**Skabelon - Beredskabsplan for informationssikkerhed**

**Beredskabsplan for informationssikkerhed**

**for**

[*xxx kommune*]

|  |  |
| --- | --- |
| Version | *Skabelon* |
| Dato |  |
| Godkendt af |  |

# Før du går i gang - vejledning til brug af skabelonen

Denne skabelon er bygget op over en generisk struktur med generel information og hints, vejledende tekstforslag og tekst og tabeller, som vil dække de flestes behov. Typografien i skabelonen er søgt anvendt på en måde, der letter opgaven med at udarbejde beredskabsplanen.

Drejebogen til håndtering af beredskab for informationssikkerhed gennemgår terminologien bag beredskabet og hvordan man lettest kommer i gang. Er principperne bag beredskabsarbejdet kommet ind under huden, vil man relativt hurtigt kunne udarbejde en første version af en plan.

Det kan ikke anbefales, at man bygger en beredskabsplan ud fra nærværende skabelon ved at bruge ’søg- og-erstat’-funktionen.

|  |  |
| --- | --- |
| **Typografi** | **Anvendelse i praksis** |
| Normal tekst | Kan anvendes som udgangspunkt for lokale beskrivelser og andet indhold, men bør erstattes med organisationens eget sprog. |
| [Gråtonet tekst i firkantede parenteser] | Generel information, hints eller anden hjælp til at udfylde skabelonen. Teksten bør slettes, inden planen bliver udgivet lokalt. |
| [*Kursiveret tekst i firkantede parenteser*] | Tekstforslag og inspiration til konkrete indholdselementer, som skal erstattes med lokalt indhold. |

## Indholdsfortegnelse

[Før du går i gang - vejledning til brug af skabelonen 2](#_Toc106783948)

[Indholdsfortegnelse 3](#_Toc106783949)

[1. Om beredskabsplanen for informationssikkerhed 4](#_Toc106783950)

[2. Beredskabsorganisation 4](#_Toc106783951)

[2.1 Roller og ansvar 4](#_Toc106783952)

[2.2 Kontaktlister 5](#_Toc106783953)

[3. Aktivering og eskalering 6](#_Toc106783954)

[3.1 Eskalering 7](#_Toc106783955)

[3.2 Kommunikation 7](#_Toc106783956)

[3.3 Nødplaner for systemer og deres forretningsunderstøttelse 8](#_Toc106783957)

[3.4 Retablering 8](#_Toc106783958)

[4. Evaluering af beredskab 9](#_Toc106783959)

[5. Vedligeholdelse af beredskabsplanen 9](#_Toc106783960)

[5.1 Distribution og opbevaring 9](#_Toc106783961)

[6. Bilag 10](#_Toc106783962)

[6.1 Kontaktlister Bilag A 10](#_Toc106783963)

[6.2 Overblik over nødplaner Bilag B 10](#_Toc106783964)

[6.3 Nødplan Bilag Bx.x 10](#_Toc106783965)

[6.4 Action cards Bilag C 10](#_Toc106783966)

[6.5 Beredskabslog Bilag D 10](#_Toc106783967)

# 1. Om beredskabsplanen for informationssikkerhed

Beredskabsplanen for informationssikkerhed er den operationelle udmøntning af <xxx *kommunes*> beredskabsstrategi for informationssikkerhed, hvor strategien fastsætter de overordnede mål og rammer for styringen af beredskabet, mens planen beskriver de operative tiltag og handlinger, der er relevante i en beredskabssituation.

Beredskabsplanen for informationssikkerhed indgår som en del af <xxx *kommunes*> generelle beredskabsplan.

Beredskabsplanen for informationssikkerhed skal afprøves og revideres med faste intervaller.

Kontaktlister, nødplaner, action cards og beredskabslog er vedlagt som bilag.

[Der er udarbejdet "Skabelon - beredskabsstrategi for informationssikkerhed", som kan bruges sammen denne plan. Skabelonen er tilgængelig på KL Videncenter.

De vedlagte bilag findes som selvstændige skabeloner, så de kan udfyldes digitalt]

# 2. Beredskabsorganisation

Informationssikkerheds beredskabsorganisationen er en del af den samlede beredskabsorganisation for [xxx kommune].

[Organisationen kan vælge at fastholde den eksisterende organisationsstruktur, eller oprette en ny organisation særligt til formålet med beredskabet for informationssikkerhed. I mange tilfælde vil det være mest hensigtsmæssigt at tage udgangspunkt i den eksisterende organisationsstruktur, da kommunikation, arbejdsgange m.v. således allerede er indøvet.

Størrelsen af beredskabsorganisationen afhænger af organisationens it-anvendelse og omfanget af opgaver i forbindelse med it-driften, som varetages internt i organisationen. Hvis organisationen selv varetager driften af en stor mængde it-systemer, vil der være behov for en tilsvarende stor beredskabsorganisation.]

Hvis det er aftalt, at eksterne leverandører varetager opgaver i forbindelse med en beredskabssituation, bør dette fremgå af beskrivelsen, så det er klart, hvilke opgaver, der udføres internt og eksternt.]

## 2.1 Roller og ansvar

Rollerne i beredskabsorganisationen og de opgaver, som er aftalt skal udføres i en beredskabssituation, er præciseret herunder for at synliggøre en optimal tildeling af rollerne i forhold til organiseringen og kompetencerne i [*xxx kommune*].

[Som udgangspunkt beskrives kun organisationens egen beredskabsorganisation, da det antages, at eventuelle leverandører selv varetager styringen i egne organisationer. Hvis der er aftalt særlige forpligtelser med leverandøren, bør disse beskrives nedenfor.

KOMBIT har eget beredskab, for de systemer de varetager.

Husk at angive stedfortrædere for de enkelte roller. Dette gøres i den efterfølgende kontaktliste.

Et eksempel på typisk beredskabsmæssige roller og opgaver er angivet nedenfor. En person kan dække flere roller, hvis det vurderes nødvendigt. Ligeledes kan en rolle deles mellem flere personer, hvis situationen kræver det. Dette skal beskrives i situationen, så opgaveansvaret er klart.]

|  |  |
| --- | --- |
| **Rolle** | **Opgaver** |
|  |  |
| Beredskabsleder | *[udpeges blandt chefgruppen - er ansvarlig for eskalering og deeskalering af beredskab, for indkaldelse af ad hoc bemanding, for kommunikation til eksterne og for orientering af topledelsen]* |
| Koordinator Sekretær | *[er ansvarlig for indsamling af informationer og for koordinering af indsatser.]* *[er ansvarlig for dokumentation af al kommunikation ud og ind af beredskabsgruppen, samt føring af beredskabsloggen.]* |
| Kommunikationsansvarlig | *[er ansvarlig for information / kommunikation med kommunens ansatte. Afhængig af situationen vil kommunikation til borgere, offentlighed og presse være i opgave efter aftale med beredskabslederen]*  |
| Ad hoc | *[Beredskabslederen indkalder efter behov personer fra organisationen. Det kan f.eks. være** *DPO, der altid skal inddrages i forbindelse med brud på persondatalovgivningen*
* *fagchefer for berørte områder, der kan sørge for praktisk iværksættelse af nødplaner*
* *I det omfang It-chef ikke allerede har en rolle i beredskabet, bør denne inddrages, hvor det vurderes relevant]*
 |

[Man kan med fordel anvende action cards, hvor ansvar, opgaver og checklister til de forskellige roller er beskrevet, så de nemt kan anvendes i en beredskabssituation.
Skabelon ”Action cards Bilag C" med udfyldte eksempler er tilgængelig på KL’s Videnscenter]

## 2.2 **Kontaktlister**

Kontaktlisterne er udgangspunktet for mobilisering af beredskabsorganisationen.

Kontaktinformationen er dokumenteret i Bilag A.

[Kontaktlisterne bør omfatte hele beredskabsorganisationen, men også relevante kontaktpersoner i den øvrige forretning samt eksterne leverandører og kontakter.
Skabelon for "Kontaktlister Bilag A" er tilgængelig på KL’s Videnscenter]

**2.3 Mødested**

Når beredskabet indkaldes, skal de mødes på:

*[xxxxxx kontor.]*

Alternativt findes der en anden passende lokation at mødes, afhængig af beredskabsledelsens nuværende lokation.

Når beredskabsledelsen er samlet, besluttes hvor en evt. kommandocentral oprettes. Mulige lokationer er:

*[xxxxxx kontor.*

*Ledigt mødelokale på xxxxx Rådhus.]*

# 3. Aktivering og eskalering

Beredskabet for informationssikkerhed træder i kraft, når en hændelse ikke kan håndteres inden for rammerne af [*xxxx kommunes*] normale processer og arbejdsgange.

Det er lederen af beredskabet der tager initiativ til aktivering efter vurdering af hændelser eller på opfordring af topledelse eller eksterne indberetninger.

[Kriterierne for aktivering af beredskabet skal defineres og beskrives, så det er klart, under hvilke omstændigheder beredskabet skal aktiveres, og hvem der kan aktivere det.

Bemærk: Hændelser, hvor løsningen er kendt, og den normale drift kan genoprettes inden for den fastsatte tidsgrænse, bør normalt ikke medføre aktivering af beredskabet.]

*[Aktivering og mobilisering iværksættes, hvis der er sikkerhed for, at et af nedenstående kriterier er opfyldt eller vurderes i risiko for at blive opfyldt:*

1. ***Tidsmæssig udstrækning af hændelsen***

*Hvis det står klart, at en hændelse ikke kan håndteres og løses inden for de ramte aktivers serviceaftaler (SLA’er) for almindelig udbedring af hændelser, kan det være en indikation af en krise, der kræver aktivering af beredskabsplanen.*

*Hvis der er risiko for, at en hændelse ikke kan håndteres og løses inden for rimelig tid (vurderet ud fra et forretningsmæssigt behov), er der utvivlsomt tale om en krise, der kræver aktivering af beredskabsplanen.*

1. ***Graden af påvirkning***

*Hvis en stor del af infrastrukturen (servere, netværk etc.) er berørt af en hændelse, kan det være en indikation af en krise, der kræver aktivering af beredskabsplanen.*

*Det samme gør sig gældende, hvis en stor procentdel af medarbejdernes mulighed for at udføre deres arbejde er umiddelbart berørt af en hændelse.*

*Hvis der er mistanke om, at der er sket brud på persondatasikkerhed, kan det kræve en hel eller delvis aktivering af beredskabsplanen. Dette afhænger af årsag til bruddet og alvoren af denne.]*

## 3.1 Eskalering

Hvis eskaleringsprocedurerne resulterer i, at beredskabsplanen træder i kraft, skal følgende retningslinjer følges:

* Beredskabslederen, eller dennes stedfortræder, indkalder og aktiverer beredskabsplanen
* Beredskabsloggen Bilag D startes op og alle beslutninger dokumenteres løbende
[Skabelon for "Beredskabslog Bilag D” er tilgængelig på KL’s videnscenter.]

Processen kan bestå af følgende aktiviteter:



[Når beredskabet mødes, kan følgende spørgsmål overvejes ift. at afdække situationen:

* Hvilke systemer er påvirket af hændelsen?
* Er systemerne utilgængelige?
* Hvilke processer/behandlingsaktiviteter er påvirket af systemernes utilgængelighed?
* Hvad er omfanget af skaden?
* Hvad er den estimerede tidsramme for nøddriften af systemer?
* Hvad er status på situationen ud fra de processer/behandlingsaktiviteter, der anvender de påvirkede systemer og tidsrammen for nøddrift]

## 3.2 Kommunikation

Et af hovedelementerne til en succesfuld styring af en beredskabssituation er at sikre en passende kommunikation til alle relevante interessenter, i rette tid og med det rette indhold.

Den kommunikationsansvarlige bør udarbejde en kommunikationsplan, der modsvarer beredskabssituationen. I kommunikationsplanen angives hvem modtageren er, hvilken kommunikation der skal gives, hvem der godkender kommunikationen, hvilken kanal der skal anvendes samt tidspunkt for kommunikationen.
Det vil oftest være formanden for beredskabet, der skal godkende kommunikationen.

Kommunikation og kommunikationsplan kan udarbejdes med inspiration fra nedenstående model:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Besked** | **Effekt** | **Modtager** | **Godkender** | **Kanal** |
| Beskeden varierer afhængig af situationen.Når der kommunikeres, skal følgende inkluderes i kommunikationen:* Skadens type
* Skadens omfang
* Skadens varighed
 | Det skal vurderes hvad effekten af kommunikationen skal være. Eks.:* Skabe arbejdsro
* Informere interessenter
* Få modtager til at gøre noget bestemt
* Bruge et midlertidigt system
* Sætte forretningsnødplaner i værk m.m.
* Informere borgere hvis der er sket brud på persondatasikkerhed
* Informere medier
 |  Systemejere |  Koordinator | E-mail Telefon Møder |
| Medarbejdere | Beredskabsleder | E-mail Intranet |
| Ledelsen | Beredskabsleder | Møder Telefon |
| Borgere | Beredskabsleder | HjemmesideE-mailTelefon |
| Medier | Beredskabsleder | PressemeddelelseE-mail |

## 3.3 Nødplaner for systemer og deres forretningsunderstøttelse

Nødplanerne er grundlaget for at holde forretningskritiske processer og behandlingsaktiviteter i gang under beredskabssituationen.

Nødplanerne er udarbejdet af de ansvarlige systemejere i samarbejde med de forretningsejere, der anvender de enkelte systemer. Nødplanerne tager afsæt i de udarbejdede konsekvens- og risikovurderinger for behandlingsaktiviteter og deres understøttende it-systemer. Nødplaner iværksættes af beredskabslederen i samarbejde med relevante fagchefer.

Nødplaner er dokumenteret i Bilag B (oversigt) og Bx.x – Bx.x.

[Det er vigtigt, at nødplanerne er operationelle og tydelige, samt målrettet de enkelte aktiviteter og forretningsprocesser.
Skabeloner for "Nødplaner Bilag B og Bx.x" er tilgængelig på KL’s videnscenter.]

## 3.4 Retablering

Retableringsplanerne er grundlaget for den strukturerede løsning / afværgning af beredskabssituationens konsekvenser / årsag.

Retableringsplanerne er udarbejdet af de drifts ansvarlige ud fra dokumentation af infrastruktur og systemer.

Retablering iværksættes og koordineres af beredskabslederen/koordinatoren.

[Retableringsplaner er til forskel fra nødplaner målrettet “Root Cause” og ikke de enkelte forretningsprocesser.

Det er vigtigt, at retableringsplaner er operationelle og tydelige. Indholdet i disse afhænger af kommunens it-anvendelse og graden af outsourcing.]

**3.4 Afslut beredskab**

Beredskabslederen beslutter, om beredskabet kan afsluttes, så snart normaldrift er blevet reetableret. Denne beslutning tages i samråd med systemejere og resten af beredskabet.
Når beredskabet afsluttes, afsluttes beredskabsloggen.

# 4. Evaluering af beredskab

Beslutninger og handlinger fra beredskabshændelsen evalueres på et møde organiseret af beredskabslederen.

Formålet med dette møde er at evaluere på beredskabsindsatsen for at identificere områder, hvor processen kan blive forbedret.
Der udarbejdes en beredskabsrapport over beredskabshændelsen.

["Skabelon til Beredskabsrapport" findes på KL’s videncenter]

5. Vedligeholdelse af beredskabsplanen

Beredskabsplanen for informationssikkerhed skal opdateres mindst en gang om året i forlængelse af den årlige afprøvning. Desuden skal den opdateres efter evalueringen af en beredskabssituation.

Planen skal sammenholdes med de erfaringer der er opsamlet i forbindelse med en sikkerhedshændelse.

Planen bør desuden opdateres, hvis der sker væsentlige ændringer i it-anvendelsen (f.eks. en ny leverandør), beredskabsorganisationen m.v.

**Versionshistorik**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Dato** | **Ansvarlig** | **Ændringsbeskrivelse** | **Godkendt** | **Distribueret** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 5.1 Distribution og opbevaring

Beredskabsplanen for informationssikkerhed skal opbevares, så den altid er tilgængelig i en beredskabssituation. Hvert medlem af beredskabsorganisationen bør opbevare et fysisk eksemplar af planen. Den vedligeholdelsesansvarlige er ansvarlig for distribution af opdateringer til alle modtagere af planen.

# 6. Bilag

## 6.1 Kontaktlister Bilag A

Find bilaget her: <https://videncenter.kl.dk/media/50630/skabelon-kontaktlister-bilag-a.xlsx>

## 6.2 Overblik over nødplaner Bilag B

Find bilaget her: <https://videncenter.kl.dk/media/50627/skabelon-overblik-over-noedplaner-bilag-b.docx>

## 6.3 Nødplan Bilag Bx.x

Find bilaget her: <https://videncenter.kl.dk/media/50631/skabelon-noedplan-bilag-bx.docx>

## 6.4 Action cards Bilag C

Find bilaget her: <https://videncenter.kl.dk/media/50636/action-cards-bilag-c.docx>

## 6.5 Beredskabslog Bilag D

Find bilaget her: <https://videncenter.kl.dk/media/50637/beredskabslog.docx>

|  |  |
| --- | --- |
|  |  |
|  |   |