Skabelon - beredskabsstrategi for informationssikkerhed

**Beredskabsstrategi for informationssikkerhed**

**for
[*xxx kommune*]**

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

# Før du går i gang - vejledning til 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 beredskabsstrategien.

Skabelonen er beskrevet ud fra den antagelse, at kommunen ikke har en tidligere beredskabsstrategi at bygge på.

|  |  |
| --- | --- |
| **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 skabelonen 2](#_Toc517094760)

[1 Formål med beredskabsstrategien 4](#_Toc517094761)

[2 Udgangspunkt for beredskabet for informationssikkerhed 5](#_Toc517094762)

[3 Omfang og anvendelsesområde 5](#_Toc517094763)

[4 Afgrænsning og antagelser 6](#_Toc517094764)

[5 Målsætning for beredskabet for informationssikkerhed 6](#_Toc517094765)

[6 Roller og ansvar 7](#_Toc517094766)

[7 Eksterne leverandører 8](#_Toc517094767)

[8 Beredskabsscenarier 8](#_Toc517094768)

[9 Implementering af beredskabet for informationssikkerhed 9](#_Toc517094769)

1 Formål med beredskabsstrategien

Formålet med denne beredskabsstrategi for informationssikkerhed er at fastlægge de overordnede rammer for [*xxxx kommunes*] arbejde med og implementering af beredskabet for informationssikkerhed. Strategien indeholder en beskrivelse af det ønskede niveau for beredskabet og er udtryk for [*xxxx kommunes*] forventninger og krav til hertil.

Den operationelle udmøntning af strategien beskrives særskilt i en beredskabsplan for informationssikkerhed.

Nedenstående figur viser hierarkiet mellem de forskellige dokumenter i beredskabet for informationssikkerhed.



Operationelt niveau

Taktisk niveau

Strategisk niveau

[På KL og KOMBITs videncenter findes "Skabelon - beredskabsplan for informationssikkerhed" og "Skabelon - Nødplan for it-system" (forretningsnødplan)]

[Opdelingen af beredskabet i en strategi og en plan med et operationelt sigte skyldes hensynet til det løbende vedligeholdelsesarbejde, da strategien som udgangspunkt er mere langsigtet og dermed mindre vedligeholdelseskrævende end de operationelle planer.]

Beredskabet er ledelsens ansvar, og strategien godkendes af ledelsen.

# 2 Udgangspunkt for beredskabet for informationssikkerhed

Beredskabet for informationssikkerhed er udarbejdet med udgangspunkt i en risikovurdering, som er baseret på de forretningsmæssige behov eller krav.

Beredskabsplanen for informationssikkerhed skal være koordineret med den samlede beredskabsplan for *[xxx kommune],* herunder benævnt øvrigt beredskab.

Sammenhængen mellem de forskellige elementer i beredskabet er illustreret i figuren nedenfor.

**Beredskab for informationssikkerhed**

**Øvrigt beredskab**

I

I

I

I

I

I

I

I

I

I

I

I

I

I

I

I

I



# 3 Omfang og anvendelsesområde

Beredskabet for informationssikkerhed skal skabe sikkerhed for, at *[xxx kommune]* kan genskabe en normal driftssituation hurtigt, sikkert og i prioriteret rækkefølge. Beredskabet skal desuden også sikre, at et eventuelt brud på informationssikkerheden bliver håndteret.
Relevante dele af beredskabet kommunikeres ud til kommunens it-brugere således, at der er synlighed omkring det sikkerhedsniveau, som er etableret.

Konsekvensen ved ikke at have et beredskab kan være, at opgaverne ikke kan løses med deraf følgende livstruende, økonomiske, juridiske og imagemæssige konsekvenser.

Nedenstående er eksempler på hændelser, der kan aktivere beredskabet for informationssikkerhed:

* [*Vandskader som følge af skybrud/oversvømmelser*.]
* [*Nedbrænding af serverrum eller andre væsentlige lokationer*.]
* [*Strømudfald, uanset årsag*.]
* [*Sikkerhedsbrud, så som virus og hackerangreb*. /Cyberhændelser]
* [Omfattende b*rud på persondatasikkerhed* .]
* [*Tyveri af vitalt it-udstyr*.]
* [*Terrorhandlinger der direkte eller indirekte skader it-anvendelsen* /Cyberhændelser]

# 4 Afgrænsning og antagelser

Nedenfor fremgår de afgrænsninger, [*xxxx kommune*] har lagt til grund for omfang og indhold af beredskabet og den udarbejdede beredskabsplan:

* [*At beredskabet kun gælder for bestemte geografiske områder, hvis organisationens opgaveløsning finder sted fra flere lokationer. Afgrænsningen konkretiseres*.]
* [*At beredskabet kun gælder for bestemte forretningsområder/opgavetyper. Afgrænsningen konkretiseres*.]
* [*At beredskabet kun gælder for en del af driften, fx systemer organisationen selv drifter. Afgrænsningen konkretiseres*.]
* [*At beredskabet kun gælder for en delmængde af de driftsleverandører, der anvendes. Afgrænsningen konkretiseres*.]
* [*At beredskabet kun gælder for infrastruktur og ikke applikationer, eller omvendt*.]

[Herudover kan der også være særlige ekstreme hændelsesscenarier (såkaldte ”Black Swans”) – kendetegnet ved meget lave sandsynligheder og meget ødelæggende konsekvenser – som organisationen ikke ønsker at tage højde for (pga. den meget lave sandsynlighed for forekomst af hændelser). Eksempler på sådanne scenarier bør, om muligt, anføres sammen med en beskrivelse af, hvordan risikoen ved det manglende beredskab håndteres (accept af risiko, overførsel/outsourcing, undgåelse).]

Beredskabet forventes at fungere effektivt under forudsætning af følgende antagelser:

* [*Det antages, at en katastrofe ikke samtidigt ødelægger organisationens og driftsleverandørens fysiske lokationer*.]
* [*Det antages, at en katastrofe ikke er sammenfaldende med flere af beredskabsledelsens nøgleaktørers fratræden fra deres stillinger*.]

# 5 Målsætning for beredskabet for informationssikkerhed

Med udgangspunkt i de forretningsmæssige behov er en række elementer afgørende for, at beredskabet lever op til ledelsens målsætning. Elementerne er desuden grundlag for valg af retableringsstrategi.

[Den overordnede målsætning for beredskabet for informationssikkerhed fremgår desuden typisk af informationssikkerhedspolitikken.]

Følgende målsætninger skal opfyldes i beredskabet:

* *[Beredskabet skal begrænse skadevirkningerne ved ikke planlagt utilgængelighed på it-understøttede forretningsprocesser.]*
* *[Beredskabet skal understøtte smidig retablering af data og systemer efter et nedbrud.]*
* *[Beredskabet skal understøtte at medarbejdere uddannes i håndtering af et nedbrud, der berører it-anvendelsen.]*
* *[Beredskabet skal understøtte at medarbejdere uddannes i håndtering af sikkerhedshændelser, der vedrører tab af integritet og/eller fortrolighed*.]
* *[Beredskabet skal understøtte kommunikationen i en beredskabssituation inklusiv valg af informationskanal]*
* *[Beredskabet skal understøtte, at der kan etableres et smidigt samarbejde med leverandører i tilfælde af et nedbrud, der berører kommunens it-anvendelse*.]
* *[Beredskabet skal understøtte, at efterfølgende vurdering og evt. kontrol af forløbet kan redegøres gennem fyldestgørende udfyldelse af hændelsesjournal/-log*.]

# 6 Roller og ansvar

Ledelsen har det overordnede ansvar for beredskabet.

[I praksis vil det ofte være it-sikkerhedskoordinatoren og/eller beredskabskoordinatoren, der koordinerer de forskellige opgaver, som er forbundet med beredskabsstyringen.]

Beredskabsstyringen omfatter en række opgaver af meget forskellig karakter, og der er flere forskellige aktører, som bidrager til såvel planlægning, udarbejdelse og vedligeholdelse af beredskabet.

Dette afsnit beskriver roller og ansvar i relation til udarbejdelsen og vedligeholdelsen af de enkelte operationelle delelementer i beredskabsplanlægningen og de væsentligste planlægningsområder. For at lette vedligeholdelsen af den skrevne operationelle beredskabsplan er opgaver og aktiviteter primært placeret i funktionelle enheder eller hos rolleindehavere frem for hos navngivne personer.

[Det anbefales helt overordnet at skelne mellem organisationens eget ansvar og et leverandøransvar.]

Nedenstående aktivitetsliste og ansvarsbeskrivelser præciserer, hvem der har ansvaret for de forskellige opgaver i forbindelse med planlægning og vedligeholdelse af [*xxxx kommunes*] beredskab for informationssikkerhed.

[Aktiviteterne kan præciseres yderligere, hvis kommunen finder det nødvendigt.]

| **Aktivitet** | **Ansvarlig** | **Udførende** | **Leverandøransvar** |
| --- | --- | --- | --- |
| **Ansvar for beredskabsstrategi for informationssikkerhed** | *[Topledelse / direktion]* | *[Informationssikkerhedskoordinatoren]* |  |
| **Ansvar for beredskabsplan for informationssikkerhed** | *[Informationssikkerhedsudvalget på vegne af topledelse/direktion]* | *[Informationssikkerhedskoordinatoren]* |  |
| **Ansvar for beredskabsplaner for system (nødplaner)** | *[Systemejer]* | *[Systemejer]* | [Kriterier for aktivering af beredskabsplanen skal aftales med leverandøren]. |
| **Kontaktlister** | *[Alle parter har et ansvar for at sikre, at kontaktoplysningerne opdateres.]* |  |  |

#

# 7 Eksterne leverandører

[*xxxx kommunes*] krav til sikkerhed og tilgængelighed skal opfyldes, også selvom [*xxxx kommunes*] er afhængig af eksterne leverandører. Derfor skal det som en del af beredskabet sikres, at leverandørerne kan leve op til de sikkerhedskrav til beskyttelse af data og det serviceniveau i forhold til tilgængelighed, som [*xxxx kommunes*] forventer.

I forhold til fortroligheden af data skal det sikres, at leverandøren er bekendt med [*xxxx kommunes*] klassifikationsniveauer, og hvilke krav til håndteringen af data det medfører. I en beredskabssituation kan det være nødvendigt at ændre eller omgå de normale sikringsforanstaltninger, og leverandøren skal derfor være særlig opmærksom på, hvilke krav der er til beskyttelse af fortroligheden.

[*xxxx kommunes*] konkrete krav til maksimal accepteret nedetid (Recovery Time Objective / RTO) og tolerance for datatab (Recovery Point Objective / RPO) fremgår af driftsaftalerne og er beskrevet i beredskabsplanen for informationssikkerhed. Løbende kontrol af om leverandøren kan efterleve disse krav udføres jf. de konkrete aftaler og består af en eller flere af følgende kontroller:

* SLA-aftaler samt aftaleforhold, der forpligter leverandører til et højt kvalitets- og sikkerhedsniveau (fx efterlevelse af ISO-standarder).
* Periodevise revisionserklæringer.
* Via periodiske test og målinger.
* Løbende rapportering af resultater.

# 8 Beredskabsscenarier

I dette afsnit er der en oversigt over de valgte beredskabsscenarier, som [*xxxx kommunes*] anser som mulige konsekvenser ud fra trusselsbilledet, og som den operationelle beredskabsplan skal kunne håndtere. Scenarierne indikerer hvilke operationelle delplaner, der skal defineres i beredskabsplanen og aktiveres i en beredskabssituation.

[I beredskabsmæssig henseende fokuseres traditionelt på scenarier, der vedrører tilgængeligheden af it-understøttelsen.
Dog kan man med fordel lade beredskabsplanen omfatte scenarier, der vedrører tab af integritet og/eller fortrolighed. Hændelser i disse kategorier kan sagtens have en alvorlighed, der kræver aktivering af den ”undtagelsestilstand”, som beredskabsplanen er udtryk for.
Scenarierne kan enten beskrives med udgangspunkt i den trussel (brand, hackerangreb, etc.), der udløser katastrofen eller med udgangspunkt i konsekvensen af hændelsesforløbet (eller begge dele). Følgende er eksempler på scenarier beskrevet med udgangspunkt i konsekvensen.]

| **Scenarie** | **Primære trusler** |
| --- | --- |
| [*Svigt af en enkelt komponent i it-infrastrukturen, som udgør ”single point of failure” (SPOF), hvorved der udløses et hændelsesforløb af beredskabsmæssig karakter.*] | [*Fejlende hardware, menneskelige fejl*] |
| [*Svigt af netværksinfrastruktur, hvorved en hel lokation afskæres fra it-understøttelse*]*.* | [*Fejlende hardware, hackerangreb*] |
| [*Svigt af centrale servere, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses*]*.* | [*Malware, hackerangreb, sabotage*] |
| [*Fysisk ødelæggelse af serverrum, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses.*] | [*Naturkatastrofer, terrorisme, sabotage*] |
| [*Forsyningssvigt, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses*]  | [*Naturfænomener, terrorisme, sabotage, menneskelige fejl*] |
| [*Ødelæggelse af fysiske lokationer, hvorved kritiske systemer bliver utilgængelige, og væsentlige opgaver ikke kan løses.*] | [*Naturfænomener, terrorisme*] |
| [*Brud på fortrolighed af følsomme personoplysninger, hvorved borgere udsættes for risiko for identitetstyveri eller andre væsentlige indskrænkninger i deres handlefrihed*] | [*Hackerangreb, konfigurationsfejl*] |
| [*Medarbejdere videregiver (u)bevidst personoplysninger om flere borgere til en andre borgere eller 3. part*] | [*Menneskelig fejl, bevidst handling*] |

[Det anbefales at præcisere ovenstående generiske scenarier, så de er bedst muligt målrettet mod den enkelte kommunens forhold. Fx at udpege komponenter, som på forhånd er kendt som Single Point Of Failure (eksempelvis komponenter i infrastrukturen, der, hvis de svigter, via en kaskade-effekt vil betyde udbredt brud på tilgængeligheden]

# 9 Implementering af beredskabet for informationssikkerhed

Kommunikation og implementering i kommunen sker efter "top-down" princippet, hvor ledelsen og informationssikkerhedskoordinatoren har ansvaret for at kommunikere videre til de medarbejdere, som indgår i beredskabsorganisationen.

Kommunikationen spiller en vigtig rolle og skal sikre, at både den operationelle plan og fremtidige opdateringer hertil formidles effektivt og direkte.

Målet med kommunikationen er at:

* gøre medarbejdere opmærksomme på, at der eksisterer en beredskabsplan for informationssikkerhed, hvad den indeholder, og hvordan den vil kunne påvirke medarbejderen i en beredskabssituation,
* informere beredskabsorganisationen og it-afdelingen om opdateringer til beredskabsplanen, når det er relevant,
* skabe en distributionskanal for den opdaterede beredskabsplan og sikre og forbedre beredskabssituationen.

En god implementering af beredskabsplanen viser sig i en beredskabssituation, hvor kommunikationen og håndteringen af beredskabet:

* er præcis og rettidig,
* sikrer tilstrækkelig information til medarbejdere, brugere, samarbejdspartnere og pressen,
* sikrer konsistens i informationen om hvilke systemer, der er berørte, hvilken konsekvens situationen medfører, forventninger til retableringstidsrammen m.v.

[Modtagerne af informationen vil variere fra situation til situation, men relevant information til brugerne er af særlig vigtighed.]