DELPLAN 8

PLAN FOR
IT-BEREDSKABET

Februar 2020

REGION SJÆLLAND
– vi er til for dig

Indhold

1 FORMÅL MED IT-BEREDSKABSPLANEN

Formålet med it-beredskabsplanen er at fastlægge de overordnede rammer for Region Sjællands arbejde med og implementering af it-beredskabet. Planen beskriver, hvorledes niveauet for it-beredskabet fastlægges med afsæt i Region Sjællands forventninger og krav hertil.

Den operationelle udmøntning af it-beredskabsplanen uddybes særskilt i it-beredskabets beskrivelser af eskalering, varsling, mobilisering, fremmødesteder, kontaktlister, checklister, ledelsesoverblik og kommunikation samt nødhjemmeside.

Nærværende dokument udgør en delplan til Region Sjællands sundhedsberedskabsplan og indeholder en overordnet beskrivelse af indholdet i Region Sjællands it-beredskab. Når der i teksten henvises til it-beredskabsplanen, henvises der derfor ikke blot til nærværende dokument, men til den samlede it-beredskabsplan i Region Sjælland, jf. afsnit 3.

2 ANSVAR OG PROCEDURE

Ledelsen i Koncern IT er ansvarlig for udarbejdelse og revision af it-beredskabsplanen.

Informationssikkerhedsfunktionen er ansvarlig for udarbejdelse og ajourføring af it-beredskabsplanen. Planen godkendes af ledelsen i Koncern IT og Regionens Beredskabsudvalg.

It-beredskabsplanen *vedligeholdes* med udgangspunkt i følgende:

- Regionens sundhedsberedskabsplan
- Regionens It-strategi
- Regionens Informationssikkerhedspolitik
- Krav fra virksomhedsområderne
- Information fra øvrige regioner
- Nationalt Risikobillede (NRB) fra Beredskabsstyrelsen
- Efterretningsmæssig risikovurdering fra Forsvarets Efterretningstjeneste
- Information fra Center for Cybersikkerhed, Forsvarets Efterretningstjeneste
- Resultater af afholdte øvelser og test
- Oplevede nød- og katastrofesituationer

3 UDGANGSPUNKT FOR IT-BEREDSKABET

På baggrund af kravene i Region Sjællands sundhedsberedskabsplan, it-strategi og informationssikkerhedspolitik etableres et it-beredskab, således at regionens virksomhedsområder påvirkes minimalt ved en it-mæssig beredskabshændelse (nød-eller katastrofesituation).

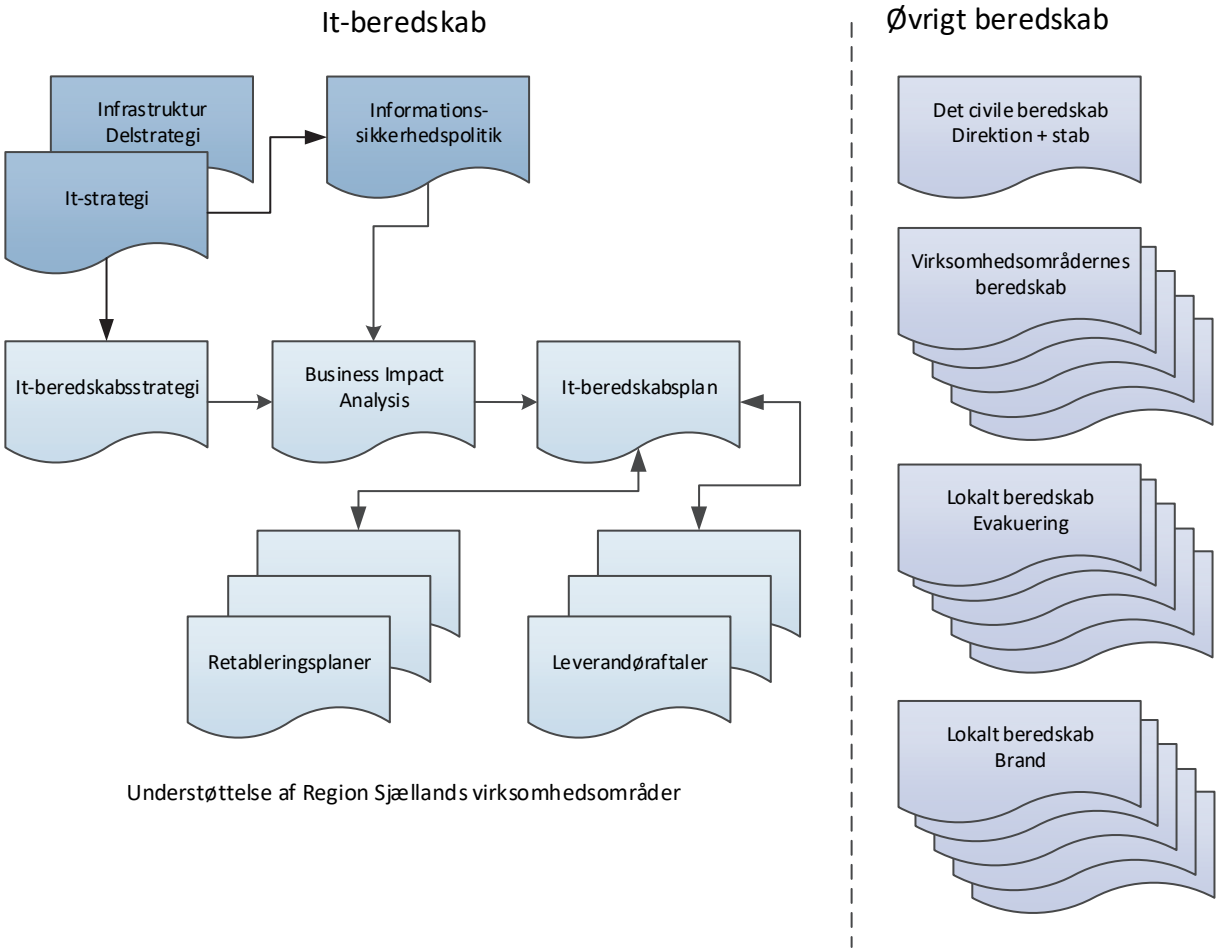
It-beredskabsarbejdet bygger på ITIL[1] processen IT Service Continuity Management og standarden ISO 22301 (Samfundssikkerhed – Ledelsessystemer – Videreførelse af virksomhedsdrift – Krav).

It-beredskabsplan
It-beredskabsplanen udmøntes (håndteres og vedligeholdes) i et krisestyringsværktøj, som er et selvstændigt system (SaaS, Software as a Service, benævnt Crisis Commander), der muliggør tilgang til it-beredskabsplanen uafhængigt af Region Sjællands it-driftssituation. It-beredskabsplanen håndterer eskalering, varsling, mobilisering, fremmødesteder, kontaktlister, checklister, ledelsesoverblik og kommunikation samt nødhjemmeside.

Retableringsplaner
Der udarbejdes retableringsplaner samt udfø-

[1] ITIL (Information Technology Infrastructure Library) refererer til et sæt af standarder for IT-servicestyring

res test heraf for alle kritiske it-systemer. Det gælder for it-systemer med beredskabsprioriteringen 0, 1 og 2.
Retableringsplaner er tekniske og detaljerede dokumenter, der beskriver, hvordan et givent it-system retableres. It-systemernes retableringsorden fremgår af it-beredskabsplanen.



Understøttelse af Region Sjællands virksomhedsområder

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

Der skal i arbejdet med it-beredskabet være fokus på:

- Identifikation af sårbarheder og afdækning af sandsynligheden for, at nød- eller katastrofesituationer opstår
- Konsekvenser ved opståede nød- eller katastrofesituationer
- Procedurer for overvågning af it-beredskabsforhold og for at detektere og reagere effektivt på en beredskabshændelse (nød- og katastrofesituationer).
- Hurtig retablering efter en beredskabshændelse (nød- eller katastrofesituation) under anvendelse af it-beredskabsplan og de nødvendige ressourcer.

4 AFGRÆNSNING OG ANTAGELSER

Region Sjælland har lagt følgende afgrænsninger til grund for omfang og indhold af it-beredskabet og de udarbejdede it-beredskabsplaner:

- It-beredskabsplanen omfatter datacentrene i Ringsted og Slagelse samt, i prioriteret orden, alle lokationer i regionen.
- It-beredskabsplanen skal sikre den grundlæggende it-infrastruktur, IP-telefoni, email-kommunikation og sygehusenes væsentlige og patientkritiske it-systemer. Det drejer sig om it-systemer med beredskabsprioriteringen 0, 1, 2, 3, 4 og 5.
- It-beredskabsplanen omfatter også it-systemer som driftes eksternt. Endvidere er også it-systemer, som driftes delvist hos eksterne leverandører og i regionens egne datacentre, omfattet. Opgaveløsningen sker i samarbejde med leverandørerne. Der stilles, jf. afsnit 7, krav til aftaleindgåelsen med sådanne leverandører.
- It-beredskabsplanen omfatter et samarbejde med Region Hovedstaden vedrørende det fælles system Sundhedsplatformen. It-beredskabsledelsen i Region Hovedstaden skal holdes informeret i tilfælde af, at der erklæres en it-mæssig nød- eller katastrofesituation Region Sjælland.

Med hensyn til sandsynligheden for, at kritiske sikkerhedsmæssige hændelser indtræffer, er der gjort følgende antagelser:

- Det antages, at en katastrofe ikke samtidigt ødelægger Region Sjællands og en ekstern driftsleverandørs fysiske lokationer.
- Det antages, at en katastrofe ikke samtidigt ødelægger Region Sjællands datacentre i Ringsted og Slagelse.
- Det antages, at en katastrofe ikke samtidigt ødelægger Region Hovedstadens datacenter i Hvidovre og Region Sjællands datacenter i Ringsted (DCR2).
- Det antages, at en katastrofe ikke er sammenfaldende med, at flere af it-beredskabsledelsens nøgleaktører fratræder deres stillinger, rammes af sygdom eller nedlægger arbejdet.

Sandsynligheden for at disse hændelser indtræffer, enkeltvis eller flere samtidigt, vurderes som meget lav og accepteres derfor som en risiko.
De nævnte hændelser ligger over grænsen for, hvornår it-beredskabet forventes at kunne retablere it-services til den til enhver tid gældende MTPOD[1].
Skulle én eller flere af hændelserne blive realiseret, vil det betyde, at Region Sjælland vil være uden it-understøttelse i en ukendt retableringsperiode.

5 MÅLSÆTNING FOR IT-BEREDSKABET

Den samlede it-drift skal understøttes af et passende it-beredskab til at minimere virkningerne af driftsafbrydelser som følge af nødsituationer eller katastrofer. Ved nødsituationer forstås nedbrud, der ikke kan håndteres inden for de normale rammer for daglig driftsafvikling. Det gælder såvel nedbrud, der påvirker tilgængeligheden, som nedbrud, der påvirker fortroligheden og integriteten af data.

Nedbruddet kan skyldes en tilsigtet eller utilsigtet hændelse som:

- Brand
- Eksplosion
- Vandskade
- Strømafbrydelse
- Spærret adgang til udstyr eller lokaler

[1] Se bilag 1.

- Gasudslip
- Overgravning af kabler
- Kemikalieudslip
- Afbrud af kølesystem
- Oversvømmelse
- Hærværk
- Simpelt indbrud
- Sabotage
- Misbrug
- Sygdom
- Systemnedbrud
- Personale i chokfase
- Cyberangreb
- Virusangreb.

It-beredskabet kan også aktiveres ved hændelser, som ikke umiddelbart forbindes med en katastrofe. Hændelser af ukendt karakter og under langsom udvikling kan vise sig at være yderst kritiske og vanskelige at erkende. Derfor er det af stor betydning at få en beslutningsdygtig ledelse etableret så tidligt som mulig.

Regionens virksomhedsområder skal ligeledes understøttes af et selvstændigt beredskab med det formål, at kunne håndtere kritiske arbejdsgange under en nødsituation eller katastrofe med manglende it-understøttelse. Dette beredskab er ikke omfattet af it-beredskabsplanen.

Følgende målsætninger skal understøttes. It-beredskabet skal:

- Begrænse skadevirkningerne af en nødsituation/katastrofe, der rammer de it-understøttede processer
- Understøtte en smidig overgang til alternative driftsfaciliteter
- Understøtte en hurtig retablering af data og systemer efter en katastrofe
- Sikre, at hændelser bliver erkendt, kategoriseret og eskaleret efter fastlagte procedurer, herunder at fejlretning pågår løbende og om nødvendigt i parallelle spor
- Understøtte aktivering af alternative it-driftsscenarier i tilfælde af en katastrofe
- Understøtte, at medarbejdere uddannes i håndtering af en katastrofe, der berører it-anvendelsen.
- Understøtte, at der kan etableres alternative pc-arbejdspladser til medarbejderne i Koncern IT
- Understøtte, at der kan etableres et smidigt samarbejde med eksterne leverandører og samarbejdspartnere i tilfælde af en katastrofe, der berører regionens it-anvendelse. Omfang og form skal være dokumenteret i de indgåede driftsaftaler
- Understøtte, at efterfølgende vurdering og eventuel kontrol af retableringsforløbet kan gennemføres ved fyldestgørende udfyldelse af hændelsesjournal/-log.

Det er et bærende princip, at it-beredskabet opbygges således, at de nødvendige ressourcer, informationer, værktøjer, kommunikationsformer og aktiver er til stede til håndtering af en nødsituation/katastrofe. Der opbygges således ikke detaljerede scenariebaserede operationelle planer for alle potentielle typer af nødsituationer og katastrofer, men én generisk plan.

<u>Overordnet beskrivelse af den operationelle indsats ved opstået beredskabshændelse</u>
IT-beredskabsledelsen er øverste ledelsesinstans i forbindelse med en opstået beredskabshændelse på it-området, med mindre den regionale krisestab er etableret. IT-beredskabsledelsen er ansvarlig for at lede aktiviteterne i IT-beredskabsplanen. IT-beredskabsledelsen har det operative ansvar for,

- at varsle
- at mobilisere
- at holde alle berørte interessenter informeret
- at kommunikere med regionens krisestab
- at kommunikere med AMK og sygehusenes kriseledelser

- at kommunikere med Region Hovedstadens it-beredskabsledelse
- at kommunikere med de øvrige regioner vedrørende it-systemer i RSI[2] regi
- at sørge for, at de enkelte opgaver bliver udført
- at vende tilbage til normaldrift og afvikle it-beredskabet

Følgende roller indgår i it-beredskabsledelsen:
It-beredskabsleder
Stabschef
Teknisk leder
Informationsansvarlig
Sekretariatsfunktion

De instrukser, som it-beredskabsledelsen skal følge, findes i Krisestyringsværktøjet. Kun medlemmerne af it-beredskabsledelsen kan erklære beredskab på it-området.

For hver opgave er der udpeget en it-beredskabsteamkoordinator fra Koncern IT. De instrukser, som it-beredskabsteamkoordinatorerne skal følge, findes i Krisestyringsværktøjet.

Organisationen er beskrevet i et organisationsdiagram, som er tilgængeligt i krisestyringsværktøjet og på teamsite i Koncern IT. Rollerne er dokumenteret og findes i krisestyringsværktøjet.

IT-beredskabsorganisationen udvides gradvis i den takt, som tilstanden tilsiger. It-beredskabet afvikles, når det vurderes, at it-driften fungerer tilfredsstillende, og at tilbageværende opgaver kan løses i den almindelige organisation.

It-beredskabet opererer med 3 niveauer.

- **Informationsberedskab (GUL)**

Ved informationsberedskab varsles it-beredskabsledelsen til et niveau, hvor de skal kunne træffes på mobiltelefon og kunne møde i primært eller sekundært kommandocenter. Mobiliseringsplaner, checklister, kontaktlister, supplerende dokumentation og kommunikationsplan findes i krisestyringsværktøjet. Inden it-beredskabet afblæses, rapporteres der i krisestyringsværktøjet, og alle åbne opgaver lukkes.

- **Stabsberedskab (ORANGE)**

Ved stabsberedskab mobiliseres it-beredskabsledelsen til et niveau med fysisk fremmøde på primært eller sekundært kommandocenter. Mobiliseringsplaner, checklister, kontaktlister, supplerende dokumentation og kommunikationsplan findes i krisestyringsværktøjet. Inden it-beredskabet afblæses, rapporteres der i krisestyringsværktøjet, og alle åbne opgaver lukkes.

- **It-beredskab (RØD)**

Ved it-beredskab mobiliseres Koncern IT's medarbejdere i det omfang, det skønnes nødvendigt. Der mødes efter it-beredskabsledelsens anvisninger. Mobiliseringsplaner, checklister, kontaktlister, supplerende dokumentation og kommunikationsplan findes i krisestyringsværktøjet. Inden it-beredskabet afblæses, rapporteres der i krisestyringsværktøjet, og alle åbne opgaver lukkes.

6 KOMMUNIKATION OG INTEGRATION TIL REGION SJÆLLANDS ØVRIGE BEREDSKAB

Det er it-beredskabsledelsens ansvar, at alle berørte virksomhedsområder løbende holdes informeret i en nød- eller katastrofesituation. It-beredskabet skal ligeledes understøtte virk-

[2] RSI refererer til regionernes samarbejde om sundhedsteknologi, herunder IT, og innovation.

somhedsområdernes overgang fra it-understøttet drift til nøddrift baseret på nødplaner.

It-beredskabsplanen indeholder de nødvendige kontaktinformationer, som gør det muligt at varsle den regionale krisestab i tilfælde af en nød- eller katastrofesituation vedrørende it-driften.

Den regionale krisestab, virksomhedsområdernes krisestabe og AMK (Akut Medicinsk Koordinationscenter) skal altid underrettes, når it-beredskabet aktiveres.

7 ROLLER OG ANSVAR

Dette afsnit beskriver roller og ansvar i relation til *udarbejdelse og vedligeholdelse* af it-beredskabets operative opgaver.

Ledelsen i Koncern IT har det overordnede ansvar for it-beredskabet.

Nedenstående aktivitetsliste præciserer, hvem der har ansvaret for de forskellige opgaver i forbindelse med planlægning og vedligeholdelse af Region Sjællands it-beredskab.

Opgave:	**Ansvarlig:**	**Udføres af:**	**Godkender:**
Beredskabsstrategi for it-services	It-direktør	IT Continuity Manager	Direktionen
IT Continuity Manager	IT Continuity Manager	IT Continuity Manager, Virksomhedsledelse	Chefgruppen
Gennemførelse af detaljeret risiko- og konsekvensanalyser på forretningskritiske it-systemer	IT Continuity Manager	Virksomhedsledelse, IT Continuity Manager, systemsansvarlige, IT infrastruktur	Chefgruppen
Etablering af kriseledelse/beredskabsorganisation	IT Continuity Manager	Informationssikkerhed IT Continuity Manager	Chefgruppen
Etablering af retableringsteams	Informationssikkerhed IT Continuity Manager	IT infrastruktur, IT support, Helpdesk	Relevant Funktionschef
Etablering af værktøjsunderstøttelse + "beredskabskufferter"	IT Continuity Manager	IT Continuity Manager	Chefgruppen
Udarbejde eskaleringsproces	IT Continuity Manager	IT Continuity Manager	Chefgruppen

Opgave:	Ansvarlig:	Udføres af:	Godkender:
Udarbejde varslings- og mobiliseringsprocedurer	IT Continuity Manager	IT Continuity Manager	Chefgruppen
Udarbejde kontaktlister	IT Continuity Manager	IT Continuity Manager	Relevant it-chef
Systemoversigt med angivelse af beredskabs-prioritering	Service Level Manager	Service Level Manager, IT Continuity Manager	Relevant it-chef
Udarbejde kommunikationsplan	IT Continuity Manager	IT Continuity Manager, Helpdesk	Relevant it-chef
Udarbejde plan for samarbejde med eksterne leverandører	IT Continuity Manager	IT Continuity Manager	Relevant it-chef
Definering af operationelle planer (hardware)	IT Continuity Manager	IT infrastruktur	Relevant it-chef
Definering af operationelle planer (software)	IT Continuity Manager	IT infrastruktur	Relevant it-chef
Definering af operationelle planer (netværk)	IT Continuity Manager	IT infrastruktur	Relevant it-chef
Definering af operationelle detailprocedurer (bl.a. restore procedure)	IT Continuity Manager	IT infrastruktur	Relevant it-chef
Vedligehold af tekniske hjælpemidler (scripts mv.).	IT infrastruktur, IT support	IT infrastruktur, IT support	Relevant it-chef
Udarbejde katalog med øvelser	IT Continuity Manager	IT Continuity Manager	Relevant it-chef

Opgave:	Ansvarlig:	Udføres af:	Godkender:
Test af udarbejdede restore procedurer	IT infrastruktur	IT infrastruktur	Relevant it-chef
Afholdelse af øvelser	IT Continuity Manager	IT Continuity Manager	Chefgruppen
Review af plan og øvelser	IT Continuity Manager	Ekstern konsulent/ IT Continuity Manager	Chefgruppen

8 EKSTERNE LEVERANDØRER

Region Sjællands krav til sikkerhed og tilgængelighed skal opfyldes, også selv om Region Sjælland er afhængig af eksterne leverandører. Derfor sikres det, som en del af it-beredskabet, at leverandørerne lever op til de sikkerhedskrav til beskyttelse af data og det serviceniveau i forhold til tilgængelighed, som Region Sjælland forventer:

- Region Sjællands konkrete krav til retableringsmål (RTO[3], RPO[4] mv.) fremgår af driftsaftalerne og er beskrevet i it-beredskabsplanen
- Regionens prioriteringsskema benyttes og niveauet fremgår af driftsaftalen eller et bilag hertil.

I forhold til fortroligheden af data sikres det, at leverandøren er bekendt med Region Sjællands klassifikationsniveauer og de krav til håndteringen af data, der følger heraf (bl.a. personhenførbare data). 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.

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[5] samt aftaleforhold, der forpligter leverandører til et højt kvalitets- og sikkerhedsniveau (fx efterlevelse af ISO-standarder)
- Periodevise revisionserklæringer
- Periodiske test og målinger
- Løbende rapportering af resultater.

[3] Recovery Time Objective = mål for genoprettelsestid
[4] Recovery Point Objective = den maksimale tidsperiode, hvor tab af data kan accepteres
[5] Service Level Agreement = aftale om serviceniveau

Kravene til eksterne leverandører skal ses i sammenhæng med de krav, der udspringer af regionens informationssikkerhedspolitik og tilhørende retningslinjer.

9 IMPLEMENTERING AF IT-BEREDSKABET

Implementering af it-beredskab i Region Sjælland sker efter et topstyret princip, hvor ledelsen har ansvaret for at kommunikere videre til de medarbejdere, som indgår i it-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 it-beredskabsplan, hvad den indeholder, og hvordan den vil kunne påvirke medarbejderne i en beredskabssituation,
- Informere beredskabsorganisationen og Koncern IT om opdateringer til it-beredskabsplanen, når det er relevant,
- Skabe en distributionskanal for den opdaterede it-beredskabsplan og sikre og forbedre it-beredskabssituationen.