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 Hændelseslog
* 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.

Versions historik for skabelon:

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer |
| 1.0 | 28.01.2025 | MTH | Oprettet første version |

Dato | Version X.X

Hændelseshåndtering

termer

|  |  |
| --- | --- |
| Begreb eller forkortelse i teksten  | Beskrivelse |
| Workaround | En midlertidig løsning |
|  |  |

Versions- og Godkendelseshistorik

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Dato | Ansvarlig | Ændringer | Godkendt |
| [0.0] | [dd.mm.yy] | [INT] |  | [dato / navn] |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Kontaktpersoner

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

Indholdsfortegnelse

[1 Indledning 3](#_Toc189649422)

[1.1 Definitioner 3](#_Toc189649423)

[2 Hændelseshåndtering 3](#_Toc189649424)

[2.1 Registrering af hændelse 4](#_Toc189649425)

[2.2 Håndtering af hændelse 4](#_Toc189649426)

[2.3 Delegering af hændelse 5](#_Toc189649427)

[2.4 Lukning af hændelse 5](#_Toc189649428)

[2.5 Overgang til beredskab 5](#_Toc189649429)

[3 Problemhåndtering 5](#_Toc189649430)

[3.1 Analyse af problem 6](#_Toc189649431)

[3.2 Risikovurdering af problem 6](#_Toc189649432)

[3.3 Lukning af problem 6](#_Toc189649433)

[4 Indberetning 6](#_Toc189649434)

[4.1 Sikkerhedshændelser 7](#_Toc189649435)

[4.2 Persondatabrud 7](#_Toc189649436)

[5 Underretning 7](#_Toc189649437)

[5.1 Sikkerhedshændelser 8](#_Toc189649438)

[5.2 Persondatabrud 8](#_Toc189649439)

[Bilag A – Prioritering 1](#_Toc189649440)

# 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.

## Definitioner

| Definition: Hændelse |
| --- |
| En hændelse er noget uhensigtsmæssigt, der skal håndteres. |

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.

| Definition: Krise |
| --- |
| En hændelse der enten ikke kan håndteres via kendte procedurer, eller har så store konsekvenser at den eskaleres til kriseberedskab. |

| Definition: Problem |
| --- |
| Et problem er en underliggende årsag der giver hændelser. |

# Hændelseshåndtering

[Vejledning: Det er forskelligt i den enkelte organisation, hvordan fejl og hændelser indberettes. I forsyningsvirksomheder er der normalt en Driftsvagt, som er bemandet 24/7, i andre virksomheder kan det være en kundeservice, eller helpdesk eller noget helt tredje. Det vigtige her er, at hændelser (inkl. it-hændelser) håndteres i de allerede etablerede processer for håndtering af fejl og driftsforstyrrelser.
Med ”sagsbehandlingssystem” menes den proces eller den it-løsning, hvor I normalt registrerer fejl og driftsforstyrrelser, og som bruges til at fordele opgaver og følge op på status. Hvis I ikke har en sådan proces eller løsning er det noget I skal have etableret, fx vha. en Hændelseslog. Hændelseslog skabelonen er et excel-ark, og den simpleste form for opsamling på hændelser og nærved-hændelser. Dette kan være fyldestgørende for en lille organisation, men I vil nok hurtigt opleve, at I ønsker et bedre værktøj til opsamling og fordeling af opgaver i forbindelse med hændelser.]

Her beskrives jeres hændelseshåndtering overordnet: fx <Organisation> har en driftvagt som er tilgængelig 24/7. Driftvagten er understøttet af serviceaftale med leverandør X og Y.]

## Registrering af hændelse

1. Kundeservice/Driftsvagt bliver opmærksomme på hændelsen. Der er som regel tre kilder til identifikation af en hændelse: brugerindmeldte (kunder, medarbejdere eller leverandører), eksterne kilder (CyberCERT, SektorCERT etc.) og tekniske hændelser (monitorering)
2. Kundeservice/Driftsvagt opretter en hændelses-sag i <Organisation>s sagsbehandlingssystem/hændelseslog og noterer alle de oplysninger om hændelsen, som de har brug for i det videre arbejde: fx hvad brugeren oplever, hvornår det begyndte, de umiddelbare konsekvenser osv.
3. Kundeservice/Driftsvagt benytter den aftalte klassifikation (se Bilag A) til at bestemme det hvor tidskritisk det er at få afhjulpet hændelsen. Prioriteten er som regel udtrykt på en skala, fx ”lav”, ”normal” eller ”høj”. Ved ”høj” skal man overveje om der er tale om en krise, se afsnit 2.5.

## Håndtering af hændelse

Kundeservice/Driftsvagt undersøger 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.

Hvis Kundeservice/Driftsvagt kan afhjælpe hændelsen under 1. kontakt med brugeren eller alarmen som gav hændelsen, løses hændelsen med det samme, og løsning/workaround registreres, og sagen lukkes (se afsnit 2.4).

## Delegering af hændelse

Hvis sagen ikke kan løses umiddelbart, tildeles hændelsessagen den instans/person/afdeling/partner/leverandør som forventes at kunne afhjælpe hændelsen. Efter delegering kan prioritering opdateres baseret på yderligere viden.

Den ansvarlige instans arbejder videre på sagen jf. prioritet.

Der er altid kun én enhed som er tildelt en hændelsessag ad gangen. Hvis de ikke kan løse sagen, delegeres sagen videre eller eskaleres til beredskab.

## Lukning af hændelse

Når hændelsen er afhjulpet, opdateres sagen med de oplysninger, som man har besluttet er nødvendige og lukkes. Hvis hændelsen er afhjulpet med en workaround, eller den underliggende årsag (problem) ikke er fundet, startes en problemhåndteringsproces, se afsnit 3.

## Overgang til beredskab

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

# Problemhåndtering

[Vejledning: Det er vigtigt at problemhåndteringen og værktøjer til udforskning af problemer følger andre processer mest mulig. Det vil dog typisk kræve en dybere teknisk forståelse at finde frem til den underliggende årsag (problemet), hvorfor det ikke forventes at det fx kan være en kundeservice funktion der varetager denne opgave. Den rolle eller det team der undersøger et problem, skal have de rette kompetencer, adgange og tid til at undersøge, belyse og evt. løse problemet. Ved problemer der ikke kan løses umiddelbart, indrapporteres det til risikostyringsorganisationen og prioriteres ind baseret på en risikovurdering.
Det vil være fordelagtigt, hvis den samme proces eller it-løsning som benyttes til registrering af hændelser også benyttes til dokumentation af problemer.]

En gang i kvartalet/hvert halve år/årligt laver Problemteamet en gennemgang af registrerede hændelser, med henblik på at vurdere om der fx er mange hændelser der omhandler det samme, og der derfor kunne være noget mere grundlæggende galt. Gennemgangen af registrerede hændelser kan også foretages 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.

Problemteamet fastsættes af ledelsen, og sammensættes af personer med de faglige kompetencer nødvendigt for problemanalysen.

## Analyse af problem

1. Problemteamet kigger i logs og undersøger om der er noget der ser ud til at danne et mønster. Problemteamet opretter eller opdaterer en problem-sag i sagsbehandlingssystemet og noterer 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.
2. Problemteamet benytter den aftalte klassifikation (se risikovurderingspolitikken) til at bestemme konsekvens, hvis problemet ikke bliver afhjulpet, samt sandsynligheden for at konsekvensen vil indtræffe.
3. Problemteamet undersøger om det er en kendt fejl med en kendt løsning / workaround, eller om der er en kendt procedure for at afhjælpe/løse problemet.

## Risikovurdering af problem

Problemsagen indrapporteres som risiko til risikoorganisationen, hvor den prioriteres og håndteres. Problemsagen skal indeholde beskrivelse af trussel, sårbarhed, sandsynlighed og konsekvens, samt forslag til mitigering.

Risikoorganisationen behandler problemsagen og fastlægger en handlingsplan.

## Lukning af problem

Når problemet er afhjulpet, opdateres sagen med de oplysninger, man har besluttet er nødvendige og lukkes.

# Indberetning

Visse hændelser og nærved-hændelser skal indrapporteres til forskellige myndigheder og virksomheder i sektorberedskabet. Indberetning foregår via virk.dk[[1]](#footnote-2). Indberetningsløsningen på virk.dk kræver at personen der indberetter, har en medarbejderidentitet (MitID Erhverv identitet).

## Sikkerhedshændelser

[Vejledning: For virksomheder på niveau 2 og over gælder det at de skal indberette hændelser og væsentlige cybertrusler til Energistyrelsen og CSIRT, samt hvis man er en del af el-, gas- eller brintsektoren, til Energinet. For virksomheder på niveau 1 er der ikke krav om indberetning.]

Hændelser der har en væsentlig indvirkning (ift. drift, økonomi, materiel, ikke-fysisk skade) eller aktiverer virksomhedens beredskab, på virksomhedens tjenester skal indrapporteres indenfor 24 timer til:

* Energistyrelsen
* CSIRT – ved cyberhændelser
* Energinet – for virksomheder i el-, gas- eller brintsektoren

Indenfor 72 timer underrettes Energistyrelsen om status for hændelsen.

Senest én måned efter første hændelsesindberetning, skal virksomheden sende en hændelsesrapport til Energistyrelsen.

Hændelser, hvor der er begrundet mistanke om eller kendskab til indbrud, tyveri, sabotage og spionage skal meldes til politiet.

## Persondatabrud

Ved hændelser hvori der indgår brud på persondata, skal den dataansvarlige foretage indberetningen til Datatilsynet uden unødig forsinkelse og senest 72 timer efter denne er blevet bekendt med et persondatabrud.

Ifølge databeskyttelsesforordningen gælder der en generel forpligtelse for dataansvarlige til at anmelde brud på persondatassikkerheden til Datatilsynet, *medmindre det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.*

En risiko for fysiske personers rettigheder og frihedsrettigheder omfatter bl.a. diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede.

# Underretning

Visse hændelser skal underrettes til virksomheder og personer der er berørt af hændelsen. Virksomheder kan vælge at underrette bredere og i flere tilfælde end der er kravsat, baseret på hændelsens karakter og virksomhedens forretningsstrategi og -mål.

## Sikkerhedshændelser

Virksomheder skal uden unødigt ophold underrette modtagere af deres tjenester, om væsentlige cybertrusler eller hændelser, der negativt påvirker eller har potentiale til negativt at påvirke modtagerne af virksomhedens tjenester.

Underretning af modtagerne af <Organisation>s tjenester foregår via driftsinfo på hjemmesiden, samt udsendelse af driftsinformation via sms til registrerede telefonnumre.

## Persondatabrud

Underretning af de registrerede skal (som minimum) ske, hvis bruddet sandsynligvis vil indebære en høj risiko for deres rettigheder eller frihedsrettigheder. Kommunikationen skal indeholde information om hvad der er sket, samt omfang og tidsforløb, samt information om <Organisation>s håndtering af persondatabruddet.

# Bilag A – Prioritering

[Vejledning: I dette bilag skal I fastsætte jeres egne prioriteringsværdier for hændelser og problemer. Der er indsat eksempler med gul overstregning, men de er blot eksempler og bør fastsættes ud fra jeres forretning. Der er her valgt tre konsekvenskategorier til vurdering og fastsættelse af prioritering af hændelser: produktion, cyber og persondata. Der kan sagtens indføres flere eller andre.]

Prioritering af hændelser i forhold til konsekvenser for organisationen selv, modtagere af deres tjenester og de personer om hvem der er gemt data. Nedenfor er defineret den hændelsesprioritering, som benyttes i .

| Prioritering af hændelser |
| --- |
| Prioritet | Reaktionstid | Produktion | Cyber | Persondata |
| Høj | Omgående | Opholdende effekt på produktion100+ berørte husstande | Aktivt angreb eller anden kriminalitet | 100+ berørte personer eller følsomme / fortrolige data |
| Normal | 2 arbejdsdage | Mindre opholdende effekt på produktion10+ berørte husstande | Behandling af kritiske sårbarheder fundet ved monitorering eller via sikkerheds-tjeneste. | 10+ berørte personer eller almindelige persondata |
| Lav | 10 arbejdsdage | Ingen opholdende effekt på produktion<10 berørte personer/husstande | Behandling af sårbarheder fundet ved monitorering eller via sikkerheds-tjeneste. | <10 berørte personer eller offentlige persondata |

1. Indberetning via virk.dk: <https://virk.dk/myndigheder/stat/Digitaliseringsstyrelsen/selvbetjening/Indberetning_af_brud_paa_sikkerhed/> Det forventes pt at indberetning til Energistyrelsen, CSIRT, Energinet og Datatilsynet alle vil kunne foretages via virk.dk. [↑](#footnote-ref-2)