Skabelon for Hændelseshåndtering

Følgende dokument er en skabelon til udarbejdelse af hændelseshåndtering. Dokumentet er én af flere skabelon-dokumenter, som indgår i det IT-sikkerhedsmateriale, som alle organisationer bør have.

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
* IT-sikkerhedshåndbogen
* OT-leverandørpolitik, og leverandør tjeklister
* Risikostyringspolitik og Risikolog
* Hændelseshåndteringsproces og indrapporteringsskabeloner
* Kriseberedskabspolitik, -planer og -skabeloner

Alle skabelonerne 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-property. 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 header og footer. OBS! Organisation og logo på forsiden er også i en footer.

Versionshistorik for skabelon:

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer |
| 1.0 | 28.01.2025 | MTH | Oprettet første version |
| 2.0 | 12.08.2025 | MTH | Opdateret jf. BKG 260/2025 og ENS vejledninger i hændelseshåndtering. |
| 2.1 | 03.09.2025 | MTH | Tilføjet afsnit 2.1.2 om hændelseslog for væsentlige hændelser. |

Dato | Version X.X

Hændelseshåndtering

termer

|  |  |
| --- | --- |
| Begreb eller forkortelse i teksten | Beskrivelse |
| Problem | Et problem er en underliggende årsag, der giver hændelser. |
| Workaround | En midlertidig løsning. |

Versionshistorik

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer |
| 0.0 | dd.mm.yyyy | INT |  |
|  |  |  |  |

Kontaktpersoner

|  |  |
| --- | --- |
| Fornavn Efternavn (initialer)  Skriv din titel her, fx konsulent  Tlf.: +45 xxxx xxxx  [xxx@domæne.dk](mailto:xxx@domæne.dk)  <Organisation> | Fornavn Efternavn (initialer)  Skriv din titel her, fx konsulent  Tlf.: +45 xxxx xxxx  [xxx@domæne.dk](mailto:xxx@domæne.dk)  <Organisation> |

Indholdsfortegnelse

[1 Indledning 4](#_Toc205900337)

[2 Hændelseshåndtering 5](#_Toc205900338)

[2.1 Vurdering af Hændelse 6](#_Toc205900339)

[2.1.1 Overgang til beredskab 6](#_Toc205900340)

[2.2 Håndtering af hændelse 6](#_Toc205900341)

[2.2.1 Lukning af hændelse 6](#_Toc205900342)

[2.3 Delegering af hændelse 6](#_Toc205900343)

[2.4 Indberetning af hændelse 6](#_Toc205900344)

[2.4.1 Omgående indberetning 8](#_Toc205900345)

[2.4.2 Opfølgende indberetning 8](#_Toc205900346)

[2.4.3 Evalueringsrapport 8](#_Toc205900347)

[2.4.4 Øvelsesevaluering 8](#_Toc205900348)

[3 Problemhåndtering 9](#_Toc205900349)

[3.1 Analyse af problem 9](#_Toc205900350)

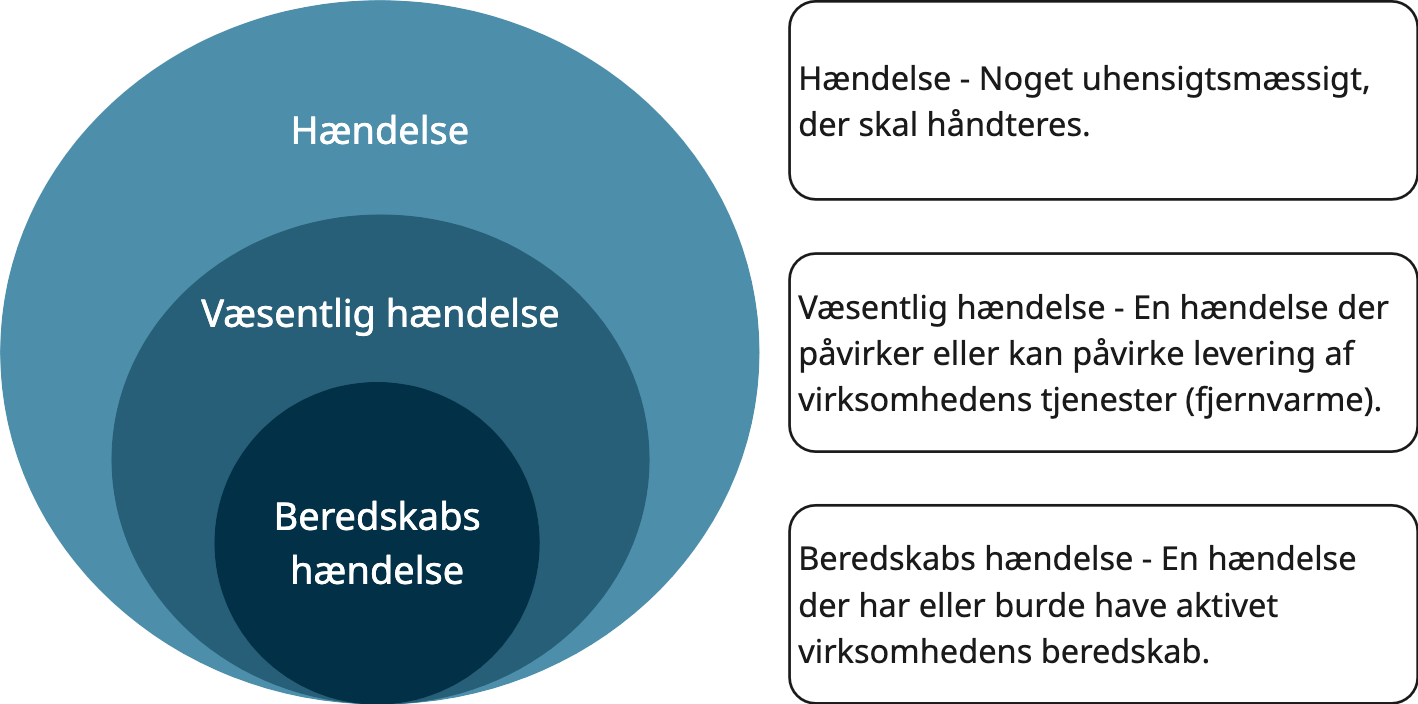
[3.2 Risikovurdering af problem 9](#_Toc205900351)

# Indledning

Dette dokument beskriver hændelseshåndteringsprocedurer for .

Formålet med procedurerne er:

* at sikre en ensartet og prioriteret behandling af hændelser,
* at sikre den nødvendige dokumentation,
* at sikre korrekt og rettidig indrapportere til myndigheder,
* at sikre underretning af berørte personer.



Figur 1: Grafisk repræsentation af hændelser: alle beredskabshændelser er væsentlige hændelser, og alle væsentlige hændelser er hændelser.

En hændelse kan være indenfor:

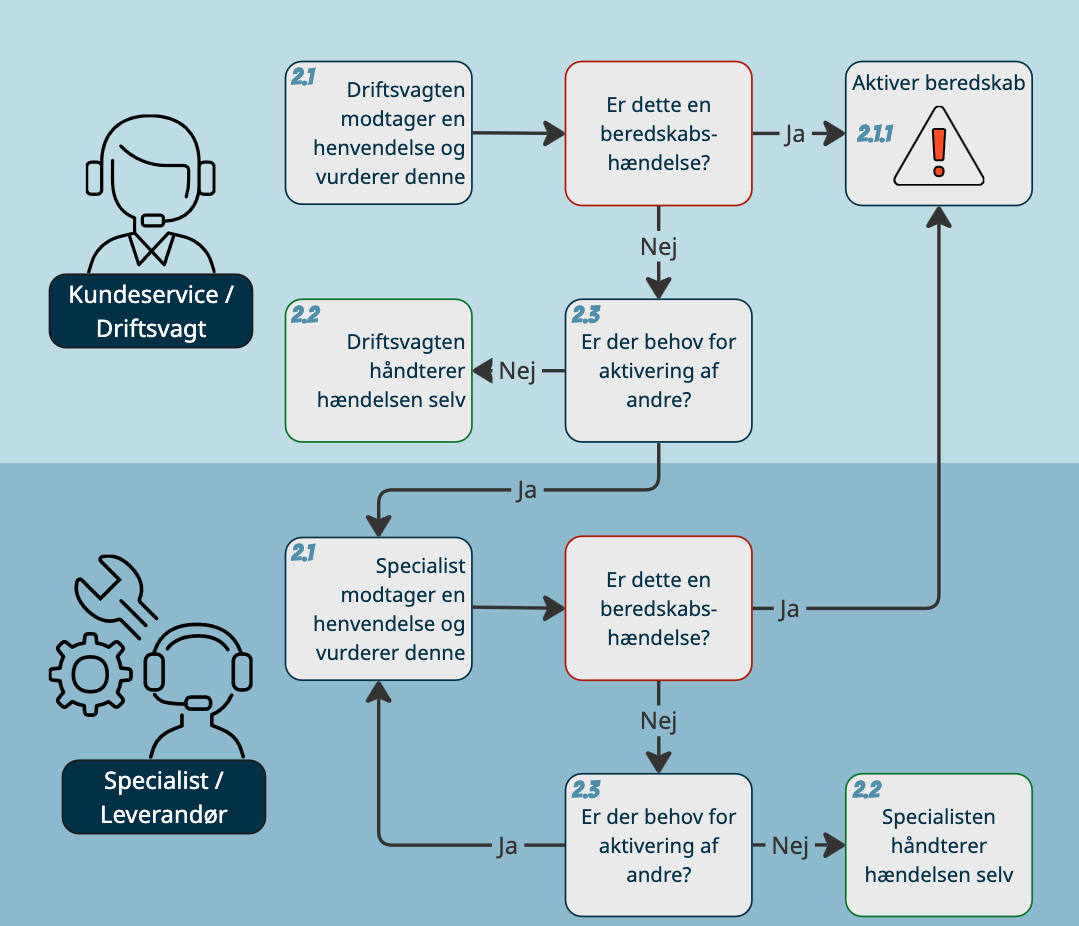
* IT-sikkerhed (fx virus, ransomware, cyberangreb, opdateringsfejl, persondatabrud),
* drift (fx fejl på anlæg eller andet der påvirker produktionen),
* fysisk sikkerhed (fx oversvømmelse, brand, indbrud),
* eller en kombination af disse.

|  |
| --- |
| Hændelser er uhensigtsmæssige situationer |
| * En begivenhed, der har potentiale til i betydelig grad at forstyrre, eller som forstyrrer, leveringen af fjernvarme * 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[[1]](#footnote-2), i fare. |

|  |
| --- |
| Væsentlige hændelser er hændelser |
| * Som enten har haft eller kan komme til at forårsage alvorlige driftsforstyrrelser, herunder:   + Havarier på anlæg   + Arbejdsmarkedskonflikter   + Manglende leverancer * Som enten har forårsaget eller kan forårsage økonomiske tab for virksomheden, som defineret i <Organisation>s risikostyringspolitik bilag B, som en alvorlig økonomisk konsekvens. * Som har påvirket eller kan påvirke andre fysiske personer eller virksomheder ved at forårsage betydelig materiel eller ikke-fysisk skade. * Hvor der er begrundet mistanke om eller kendskab til indbrud, tyveri, sabotage eller spionage. * Hvor et net- og informationssystems fortrolighed, integritet, tilgængelighed og autenticiteten er blevet kompromitteret. |

|  |
| --- |
| Beredskabshændelser er væsentlige hændelser |
| Hændelser, som har aktiveret eller burde have aktiveret virksomhedens beredskabsplaner, herunder:   * Hændelser, der har krævet bistand til situationsudredning, udbedring og genopretning af virksomhedens net- og informationssystemer, herunder fra en it-sikkerhedstjeneste, CSIRT og Energinet. |

# Hændelseshåndtering



Figur 2: Aktivering af hændelseshåndteringsprocedurer og ressourcer.

<Organisation> har en driftsvagt som er tilgængelig 24/7.

Driftsvagten foretager en vurdering af, hvorvidt der er tale om en beredskabshændelse; dvs. en hændelse der skal aktivere beredskabet jf. beredskabsplanen: er der tale om en hændelse der kan håndteres indenfor normal drift, eller skal beredskabsorganisationen indkaldes, og herefter følges beredskabsplanen.

For andre hændelser fortsættes jf. denne procedure.

## Vurdering af Hændelse

Hændelsen undersøges ift. om det er en kendt fejl med en kendt løsning/workaround, eller om der er en kendt procedure for at afhjælpe/løse problemet, fx hvis der er kommet en ny sikkerhedsopdatering, og man ikke kan få lov til at bruge en given service, før man har opdateret sin pc.

### Overgang til beredskab

Ved hændelser der ikke kan håndteres i kendte procedurer, aktiveres kriseberedskabet. Se kriseberedskabsplanen.

### Dokumentation af væsentlig hændelse

Ved væsentlige hændelser som ikke kan løses umiddelbart, og som ikke aktiverer beredskabet, føres der log over forløbet i en hændelseslog. Denne bruges til understøttelse af indberetning til de relevante myndigheder (se afsnit 2.4) og til efterfølgende læring.

## Håndtering af hændelse

Hvis hændelsen kan løses umiddelbart, gøres dette, og sagen lukkes (se afsnit 2.2.1) efter evt. indberetning er foretaget (se afsnit 2.4).

### Lukning af hændelse

Hvis hændelsen er afhjulpet med en workaround, eller den underliggende årsag (problem) ikke er fundet, startes en problemhåndteringsproces, se afsnit 3.

Når en væsentlig hændelse er afhjulpet, udarbejdes en evalueringsrapport som indsendes jf. afsnit 2.4.3.

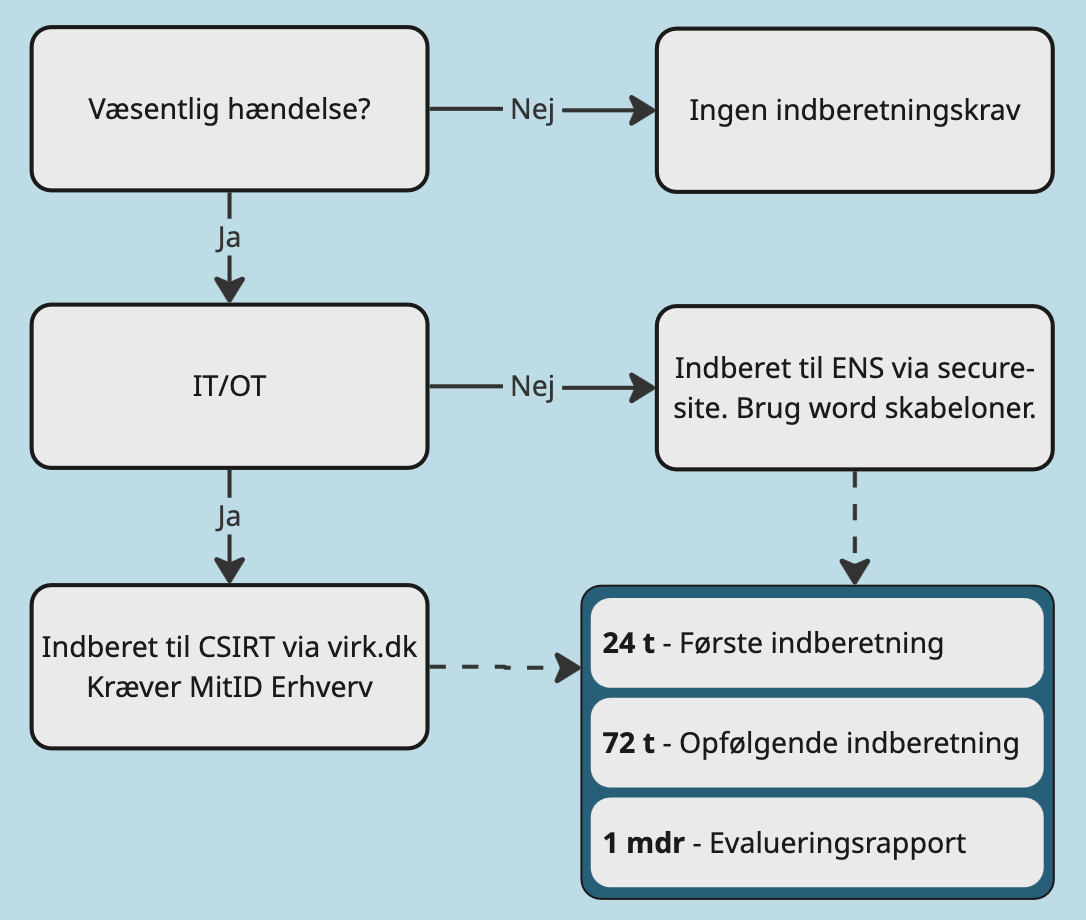
## Delegering af hændelse

Hvis sagen ikke kan løses umiddelbart, tildeles hændelsessagen den specialist (intern eller ekstern), som forventes at kunne afhjælpe hændelsen. Specialister, i form af egne medarbejdere og leverandører, aktiveres jf. kontaktlisten tilknyttet beredskabet.

Hvis den pågældende specialist ikke kan løse sagen, delegeres sagen videre eller eskaleres til beredskab.

## Indberetning af hændelse

Væsentlige hændelser skal indberettes til Energistyrelsen og for IT/OT-hændelser også til CSIRT.



Figur 3: Indrapporterings forpligtigelse jf. Bekendtgørelse om modstandsdygtighed og beredskab i energisektoren, BKG 260/2025. Indtil der er oprettet mulighed for indberetning til Energistyrelsen via virk.dk[[2]](#footnote-3), skal indberetning af væsentlige hændelser der ikke er IT/OT foregå direkte til Energistyrelsen.

| Til hvem? | Kontaktpunkt | Beskrivelse |
| --- | --- | --- |
| Energistyrelsen | Vagttelefon: 5167 4343 | I hastesituationer eller ved hændelser ringes til vagttelefonen. Her aftales hvorledes skemaerne til indberetning overleveres til Energistyrelsen, fx via det lukkede beredskabssite ved brug af skabeloner til indberetning. |
| CSIRT | Virk.dk | Udfyldelse af blanket kræver MitID Erhverv adgang på vegne af virksomheden.  Indberetningen sendes automatisk også til Energistyrelsen og ved persondatabrud til Datatilsynet.  OBS! Det er vigtigt at downloade en kopi af blanketten, når den er indsendt, da alle data slettes i systemet efter 30 dage, så kopien er virksomhedens bevis på, at indberetningen er sendt. |

### Omgående indberetning

Så hurtigt som muligt og senest 24 timer efter virksomheden er blevet bekendt med en væsentlig hændelse, skal der foretages en indledende indberetning til Energistyrelsen og evt. CSIRT.

Hændelsen indberettes med det forhåndenværende fakta. Hvad ved I med sikkerhed på nuværende tidspunkt?

Hvis hændelsen er afsluttet, og der ikke er igangværende problemhåndteringsproces, aftales det med Energistyrelsen, om der udarbejdes yderligere indberetning.

### Opfølgende indberetning

Senest 72 timer efter virksomheden er blevet bekendt med hændelsen, indsendes en opdateret indberetning.

### Evalueringsrapport

Hvis hændelsen *stadig ikke er afsluttet* 1 måned efter første indberetning, skal virksomheden indsende en foreløbig rapport med opdatering på status til Energistyrelsen. Dette kan også være fordi, der stadig er en igangværende problemhåndteringsprocedure for at klarlægge et underliggende problem, som var årsag til hændelsen, se afsnit 3.

Senest 1 måned efter *afsluttet* hændelse, udarbejdes en hændelsesevalueringsrapport, som indberettes på samme vis som de tidligere indberetninger.

### Øvelsesevaluering

Energistyrelsen kan ansøges om at godkende hændelsesevalueringsrapporten som en øvelsesevaluering, hvis konkrete øvelseselementer er blevet afprøvet i forbindelse med håndteringen af hændelsen.

Dette kræver, at der sammen med ansøgningen sendes en opdateret 5-årig øvelsesplan, hvoraf det fremgår, hvornår hændelsen er foregået og hvilke elementer fra beredskabet, som er blevet trænet i forbindelse med håndteringen af hændelsen.

# Problemhåndtering

Aktivering: Problemhåndteringsproceduren kan igangsættes som opfølgning på en eller flere hændelser, som reaktion på indrapporterede sårbarheder eller som afklaring af risici – fx efter en aktivering af beredskabet, hvor noget er gået helt galt, og man frygter, at det vil gøre det igen, med mindre noget grundlæggende bliver fikset.

Ressourcer: Problemteamets sammensætning fastsættes af ledelsen, og sammensættes af interne og eksterne personer med de faglige kompetencer nødvendigt for problemanalysen.

## Analyse af problem

Problemet analyseres fx ved, at teamet kigger i logs og undersøger, om der er noget, der ser ud til at danne et mønster. Problemteamet indsamler alle de oplysninger om problemet, som de har brug for i det videre arbejde: Teori om hvad der er galt, hvornår det begyndte, resultat af test, de umiddelbare konsekvenser osv.

Problemteamet udarbejder en sag til videre risikovurdering. Problemsagen skal indeholde beskrivelse af trussel, sårbarhed, sandsynlighed og konsekvens, samt forslag til mulige mitigerings tiltag inkl. økonomi.

## Risikovurdering af problem

Problemsagen indrapporteres som risiko til risikoorganisationen, hvor den vurderes på baggrund af risikostyringspolitikkens bilag B, prioriteres og håndteres jf. samme politik bilag C.

Risikoorganisationen behandler problemsagen og fastlægger en handlingsplan.

1. BKG 260/2025 beskæftiger sig kun med net- og informationssystemer som direkte eller indirekte benyttes til levering af virksomhedens tjeneste fx fjernvarme. [↑](#footnote-ref-2)
2. Virk.dk indberetning forventes at opdateres til at kunne dække alle typer hændelser i løbet af 2025, hvorefter denne procedure opdateres. [↑](#footnote-ref-3)