, således at medarbejderne er klædt på til at udføre deres arbejde. Sikkerhedsretningslinjer bør som minimum indeholde information om:* retningslinjer for brug af IT
* datakategorisering
* krav til systemopdateringer
* uddannelse af medarbejdere
* fjernadgang]
 | Bekendtgørelsen |
| Risiko- og sårbarheds-vurdering | 1 – Planlagt | [Vejledning: arbejdet med risikovurdering bliver mere og mere udbredt. I er sikkert vandt til at arbejde med risikovurdering i projekter (det skal stå her) men der skal også foreligge procedurer for risikovurdering for jeres virksomhed (niveau 2 og over) ift. it-sikkerhed. Disse procedurer implementeres jf. rammesætningen i. risikovurderingspolitikken]  | Bekendtgørelse |
| Beredskabsplan | 2 – Findes | [Vejledning: Beredskabsplanen implementerer Beredskabspolitikken og består af:* Beredskabsplan
* Hændelseshåndteringsprocedure
* Skabeloner til brug i beredskabsarbejdet]
 | Bekendtgørelsen |
| Leverandør-instruks inkl. databehandling  | 1 – Planlagt | [Vejledning: Der skal udarbejdes en procedure som sikrer at leverandøraftaler indeholder de relevante krav fra Bekendtgørelsen ift. at understøtte den specifikke aftale:* Passende foranstaltninger ift. håndtering af risici og hændelser fx:
	+ backup og gendannelse
	+ logning
	+ system- og sikkerhedsopdateringer
	+ netværksadgang og tilkobling af enheder på netværk
	+ adgangsstyring og fjernadgang
	+ uddannelse af egne medarbejdere
* Underretning om væsentlige hændelser
* Bistand ved jeres afrapportering om hændelser
* Inddragelse i tilsyn
* Deltagelse i øvelser
* Deltagelse i beredskab
* Brug af underleverandører
* Ejerskab af data placeret hos jeres organisation
* Indgåelse af databehandleraftaler]
 | Bekendtgørelse & GDPR |

|  |  |
| --- | --- |
| Kendte sårbarheder  | Mulige forbedringstiltag |
|  |  |

## Opfølgning

Opfølgningstiltag gives en status fra 0-4 baseret på følgende skala:

|  |  |
| --- | --- |
| 1. Mangler
 |  |
| 1. Planlagt
 |  |
| 1. Foretages ad hoc
 |  |
| 1. Foretages min det påkrævede jf. rammesætning
 |  |
| 1. Foretages mere end det påkrævede jf. rammesætning
 |  |

[Vejledning: Tanken er at der sættes en værdi i tabellens ’status’ kolonne, og cellen farvemarkres jf. ovenstående skala. Skalaen kan tilpasses den enkelte organisation, da det baseret på en risikovurdering evt. skal skærpes (fx er det måske ønskværdigt at få foretaget visse kontroller hvert kvartal og ikke kun halvårligt. Statusværdien giver en mulighed for at lave et samlet overblik og sammenligne modenhedsniveau ift. det ønskelige for jeres organisation. Tabellens rækker er udfyldt ift. de tiltag som er påkrævet af NIS2, hvilket fremgår af kolonne ’Ramme’.]

| Politik / procedure | Status | Note | Ramme |
| --- | --- | --- | --- |
| Internt tilsynKontrol & øvelser | 0 – Mangler | [Vejledning: i Bekendtgørelsen er der krav (niveau 2 og over) til en række kontroller og øvelser som skal udføres, med henblik på at afprøve effektiviteten af de implementerede foranstaltninger, samt at sikre at kontrollerne fortsat er korrekt implementeret. Øvelserne skal fremgå af en 5-årig øvelsesplan som skal sendes ind til Energistyrelsen]  | Bekendtgørelse |
| Leverandør opfølgning | 0 – Mangler | [Vejledning: Der skal laves en årlig opfølgning på overholdelse af leverandøraftaler. Der er ikke specifikke krav for virksomheder på niveau 1, men det skal sikres at der er de leverandøraftaler der skal til til understøttelse af beredskabet.] | Bekendtgørelse |
| Databehandler tilsyn | 0 – Mangler | [Vejledning: Der skal være en procedure til opfølgning på overholdelse af databehandleraftaler. Brug gerne Datatilsynets vejledning til Tilsyn.] | GDPR |

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
|  |  |

## Awareness & uddannelse

Opmærksomhed og uddannelsestiltag gives en status fra 0-4 baseret på følgende skala:

|  |  |
| --- | --- |
| 1. Mangler
 |  |
| 1. Planlagt
 |  |
| 1. Foretages ad hoc
 |  |
| 1. Foretages årligt
 |  |
| 1. Foretages løbende hen over året
 |  |

[Vejledning: Tanken er at der sættes en værdi i tabellens ’status’ kolonne, og cellen farvemarkres jf. ovenstående skala. Tabellens rækker er udfyldt ift. de uddannelsestiltag som er påkrævet af GDPR og NIS2, hvilket fremgår af kolonne ’Ramme’. ]

| Retningslinje / sikkerhedstiltag | Status | Note | Ramme |
| --- | --- | --- | --- |
| Tiltrædelses- og fratrædelsesprocedurer | 3 - Implementeret | [Vejledning: De procedurer der omhandler ny medarbejdere, skal inkludere uddannelse i sikkerhedsregler, tildeling af adgangsrettigheder, udlevering af udleveret udstyr og nøgler/nøglebrikker etc. Procedurerne for afskedigelse af medarbejdere skal omhandle fratagelse af adgangsrettigheder, indlevering af udleveret udstyr/nøglebrikker etc.Procedurerne dokumenteres fx ved tjekliste der gemmes i personalesagen. ] | Bekendtgørelsen & GDPR |
| Awareness | 0 – Mangler | [Vejledning: Awareness skal være løbende for at være effektiv.] | Bekendtgørelsen |
| IT-sikkerhedsuddannelse og træning i håndtering af persondata  | 2 – Foretages ad hoc | [Vejledning: Den generelle sikkerhedsuddannelse bør suppleres med IT-sikkerhedsuddannelse rettet mod den enkelte medarbejders arbejdsområde inkl. (ikke udtømmende):* specifikt krav til uddannelse i regler til beskyttelse af produktions- og netværkskomponenter (Drift team)
* træning i håndtering af persondata (alle)
* håndtering af fysiske data – opbevaring, deling og bortskaffelse
* cybersikkerhedsuddannelse både til medarbejdere og til ledelse / bestyrelse
* hændelseshåndtering og krisestyring]
 | Bekendtgørelsen & GDPR |

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
|  |  |

## Fysisk sikkerhed

Dette afsnit beskriver de tiltag som er opsat som fx sikring mod brand, indbrud, adgang for uvedkommende. De tiltag der er specifikke for netværket eller for specifikke løsninger beskrives i de pågældende afsnit.

[Vejledning: Beskriv:

* fysisk adgangskontrol og alarmer
* fysisk adgang til IT/OT-infrastrukturen
* brandsikring
* håndtering af strømsvigt
* andet fysisk sikring]

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
|  |  |

## Enheder og andet på IT-netværket

[Vejledning: Dette afsnit beskriver de enheder som der benyttes:

* pc’er, smartphones og tablets, inkl. indkøbsprocedure og support
* evt. styresystemer, Management af devices, og AD adgang enheder]

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
|  |  |

# Netværk

|  |  |
| --- | --- |
|  | I dette afsnit beskrives <Organisation>s netværk og netværkssegmentering, inkl. brugerstyring og leverandørforhold.<Organisation>s netværk og adgangsstyring følger CFCS vejledning til sikkerhed i industri- og kontrolsystemer. |
|

|  |
| --- |
| Center for Cyber Sikkerhed (CFCS) anbefaler at man ved valg af segmentering anvender disse fire skridt:1. Identificer grupper af komponenter eller netværk, som har et forretningsmæssigt behov for at kommunikere
2. Vurder om der er behov for yderligere opdeling i sikkerhedszoner i de forretningsmæssige fællesskaber betinget af forskellige sikkerhedsbehov
3. Definer de forbindelser mellem sikkerhedszoner, der er nødvendige for at tilgodese forretningsbehovet
4. Etabler og vedligehold et overblik, således at der kun er én forbindelse eller ét punkt for dataudveksling mellem forskellige segmenter eller sikkerhedszoner.
 |

 |

[Vejledning: Indsæt her en figur der giver det overordnede billede af virksomhedens netværk og netværkssegmenteringer, samt evt. forbindelser imellem samme.

Lav en overordnet beskrivelse af netværket/netværkene og de indbyrdes afhængigheder, samt evt. leverandørunderstøttelse af netværk.

For hvert overordnet netværk: fx OT-netværk, gæstenet, Administration beskrives yderligere jf. nedenstående skabelon.]

## Netværk-navn

[Vejledning: Dette afsnit udfyldes for hvert netværk og netværkssegmentering i ovenstående figur. Evt. en grafisk repræsentation som viser komponenter i det enkelte netværk.

Beskrivelse/formål – er netværket kablet og eller trådløst. Andre ting der er specifikke for det pågældende netværk.

Beskrivelse af tekniske foranstaltninger så som jumpstations, vpn, monitorering etc.

Beskriv hvordan adgangskontrollen fungerer for det pågældende netværk. Hvem har adgang? Hvordan tildeles adgang? Hvordan er netværket beskyttet ift. adgangskontrol fx to-faktor autentifikation?]

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
|  |  |

## leverandører til netværk

[Vejledning: leverandør(er) der står for at vedligeholde og servicere jeres netværk bør dette fremgå her. For hver leverandør med ansvar for netværk som beskrevet ovenfor beskrives yderligere jf. nedenstående skabelon.]

### Leverandør - navn

|  |  |
| --- | --- |
| Formål | [Vejledning: Beskriv overordnet jeres relation] |
| Opgaver | * Ekstern OT-administration
* Adgangsstyring til produktionsnetværk (LDAP)
* Indgå i beredskab ift. OT
* Opsætning af styring (SCADA, kodning af PLC’er)
* Opdatering og sikkerhedspatching af netværksenheder
* Backup og reetablering af netværksenheder og styring
* Logning og monitorering i OT netværk
 |
| Vurdering ift. Bekendtgørelsen | [Vejledning: Er leverandøren selv direkte eller indirekte omfattet af NIS2? Og i hvilket omfang er jeres tjenester afhængigt af leverandøren? Understøtter de fx jeres beredskab.] |
| Databehandler | [Vejledning: Ja/Nej – beskriv hvofor/hvorfor ikke] |

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
|  |  |

# Produktion (OT)

|  |  |
| --- | --- |
|  | I dette afsnit beskrives virksomhedens produktionsanlæg, komponenter og it-sikkerhedstiltag.[Vejledning: tilføj evt. beskrivelse, hvis det giver mening at opdele afsnittet i yderligere underafsnit. I fjernvarmeproduktion kan det fx give mening at differentiere imellem last-niveauer:* Grundlast
* Mellemlast
* Spidslast
* Reservelast

Da det understøttende OT (produktionsanlæg) er underlagt forskellige risici- og konsekvensberegninger, baseret på last-nveauet.] |

[Vejledning: Lav en overordnet beskrivelse af produktionsanlæggene og de indbyrdes afhængigheder, samt evt. leverandørunderstøttelse af produktionen.

For hvert produktionsanlæg beskrives yderligere jf. nedenstående skabelon.]

## Produktionsanlæg/Lastniveau

|  |  |
| --- | --- |
| Beskrivelse  | [Vejledning: Kort beskrivelse af anlægget] |
| Formål | [Vejledning: Hvad er det forretningsmæssige formål med produktionsanlægget?] |
| Kritikalitet | [Vejledning: Hvor kritisk er anlægget ift. levering af organisationens tjenester?] |

|  |  |  |
| --- | --- | --- |
| Komponent | Formål | Leverandør |
| [Vejledning: Hvad er det for en type komponent? Fx vægt, kran, kedel etc. En række pr komponent.] | [Vejledning: Formålet med komponenten] | [Vejledning: Navn på leverandør hvis det er en leverandør der har ansvar for service og vedligehold af komponenten.]  |

|  |  |  |
| --- | --- | --- |
| Afhængigheder | Beskrivelse | Imødekommelse |
| [Vejledning: her beskrives de afhængigheder som anlægget har fx til reservedele, forsyning udefra (el), kontrolsystemer, netværk, andre virksomheders anlæg.] | [Vejledning: Beskriv afhængigheden] | [Vejledning: Hvad er der gjort for at nedbringe afhængigheden? Fx er der etableret nødstrøm? En aftale ift. sikring af reservedele, redundans af anlæg etc.]  |

## Underleverandører til produktionen

Underleverandører til <Organisation> og deres medarbejdere skal have uddannelse i IT-sikkerhed og er underlagt tavshedspligt ift. arbejdet der udføres for <Organisation>.

Underleverandører til <Organisation>og deres medarbejdere skal overholde <Organisation>s IT-sikkerhedspolitik og respektere <Organisation>s sikkerhedsprocedurer – herunder netværkspolitik og proceduren for adgangsstyring.

Det er den enkelte underleverandørs ansvar at indmelde brugere der skal oprettes, samt ændringer ved fx afskedigelser eller ændring i arbejdsopgaver, og at dette sker uden unødig forsinkelse via de korrekte procedurer gennem henvendelse til <Organisation>.

[Vejledning: For hver underleverandør listet i gennemgangen af produktionsanlæggene ovenfor beskrives yderligere jf. nedenstående skabelon.]

### Navn

|  |  |
| --- | --- |
| Formål | [Vejledning: Beskriv leverandørens formål]  |
| Opgaver | [Vejledning: På punktform beskriv kort leverandørens opgaver. Fx backup og reetablering af specifikke OT-komponenter. Opdatering og servicering af vægt.] |
| Vurdering ift. NIS2 | [Vejledning: Her beskrives hvorvidt den pågældende leverandør er direkte omfattet af NIS2, bliver indirekte omfattet af NIS2 baseret på understøttelse af jeres organisation, eller om leverandøren ikke er omfattet af NIS2.] |
| Databehandler | [Vejledning: Her beskrives hvorvidt den pågældende leverandør er databehandler på vegne af jeres virksomhed, og i hvilken sammenhæng/med hvilket formål.] |

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
| Der kan være andre leverandører som ikke er fundet i gennemgangen. | Det bør sikres at der sker en løbende opsamling over hvilke leverandører der understøtter produktionen. |

## OT-Beredskab

[Vejledning: lav evt. en opdeling af prioritet ift. de beskrevne produktionsanlæg eller last-niveauer. I så fald kopieres nedenstående tabel det antal gange som giver mening for jer.]

|  |  |
| --- | --- |
| Konsekvens ved manglende produktion | [Vejledning: Indsæt en beskrivelse af konsekvensen for manglende produktion. Ved varmeproduktion angives antallet af husstande der vil stå uden varme, og evt. samfundsvigtige organisationer, såsom hospitaler, plejehjem og andet ’blå-blink’. Hvis I ikke har en liste over de blå blink der ligger i jeres område, bør I få dette afdækket.Der er pt usikkerhed omkring, hvorvidt de faktisk gør en forskel ift. jeres kritikalitetsvurdering, fordi mange af dem har selv beredskab og er ikke afhængige af jeres, men I jeres risikovurdering skal I have afdækket den samfundsmæssige og organisatoriske konsekvens ved manglende produktion. Afventer yderligere afklaring fra BRS.] |
| Prioritet | Høj |

### Eksisterende nøddriftsprocedurer

[Vejledning: beskriv eksisterende nøddriftsprocedurer. Hvad gør I i dag, når et produktionsanlæg fejler? Hvordan uddannes medarbejderne i disse?]

### Backup & recovery

[Vejledning: beskriv eksisterende backup- & genetableringsprocedurer for jeres OT. Hvad gør I i dag, når et produktionsanlæg skal genskabes? Hvordan testes disse.]

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
|  |  |

# IT

|  |  |
| --- | --- |
|  | I dette afsnit beskrives virksomhedens IT-systemer fordelt på administration- og støttesystemer, og kunderettede systemer, samt de implementerede it-sikkerhedstiltag.Under administration- og støttesystemer finder vi de systemer som understøtter følgende forretningsprocesser:* Økonomi
* Løn & udlæg
* Timeregistrering
* Bestyrelsesarbejde
* Projektstyring
* Officepakken
* Monitorering
* Fakturering og rapportering
* Kundeselvbetjening
* Udsendelse af driftsinformation
* Andet…
 |

[Vejledning: En overordnet beskrivelse af organisationens strategi for IT. Fx er IT-løsninger indkøbt som software services (SaaS), eller hostes de lokalt? Hver forretningsproces beskrives jf. nedenstående skabelon.]

## Forretningsproces

[Vejledning: Beskriv forretningsprocessen inkl. understøttende systemer, dataflows, brugerroller/bruger, leverandør, og videregivelse af data.

For hvert understøttende system gentages nedenstående skabelon.]

### **Systemnavn – kort formål (fx økonomisystem)**

|  |  |
| --- | --- |
| Formål | [Vejledning: kort beskrivelse af systemets formål] |
| Internt ansvarlig | [Vejledning: Angivelse af hvem i organisationen der er ansvarlig for kontrakten og opfølgning på samme.] |
| Leverandør | [Vejledning: Angivelse af leverandøren af systemet. Dvs. den leverandør som jeres organisation har indgået aftale med omkring brugen af systemet.] |
| Brugerroller | [Vejledning: beskrivelse af de roller der har adgang til systemet og deres adgangsbeføjelser.] |
| Adgangsmekanisme og fjernadgang | [Vejledning: beskrivelse af hvordan adgangskontrol varetages. Fx: Er der fler-faktor autentifikation? Kræves der VPN adgang? Hvordan tildeles rettigheder? Er der opsat geofencing?] |
| Persondata | [Vejledning: Indeholder/behandler systemet organisationens persondata? Hvilke og hvilken slags? (Klassifikation jf. GDPR). Hvis systemet behandler persondata på vegne af jeres organisation, kan det være en indikator på at leverandøren er databehandler, og I skal sikre at der er en databehandleraftale på plads.] |
| Anden data | [Vejledning: Ikke alle data er persondata. Her kan I angive, hvis systemet indeholder andre slags data på vegne af jeres organisation.] |
| Data persistering | [Vejledning: Hvor længe skal data gemmes ift. gældende lovgivning? I et økonomisystem skal faktureringsoplysninger fx opbevares i 5 år jf. Bogføringsloven.] |

## leverandører Af IT

SaaS-leverandører til <Organisation>og deres medarbejdere skal have uddannelse i IT-sikkerhed og er underlagt tavshedspligt ift. arbejdet der udføres for <Organisation>.

Leverandøren er ansvarlig for at implementere tekniske sikkerhedsforanstaltninger så som backup & recovery.

<Organisation> skal sikre at aftalegrundlaget med SaaS-leverandørerne opfylder organisationens behov, og via tilsyn sikre at aftalegrundlaget overholdes. Tilsyn fastlægges for hver leverandør.

[Vejledning: For hver leverandør listet i gennemgangen af IT ovenfor beskrives yderligere jf. nedenstående skabelon.]

### Navn

|  |  |
| --- | --- |
| Beskrivelse | [Vejledning: Beskriv leverandøren overordnet. Hvilke underleverandører benytter de, og hvor er de geografisk placeret.]  |
| Systemer | [Vejledning: På punktform angiv hvilke systemer de leverer som jeres organisation benytter.] |
| Vurdering ift. NIS2 | [Vejledning: Her beskrives hvorvidt den pågældende leverandør er direkte omfattet af NIS2, bliver indirekte omfattet af NIS2 baseret på understøttelse af jeres organisation, eller om leverandøren ikke er omfattet af NIS2.] |
| Databehandler | [Vejledning: Her beskrives hvorvidt den pågældende leverandør er databehandler på vegne af jeres virksomhed, og i hvilken sammenhæng/med hvilket formål.] |

[Vejledning: I kan vælge at angive kendte sårbarheder / mulige forbedringstiltag til sidst efter gennemgang af alle leverandører, eller for hver leverandør. Det kommer an på om de kendte sårbarheder / tiltag gælder på tværs af leverandørerne eller om de er gældende for enkelte leverandører. Eksempler på sårbarheder er: der ikke er indgået aftale med leverandøren om hvordan disse kommunikerer i tilfælde af en krisesituation, eller der ikke er indgået en dækkende databehandleraftale, eller at der er en afvigelse i deres sidste offentliggjorte revisionsrapport, etc.]

| Kendte sårbarheder  | Mulige forbedringstiltag |
| --- | --- |
|  |  |

**Juni 2023**

**Mette Thøgersen**

[Virksomhed] A/S

Marselisborg Havnevej 22, 2.th

8000 Aarhus C

CVR: 25450442

1. Det er dog Energistyrelsen der i sidste ende indplacerer hvert fjernvarmeselskab på rette niveau, baseret på indrapporterede informationer, samt evt. andre ikke specificerede hensyn. [↑](#footnote-ref-2)
2. Klima-, energi- og forsyningsministeriet (KEFM) har udarbejdet Lov om skærpet beredskab i energisektoren, men Bekendtgørelsen er udarbejdet af Energistyrelsen, som hører under KEFM. [↑](#footnote-ref-3)