Specialister i it-infrastruktur

IT-beredskabsplan

Jammerbugt Kommune

Indholdsfortegnelse

1 DOKUMENT HISTORIK 5
1.1 Dokument placering 5
1.2 Dokumentstruktur 5
1.3 Relaterede dokumenter 6
1.4 Opdatering 6
1.5 Distributionsliste 7
2 INTRODUKTION TIL IT-BEREDSKABSPLANEN 8
2.1 Formål af IT-beredskabsplanen 8
2.2 Succeskriterier for IT-beredskabsplanen 8
2.3 Afgrænsninger i IT-beredskabsplanen 9
2.4 Målgruppe 9
3 RISIKO HOS JAMMERBUGT KOMMUNE 10
3.1 Trusler 10
3.2 Bedømmelse og ændringer af risici 10
3.2.1 Ændringer i trusselsbilledet 11
3.2.2 Ændringer i systemer 11
3.2.3 Årlige risikoanalyser 11
3.3 Risiko med sandsynlighed og konsekvens 11
3.3.1 Definition af ”Sandsynlighed” 12
3.3.2 Definition af ”Konsekvens” 13
3.4 Prioriterede systemer - klassifikation 14
4 BEREDSKABSORGANISATION OG ANSVARSFORDELING 15
4.1 Roller og ansvar 16
4.1.1 IT-beredskabsledelsen 16
4.1.2 IT-beredskabsleder 18
4.1.3 IT-Beredskabskoordinator 18
4.1.4 Kommunikationsansvarlige 20
4.1.5 Retableringsteams/Leverandører 21
4.1.6 Andre roller: Digitalisering, IT og indkøb 21

4.1.7 Andre roller: Ejendomscenter Jammerbugt 22
4.1.8 Leverandører 22
4.1.9 Systemejere 23
5 KOMMUNIKATION 24
6 AKTIVERING AF IT-BEREDSKABSPLANEN 25
6.1 Vurdering af en hændelse 27
6.2 Beredskabsproces 27
6.3 Alarmering 28
6.4 Eskalering 28
6.5 Plan for driftsnedbrud hos leverandør 30
6.6 Ibrugtagning af alternativ driftslokation 30
6.7 Hardwarerelaterede planer 32
6.8 Servere.....32
6.9 Netværk.....32
6.10 Plan for virus eller hackerangreb 33
6.11 Plan ved brud på persondatasikkerhed.....34
7 NORMALISERING..... 35
7.1 Genetablér processer.....35
7.2 Afslut nødplaner.....35
7.3 Afslut beredskab 35
7.4 Evaluering af beredskab.....35
8 FORANKRING, VEDLIGEHOLDELSE OG TEST AF IT-BEREDSKABSPLAN..... 36
8.1 Test af IT-beredskabsplan 36
8.2 Uddannelse og træning 37
8.3 Planlægning af test.....37
9 VEDLIGEHOLD OG OPDATERING AF IT-BEREDSKABSPLAN . 38
9.1 Vedligehold af IT-Beredskabsplan.....38
9.2 Opdatering af planer.....38
9.3 Ordforklaring 39

10 GODKENDELSE OG KENDTE PROBLEMSTILLINGER..... 40
10.1 Optimeringsmuligheder.....40
10.2 IT-beredskabsplan godkendelse 40

1 Dokument historik

Denne sektion dokumenterer en historik af opdateringer i dokumentet.

Version, Dato	Forfatter	Godkender	Ændringer
3.0 - sep 2021	Peter Dinesen, Atea	Henrik Bech, Jammerbugt Kommune	Godkendt version
3.1 – sep 2022	Henrik Bech, Jammerbugt	Morten Hedegaard, Jammerbugt	Godkendt version
3.2 - nov 2023	Henrik Bech, Jammerbugt	Jacob Holst Pedersen, Jammerbugt	Godkendt ved skifte af IT chef

1.1 Dokument placering

IT-beredskabsplanen og alle relaterede dokumenter skal opbevares på "sikre lokationer" således, at det til enhver tid er muligt tilgå planer og relaterede dokumenter specificeret i afsnit"1.3 Relaterede dokumenter" både i elektronisk og fysisk form i tilfælde af aktivering af IT-beredskabet.

Primær form: I Jammerbugt Kommunes IT beredskabsplan på Teams under Team Digitalisering, IT og Indkøb: Microsoft Teams

Sekundær placering: På Jammerbugt Kommunes netværksdrev under denne filstruktur: N:\Digitalisering_IT\It-afdeling\Dokumentation\Kopi af It Beredskabsplan (Fra Teams)

Fysisk form: I pengeskab i kælderen i Aabybro rådhus samt i pengeskab i kælderen ved serverrum i Brovst rådhus

Denne udgave er en midlertidig kopi af et online dokument. Fysiske udgaver er udelukkende valide den dag de printes. Kontakt dokumentets ejer hvis du har spørgsmål.

1.2 Dokumentstruktur

IT-beredskabsplanen består af flere komponenter, som hver især vil blive vedligeholdt i separate dokumenter.

- IT-beredskabsplanen
  - Den overordnede proces i tilfælde af beredskabshændelser inkl. prioritering rolle og ansvarsbeskrivelser, og omfang af inkluderede services og ledelsesaktiviteter.
- IT-beredskabsplan strategi
  - Beskriver hensigterne, forklaringerne, principperne m.v. i forhold til IT-Beredskab

1.3 Relaterede dokumenter

Der refereres til følgende dokumenter i dette dokument:

Primære Dokumenter:	Lokation:
IT-Beredskabsplan strategi	Se ovenfor
IT-Beredskabsplan	Se ovenfor
Relaterede dokumenter:	**Lokation:**
System Recovery Plan (for alle services)	Se ovenfor
Servicedesk Driftinfo	Se ovenfor
Systemdokumentation	Se Ovenfor
Rød mappe/log	Fysisk i papirform (Kladde) ved Servicedesken I elektronisk form – Se ovenfor Listeform i Teams: Team IT-drift - "Rød Mappe" Driftsforstyrrelser - Drifts problemer (sharepoint.com)
Beredskabslog	Se ovenfor
Beredskabsrapport	Se ovenfor
Telefonkæde	Se ovenfor
Kommunikationsplan	Se ovenfor
Service Ansvar og Kontaktliste	Se ovenfor
Alarm og koder til administrationsbygninger	Se ovenfor
Disaster Recovery Test / Øvelse	Se ovenfor

Med tiden kan det udvides til:

- Action Cards
- Prioriteret systemoversigt med versioner
- Hardwarespecifikationer for kritiske enheder
- Øvelses- / Testplaner for IT-beredskabet

1.4 Opdatering

Det er den ansvarlige for IT-beredskabsplanens ansvar, at sørge for, at dette dokument til enhver tid er opdateret og tidssvarende i tilfælde af ændringer i organisationen eller IT-infrastrukturen.

Alle som læser dette dokument, og vurderer at dokumentet ikke er relevant eller tidssvarende, har til ansvar at gøre den IT-beredskabsplan ansvarlige opmærksom herpå.

Opdatering bør endvidere ske hvis:

- Erfaringer fra en hændelse eller øvelse tilsiger det
- Kommunens organisation ændres
- Myndighedernes struktur eller ansvarsområde ændres

1.5 Distributionsliste

Distributionslisten sikrer at alle relevante ressourcer har adgang til opdaterede udgaver af IT-beredskabsplanen og tilhørende dokumenter, til brug i tilfælde af totalt nedbrud.

IT-Beredskabskoordinator, som er defineret i bilag "Service Ansvar og Kontaktliste", er ansvarlig for at distribuere planen når den opdateres, så alle medlemmer har adgang til:

- 2 fysiske kopier: 1 i pengeskab i kælderen i Aabybro rådhus samt 1 i pengeskab i kælderen ved serverrum i Brovst rådhus
  Det er vigtigt at sikre kopier af både IT-beredskabsplanen og alle relaterede dokumenter.
  Yderligere indeholder mappen en sikkerhedskopi (USB Disk) af alle godkendte elektroniske dokumenter.

Samt

- Adgang til en elektronisk kopi lagret i et eksternt system, som ikke vil påvirkes af totalt nedbrud på arbejdspladsen. Placering for dokumenterne er Microsoft Teams
  Det er vigtigt at sikre at medarbejderen har det nødvendige udstyr for at få adgang til planerne remote.

Se listen af medlemmer med adgang til den elektroniske udgave af IT-beredskabsplanen i bilaget "Service Ansvar og Kontaktliste".

2 Introduktion til IT-beredskabsplanen

IT-Beredskabsplanen for IT er den operationelle udmøntning af den IT-Beredskabsstrategi, som er godkendt i Jammerbugt Kommune.

Denne IT-beredskabsplan beskriver de operationelle tiltag og handlinger, som er relevante i en beredskabssituation, mens strategien fastsætter de overordnede mål og rammer for styringen af beredskabet.

2.1 Formål af IT-beredskabsplanen

IT-systemerne i Jammerbugt Kommune danner baggrund for store dele af kommunens opgaveløsning. Samtidig er en række forretningsgange og en stor del af kommunens opgaveløsning, afhængig af velfungerende IT-værktøjer. Jammerbugt Kommunes IT-afdeling leverer primært IT ydelser til deres egne ansatte. Driftsforstyrrelser på interne IT services og systemer kan dog også have indirekte indflydelse på services, der leveres til kommunens borgerne og samarbejdspartnere. Det kan f.eks. være manglende IT-understøttelse af sagsbehandling, tvungen aflysning af møder, manglende evne til telefonisk omstilling, utilgængelige vagtnumre osv.

I forbindelse med, at Jammerbugt Forsyning er blevet juridisk adskilt fra Jammerbugt Kommune, leverer Jammerbugt Kommune stadig IT-ydelser til Jammerbugt Forsynings ansatte.

Formålet med IT-beredskabsplanen er således:

- At kortlægge procedurer vedr. ledelsesforankring, kommunikation og eskalation i tilfælde af krise- og beredskabssituationer relateret til IT services
- At dokumentere snitflader, ansvarsfordeling, prioritering, risikovurdering og genetableringstider af identificerede kritiske IT services
- Etablere og fastholde viden om identificerede kritiske IT services
- Sikre den højest mulige oppetid på identificerede IT services, i tilfælde af både mindre og større hændelser som påvirker driften af disse

IT-beredskabsplanen samt de operationelle vejledninger henvender sig til ledelsen, de IT ansvarlige og de tekniske ressourcer involveret i en genetableringssituation, og skal sikre at alle ressourcer kender deres roller, ansvar og funktion.

2.2 Succeskriterier for IT-beredskabsplanen

IT-beredskabet skal skabe sikkerhed for, at Jammerbugt Kommune kan genskabe en normal driftssituation hurtigt, sikkert og i prioriteret rækkefølge. Endvidere skal relevante dele af IT-beredskabet kommunikeres ud til kommunens IT-brugere således, at alle er bekendt med den rolle og det ansvar, de har i en beredskabssituation.

Konsekvensen af ikke at have et beredskab kan være, at opgaverne ikke kan løses med deraf følgende menneskelige, økonomiske, juridiske, omdømmemæssige konsekvenser til følge.

Succeskriterierne for denne plan er således, at:

- Direktionen skal kunne godkende IT-Beredskabsplanen
- At kunne udøve myndighedsopgaver i en krisesituation
- At der findes et reelt beredskab i en krisesituation
- Anmærkninger fra IT-revisionen undgås
- Planen etableres med udgangspunkt i en risikovurdering ud fra et forretningsmæssigt synspunkt
- Planen skal give Jammerbugt Kommunes ansvarlige for IT-beredskabsplanen en struktureret og afprøvet proces til retablering af udvalgte og kritiske IT services
- IT-beredskabet kommunikeres til relevante IT-brugere, så alle kender deres rolle og ansvar
- IT-beredskabsplanen skal løbende vedligeholdes med en gennemgang minimum 1 gang årligt
- Der udføres skrivebordstest en gang årligt med evaluering

På sigt ønsker Jammerbugt Kommune desuden:

- Der skal være foretaget test af IT-beredskabsplanen så Jammerbugt Kommune er sikre på, at kritiske IT services kan retableres
- Enkelt af de dokumenterede systemer testes minimum hvert andet år som en øvelse, indtil alle udvalgte services er afprøvet. Herefter gentages processen

2.3 Afgrænsninger i IT-beredskabsplanen

IT-beredskabsplanen omfatter ikke beredskabsplaner for bygninger, personale eller andre forretningsnødplaner, der anvendes i kommunen. Retablering af forretningsprocesser, hvor IT-systemerne indgår, er ikke omfattet af IT beredskabet. Det er systemejere, der har ansvaret for, at retablering af processerne sker på betryggende vis.

Beredskabsplanen tager ikke højde for en nødsituation, der på ét og samme tidspunkt forårsager, at samtlige lokaliteter bliver uanvendelige.

2.4 Målgruppe

IT-beredskabet fastlægges af de medarbejdere, som enten har det overordnede ansvar for, at opgaverne løses eller som varetager den konkrete opgaveløsning:

- Ledelsen - direktionen, systemejere/systemansvarlige og andre relevante ansvarlige medarbejdere
- IT-chefen
- IT-medarbejdere
- Ledelsen i Digitalisering og IT og Indkøb
- Kommunikationsmedarbejdere i forhold til information på hjemmeside, sociale medier og intranet til borgere og medarbejdere
- Opgaveansvarlige – IT-medarbejdere og andre medarbejdere, som løser opgaver i forbindelse med IT-beredskabet

3 Risiko hos Jammerbugt kommune

Omfanget af kommunens IT-beredskab fastlægges ud fra en forretningsmæssig risikovurdering, der kortlægger de forretningsmæssige konsekvenser ved at være uden IT understøttelse.

Risikoanalyser identificerer, hvilke trusler og risici kommunens IT-infrastruktur, IT-systemer med tilhørende data kan udsættes for således, at nødvendige tiltag kan implementeres for enten at nedsætte, dele eller undgå sandsynligheden for eller konsekvenserne af en sikkerhedshændelse.

Når risikovurdering er foretaget, kan kommunens ledelse prioritere ressourcer og sikkerhedstiltag effektivt i forhold til, hvor de giver mest værdi. Ledelsen bliver dermed bekendt med aktuelle trusler, så kommunen ikke udsætter sig selv, medarbejdere, borgere og samarbejdspartnere for større risici, end hvad der er acceptabelt.

3.1 Trusler

Selvom Jammerbugt Kommune allerede måtte have etableret nødvendige sikkerhedsværn, vil en hændelse, der fører til en beredskabssituation, alligevel kunne opstå. De trusler, der kan påvirke kommunens IT-understøttelse kan f.eks. være (men ikke begrænset til):

- Sikkerhedsbrud, som virus- og hackerangreb, der skader informationer eller forhindrer IT understøttelsen.
- Planlagte ændringer i IT-systemer, som medfører alvorlige fejl
- Udstyr, som svigter – f.eks. på grund af fejl i komponenter, slitage, overophedning, overkapacitet mv.
- Tyveri af vitalt IT-udstyr
- Strømudfald, uanset årsagen
- Brud på netværksforbindelser eller andre kommunikationsforbindelser, f.eks. på grund af overgravning eller strømsvigt hos leverandører
- Brande og eksplosionsulykker, nedbrænding af serverrum eller nedbrænding af andre væsentlige lokationer
- Naturkatastrofer eller andre forhold, der kan medføre utilgængelighed til bygninger, vandskader, strømsvigt mv.
- Terrorhandlinger der direkte eller indirekte skader eller forhindrer IT understøttelsen

3.2 Bedømmelse og ændringer af risici

Når trusler og sårbarheder er identificeret, måles risikoen ved at bedømme sandsynligheden for, at en trussel kan udnytte en sårbarhed samt hvilke konsekvenser det kan få for kommunen. Med udgangspunkt i risikovurderingen opdeles alle systemer i de i afsnit ”3.4 Prioriterede systemer - klassifikation” nævnte 3 kategorier efter en konkret prioritering. Prioriteringen finder sted i samarbejde med IT-Beredskabskoordinator, system- og dataejerne og IT-chefen. Efterfølgende indgår systemet i nødberedskabet med deraf følgende instrukser og vejledninger.

3.2.1 Ændringer i trusselsbilledet

System- og dataejere skal meddele ændringer i risikobilledet vedrørende det enkelte system til IT-Beredskabskoordinator, som herefter kan vurdere truslen og træffe beslutning om mitigerende handlinger.

3.2.2 Ændringer i systemer

Ved væsentlige ændringer af systemer skal der foretages en fornyet risikovurdering, og det skal vurderes, om ændringerne skal medføre en revision af IT-beredskabet.

3.2.3 Årlige risikoanalyser

IT-Beredskabskoordinator har ansvaret for, at der en gang årligt gennemføres en risikovurdering for alle væsentlige systemer og data i Jammerbugt Kommune således, at såvel det generelle sikkerhedsniveau som IT-beredskabet kan justeres herefter. IT-Beredskabskoordinator har endvidere ansvaret for kvalitetssikring af risikovurderingen og for vedligeholdelse af risikovurderingsmetoden.

3.3 Risiko med sandsynlighed og konsekvens

En risiko defineres som en kombination af sandsynligheden for at en hændelse indtræder og dertil graden af dens indvirkning på målet (konsekvens). Denne hændelse kan være en trussel, som kan have en negativ indvirkning. Den samlede risikoscore udregnes som sandsynligheden ganget med den højeste konsekvensscore, dvs. **"<Sandsynlighed> * <Konsekvens>"**, i et forsøg på at skabe et samlet input til vurdering af services prioritet.

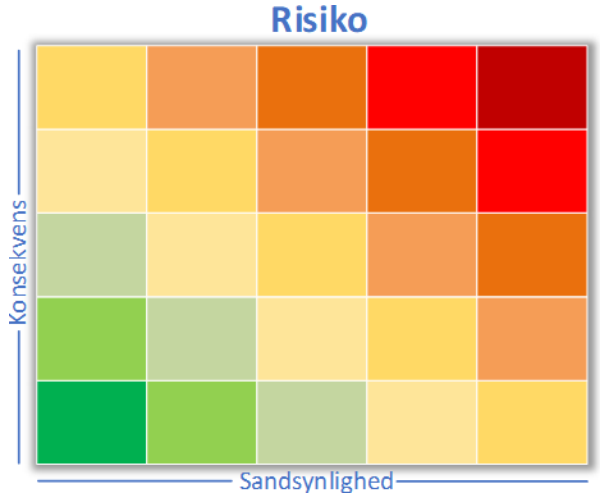
Farverne afspejler risici:

Grøn: *Mindst risici*

Gul: *Konsekvens er stor, men risikoen er lav*

Orange: *Større sandsynlighed, men mindre konsekvens*

Rød: *Større sandsynlighed og stor konsekvens*



3.3.1 Definition af "Sandsynlighed"

Jammerbugt kommune har udarbejdet en sandsynlighedsskala fra 1-5. Skalaen bruges i System Recovery Plan til at vurdere risici, og er ud fra følgende:

Værdi	Sandsynlighed	Eksempler
5	**Meget sandsynligt**	Flere dokumenterede eksempler på hændelsen inden for de sidste 3 måneder - Sker / er sket på tværs af både private og offentlige virksomheder (i pressen på månedsbasis).
4	**Mere sandsynligt**	Det ventes at hændelsen vil forekomme - Man har erfaring med hændelsen inden for de sidste 12 måneder - Sker / er sket jævnligt i andre offentlige og private virksomheder (omtales ofte i pressen).
3	**Sandsynligt**	Det er sandsynligt at hændelsen vil forekomme - Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder - Kendes fra andre offentlige og private virksomheder i Danmark (omtales årligt i pressen).
2	**Mindre sandsynligt**	Hændelsen forventes ikke at komme - Ingen erfaring med hændelsen - Kendes kun fra få andre offentlige og private virksomheder, men ikke i Danmark.
1	**Usandsynligt**	Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme - Ingen erfaring med hændelsen - Kendes kun fra andre offentlige og private virksomheder, men ikke i Danmark.

3.3.2 Definition af "Konsekvens"

I System Recovery Planerne vurderes konsekvensen for at en defineret risici opstår på en skala fra 1-5, ud fra følgende definitioner:

Værdi	Størrelse	Drift	Forretning	Mennesker	Lovgivning
5	**Meget kritisk (Major)** Påvirker i høj grad hele organisationen. Alle kunder er berørte.	Hele driften fejler og der er nedbrud på alle services, netværk, applikationer og forretningsprocesser.	Tab af troværdighed og stor konsekvens for organisationens økonomi og interesse fra nationale medier (f.eks. ComputerWorld) og muligvis internationale medier	Udstrakte og langvarige forstyrrelser, som skal udføres af flere medarbejdere, partnere og kunder.	Kommunen sat under administration. Højt profilerede nøglepersoner (Direktører) risikerer fyring, eller medarbejdere kan risikere fængselsstraf.
4	**Kritisk (High)** Hændelsen påvirker en stor eller større del af organisationen. Mange kunder er berørte.	En stor del af driften fejler, og der er nedbrud på flere væsentlige services, netværk, applikationer og forretningsprocesser.	Mindre tab af troværdighed og stor konsekvens for organisationens økonomi og interesse fra nationale medier (f.eks. ComputerWorld).	Stor forstyrrelse for medarbejdere, partnere og kunders opgaver.	Overtrædelse kan medføre kraftig kritik af kommunen. Som konsekvens kan administrative medarbejdere risikere fyring, eller kommunen kan idømmes betydelig bødestraf
3	**Mindre kritisk (Medium)** Hændelsen påvirker en mellem eller mindre del af organisationen. Flere kunder er berørte.	En del af driften fejler, og der er nedbrud på flere services, netværk, applikationer og forretningsprocesser.	Tab i troværdighed og interesse fra lokale medier.	Forstyrrelse for medarbejdere, partneres opgaver og/eller mindre forstyrrelser for kunders opgaver.	Kan medføre kritik af kommunalbestyrelse / højt profilerede nøglepersoner (Borgmester / Kommunaldirektør) Mindre juridiske konsekvenser
2	**Generende (Low)** Hændelsen påvirker en mindre del af organisationen. En enkelt er berørt.	En mindre del af driften fejler, og der er nedbrud på flere services, netværk, applikationer og forretningsprocesser.	Mindre tab af troværdighed og interesse fra lokale medier.	Mindre forstyrrelser for medarbejdere og partneres opgaver og ingen forstyrrelser for kunders opgaver.	Ingen juridiske konsekvenser, men da interesse er fra lokale medier holdes direktion / administration orienteret.
1	**Uvæsentlig (Planning)** En mulig hændelse. Ingen påvirkning af kunder.	Mulig fejl på et enkelt ikke-kritisk service, netværk, applikationer eller forretningsproces.	Lille eller intet tab af troværdighed uden for mediernes interesse.	Enkelte medarbejdere kan være nødt til at ændre den planlagte rutine. Ingen forstyrrelse for partnere og kunders daglige arbejdsrutiner.	Har ingen berøring til det administrative ledelseslag (direktører / kommunaldirektører)

3.4 Prioriterede systemer - klassifikation

Jammerbugt Kommune har udarbejdet en systemoversigt over relevante IT-systemer der anvendes i kommunen. Formålet med systemoversigten er dels at identificere systemejerskabet med ansvar og kontaktoplysninger, dels at vedligeholde vurdering af risici, og dels at vedligeholde systemernes individuelle kritiskhed samt forretningens krav til retablering (prioritering, retableringstider og acceptabel mængde mistede data mv.).

De udvalgte systemer er opdelt i to kategorier.

- Kerne systemer: IT-systemer, som er kritiske for den basale infrastruktur i organisationen. Uden disse vil de andre services ikke kunne fungere, og de prioriteres derfor højest i tilfælde af større nedbrud. Prioriteringen af disse services er tilrettelagt så man opnår den mest effektive opstart af IT-miljøet, og bør ikke afviges.

- Kritiske fag systemer: IT-systemer, som er vurderet kritiske for organisationen ud fra deres funktion, antallet af brugere som påvirkes samt konsekvens for kommunen hvis servicen er nede.

For at undgå tvivl om de enkelte systemers væsentlighed for kommunen, skal alle systemer være prioriteret indenfor tre kategorier. Kategorierne er beskrevet nedenfor. Indplaceringen foretages med udgangspunkt i en sårbarheds- og afhængighedsvurdering i dialog mellem systemejere, IT-beredskabskoordinatoren og IT-afdelingen. I prioriteringen tages højde for indbyrdes afhængigheder mellem kernesystemer, fagsystemer og eventuelle andre systemer.

Systemer som Jammerbugt Kommune ikke selv driver, skal systemejere sikre, at leverandørerne er bekendt med prioriteringen, og fastlægge eget beredskab ud fra dette.

Prioritet	Beskrivelse
HØJ prioritet	Kerneopgaver og forretningsgange kan ikke udføres uden IT, eller kun udføres uden IT ved anvendelse af et uforholdsmæssigt stort ressourceforbrug. Systemer til løsning af disse opgaver har prioriteret 1. Til sikring af den pågældende opgaveløsning, skal der derfor etableres et nødberedskab, som - i det væsentlige – sikrer fortsat drift af systemet. Samtidig skal der beskrives manuelle forretningsgange, som kan medvirke til at minimere konsekvenserne ved manglende IT-understøttelse.
	Prioritet 1 systemer garanteres normalt i drift indenfor højst en arbejdsdag
MELLEM prioritet	Nogle opgaver og forretningsgange kan udføres uden IT understøttelse i en kortere periode. Systemer til løsning af disse opgaver har prioritet 2. Til sikring af den pågældende opgaveløsning, skal der derfor etableres et nødberedskab, der dels beskriver en kortvarig manuel forretningsgang, dels – i det væsentlige – sikrer fortsat drift af systemet efter en kortere periode.
	En kortere periode defineres som 2-3 arbejdsdage
LAV prioritet	En række opgaver og forretningsgange kan udføres manuelt - dog med nogen ulempe. Systemer til løsning af disse opgaver har prioritet 3. Til sikring af den pågældende opgaveløsning, skal der etableres et nødberedskab, der dels beskriver en manuel forretningsgang, og dels – i det væsentlige – sikrer fortsat drift af systemet.
	Der er ingen krav til retableringstid, og defineres for snarest muligt

Systemerne og prioritet er beskrevet i bilag ”Systemoversigt, Reetablering og Risici”.

4 Beredskabsorganisation og ansvarsfordeling

Effektiviteten af IT-beredskabet afhænger af, i hvilket omfang de der involveres i en beredskabssituation, kender deres rolle og ansvar. Der er både en række opgaver der skal varetages i det daglige (i "fredstid"), og som er forudsætningen for, at IT-beredskabet overhovedet vil fungere i beredskabssituationen. Samtidig er der en række opgaver, som skal fordeles ud på de forskellige involverede, når katastrofen rammer.

I dette afsnit beskrives den organisation og bemanding, som skal mobiliseres i en IT-beredskabssituation, og som skal sikre, at planen kan effektueres i en beredskabssituation. Nedenfor er rollerne angivet, og deres ansvar og opgaver er beskrevet i de følgende afsnit.

Funktion	Roller
IT-Beredskabsledelsen	Øverste beredskabsmyndighed. Varetager væsentlige beslutninger vedrørende håndtering af beredskabsmæssige situationer
IT-beredskabsleder	I en katastrofesituation udpeges en IT-beredskabsleder, som har det overordnede ansvar for, at reetableringen af IT-services under katastrofen forløber effektivt, smidigt og styret.
IT-Beredskabs-koordinator	IT-Beredskabskoordinator alarmeres når det er vurderet, at der er tale om en nød-/katastrofesituation eller situationen er i fare for at indtræffe.
IT-Retablerings-teams	Det er IT-Retableringsteams opgave at sikre, at nødvendige forretningsunderstøttede IT-systemer og processer genskabes hurtigst muligt.
Digitalisering, IT og Indkøb	Digitalisering, IT og Indkøb dækker over Jammerbugt Kommunes forskellige Level 1 og Level 2 ressourcer og IT-ledelse samt tekniske personale med faglig ekspertise. Kan både være interne og personer ansat hos leverandøren af en løsning.
Ejendomscenter Jammerbugt	Ejendomscenter Jammerbugt har det overordnede ansvar for kommunale bygninger i Jammerbugt Kommune, og sørger for det praktiske i forbindelse med etablering af midlertidige/permanente lokaler/arbejdspladser

Funktion	Roller
Kommunikations-ansvarlig	Ansvarlig for intern og ekstern kommunikation
Leverandører	Leverer udstyr, software, forbindelser mv. til genetablering af kerne- og/eller fagsystemer, og/eller sikrer genoprettelse af hostede kerne- og/eller fagsystemer
Systemejere	Sikrer løbende risikovurdering og prioritering af fagsystemer

4.1 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 Jammerbugt Kommune.

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

4.1.1 IT-beredskabsledelsen

IT-Beredskabsledelsen er øverste myndighed i forhold til alle beslutninger, der vedrører den operationelle håndtering af en IT-Beredskabsmæssig krise. I en krisesituation håndterer beredskabsledelsen kommunikation og rapportering i samarbejde med kommunaldirektøren, stabschefer og berørte direktører/chefer af relevante forretningsområder. Disse kan tage beslutning om eskalering såfremt det bliver nødvendigt. IT-Beredskabsledelsen har ledelse af alle retableringsaktiviteter.

I en krisesituation nedsættes altid en ledelsesgruppe, som består af den øverst rangerede tilgængelige chef, IT-ledelsen, IT-Beredskabskoordinator, kommunikationsansvarlige, ledere af relevante forretningsområder, kommunens jurist samt eventuelle repræsentanter fra leverandører. Formanden er den til enhver tid øverst rangerende chef.

Eksempel på IT-beredskabsledelsen:

IT-beredskabsledelsen	Rolle	Kontakt info
Det er den til enhver tid øverst rangerende tilgængelige chef der træffer beslutning om, hvem der skal være formand for beredskabsledelsen, og dermed har mandat til at træffe endelige beslutninger	**Formand**	Besluttes i beredskabssituationen
Leder af Digitalisering, IT og Indkøb	**Deltager**	
IT-Beredskabskoordinator	**Deltager**	
Kommunikationsansvarlig (web/intra/FB)	**Deltager**	
Ansvarlig for fysiske bygninger	**Deltager**	*Besluttes i beredskabssituationen*
Ledere fra relevante/berørte forretningsenheder	**Deltager**	*Besluttes i beredskabssituationen*
Juridisk ansvarlig	**Deltager**	*Besluttes i beredskabssituationen*
Leverandører	**Deltager**	*Besluttes i beredskabssituationen*

I "Service Ansvar og Kontaktliste" er medlemmer, roller og kontakt info for IT-beredskabsledelsen beskrevet

Dagligt ansvar

- IT-Beredskabsledelsen har ikke et egentligt ansvar i det daglige, da gruppens medlemmer kan variere afhængig af tilstedeværelse og situationens karakter.

Ansvar i beredskabssituationen

I beredskabssituationen har IT-beredskabsledelsen et særligt ansvar og skal udføre en række specifikke opgaver. Nedenfor er eksempler på opgaver IT-Beredskabsledelsen har i beredskabssituationen:

- Tager væsentlige ledelsesmæssige beslutninger vedrørende den operationelle håndtering af den IT-Beredskabsmæssige krise
- Håndterer kommunikation og rapportering til kommunaldirektøren, stabschef, centerchefer mv.
- Sikrer rettidig og relevant kommunikation med relevante myndigheder
- Ledelse af retableringsaktiviteter, herunder prioritering af disse
- Kan erklære en krise på grundlag af en konkret vurdering, selvom hændelsen ikke nødvendigvis opfylder kriterierne for iværksættelse af IT-beredskabet. Her kan dele af de operationelle handlingsplaner benyttes, fx kommunikationsplanen af hensyn til håndtering af interessenter (både interne og eksterne)
- IT-Beredskabsledelsen vurderer og igangsætter løbende passende aktiviteter der modsvarer situationen

4.1.2 IT-beredskabsleder

IT-Beredskabslederen er ansvarlig for IT-beredskabsplanen og sikrer, at den løbende opdateres og justeres i forhold til det aktuelle trusselsbillede, løbende risikovurderinger, test og evaluering af IT-beredskabet mv. samt godkendes. IT-Beredskabslederen varetager endvidere en række specifikke opgaver i en krisesituation: Ledelse af retableringsaktiviteter, rapportering til beredskabsledelsen, intern kommunikation mv.

Beredskabslederen er altid kommunens til enhver tid siddende IT-chef. I "Service Ansvar og Kontaktliste" er medlem, rolle og kontakt info for IT- beredskabslederen beskrevet

Dagligt ansvar

- IT-Beredskabslederen er den formelle ejer af IT-beredskabsplanen og tilhørende dokumenter
- Sikrer, at den seneste version til enhver tid er godkendt
- Ansvarlig for ressourceallokering til oplæring af medarbejdere i IT-beredskabet
- Ansvarlig for at interne og eksterne kommunikationsplaner relateret til IT beredskabet udarbejdes og er godkendt
- Sikrer, at ressourcer og kompetencer til genskabelse af kernesystemer er til stede

Ansvar i beredskabssituationen

I beredskabssituationen har IT-beredskabslederen et særligt ansvar og skal udføre en række specifikke opgaver.

- Håndterer kommunikation og rapporter til IT-Beredskabsledelsen, kommunaldirektøren, stabschef og berørte direktører
- Ledelse af IT-Beredskabskoordinator
- Tager væsentlige ledelsesmæssige beslutninger vedrørende den operationelle håndtering af den beredskabsmæssige krise.
- Ledelse af retableringsaktiviteter
- Kan erklære en krise på grundlag af en konkret vurdering selvom hændelsen ikke nødvendigvis opfylder kriterierne. Her kan dele af de operationelle handlingsplaner benyttes, fx kommunikationsplanen af hensyn til håndtering af interessenter
- Erklærer IT beredskabet overstået, når alle kerne- og fagsystemer er genskabt til normal drift
- IT-beredskabslederen vurderer situationen og igangsatte aktiviteter bekræftes eller tilpasses.

4.1.3 IT-Beredskabskoordinator

IT-Beredskabskoordinator er ansvarlig for den overordnede styring i forbindelse med beredskabsøvelser og genskabelse (recovery) af IT-systemer i forbindelse med større nedbrud.

IT-Beredskabskoordinatoren vedligeholder løbende den praktiske del af IT-beredskabet samt opretter og vedligeholder kontaktinformationslister (Service Ansvar og Kontaktliste dokumentet), notifikationsdiagrammer, eskalationsdiagrammer mv. IT-Beredskabskoordinatoren bistår ledelsen som sekretær i beredskabssituationer med at skrive i Rød Mappe / Log mv., samt bistår med koordinering af de enkelte aktiviteter.

I "Service Ansvar og Kontaktliste" er medlem, roller og kontakt info for IT-Beredskabskoordinatoren beskrevet

Dagligt ansvar

- Bidrage til beslutninger om hvilke tiltag der skal initieres, for at sikre et stabilt IT-miljø og nødvendige tiltag, som sikrer at de aftalte serviceniveauer kan overholdes.
- Sikre den nødvendige kompetence i organisationen, til at varetage Level 2 fejlsøgning.
- Udarbejder og opdaterer den nødvendige dokumentation (IT-beredskabsplan, System Recovery Planer og system dokumentation) for kritiske services.
- Løbende opdatere System Recovery Planer og system dokumentation, i tilfælde af ændringer.
- Sikrer, at eskaleringsprocessen er beskrevet og løbende ajourføres med aktuelle medarbejdere og aktører
- Sikrer, at IT-beredskabsplanen og tilhørende dokumenter altid er opdaterede og modsvarer det aktuelle trusselsbillede, for så vidt angår kernesystemer.
- Foretager årlige risikovurdering af kernesystemer, og implementerer passende korrigerende indsatser, og tilretter eventuelt IT-Beredskabsplanen i overensstemmelse hermed
- Vedligeholder SMS-kæde
- Sikrer, at fysiske forhold i datacentrene er opdaterede, efterset og vedligeholdt efter forskrifterne
- Sikrer, at IT-infrastruktur og kernesystemer er opdaterede og vedligeholdt med seneste sikkerhedsindstillinger jf. kommunens principper herom
- Opdaterer kontaktinformationslister (Service Ansvar og Kontaktliste dokumentet)

Ansvar i beredskabssituationen

I beredskabssituationen har IT-Beredskabskoordinatoren et særligt ansvar og skal udføre en række specifikke opgaver.

- Bistår IT-Beredskabsledelsen og IT-Beredskabslederen i den operationelle håndtering under IT-beredskabet
- Evaluere omfanget af skaden og potentielle konsekvenser i samarbejde med de tekniske ressourcer.
- Formidle information om omfanget af skaden og forventede udbedrings tid til ledelsen, brugere og andre relevante interessenter.
- Igangsætte recovery processen.
- Allokere og koordinere de nødvendige ressourcer og teams.
- Sikre kontakt imellem flere reetableringsteams eller leverandører
- Overvåge og dokumentere recovery forløbet inkl. tidtagning.
- Dokumentere og kontrollere udgifter i forbindelse med recovery processen.
- Informere ledelsen om eventuelle ændringer under processen og eventuelle problemstillinger.
- Sikre at alle verifikationstests er udført efter System Recovery Planerne afsluttes.
- Verificere at alle backup processer er igangsat efter System Recovery Planerne afsluttes.
- Erklære når miljøet er i normal drift.
- Dokumentere eventuelle skader med henblik på efterfølgende forsikringskrav.

4.1.4 Kommunikationsansvarlige

Kommunens ansatte, borgere og samarbejdspartnere skal informeres om beredskabssituationen og de løbende skridt der tages, for dels at bringe situationen under kontrol og dels for at sikre fremskridt under retableringsprocessen. Afhængig af situationen vil både ansatte, borgere, samarbejdspartnere, den generelle offentlighed og presse kunne være interessenter i forhold til kommunikation.

I "Service Ansvar og Kontaktliste" er medlemmer, roller og kontakt info for kommunikationsansvarlige beskrevet

Dagligt ansvar

- Bidrage til meddelelser for ekstern kommunikation er klar i forvejen (skabelon)
- Bidrage til kommunikationsplanen såfremt organisationen eller funktioner ændres
- Bidrage til kommunikations tidsplan skabelon
- Kan sikre udarbejdelse af en FAQ

Ansvar i beredskabssituationen

- I beredskabssituationen har den kommunikationsansvarlige et særligt ansvar og skal udføre en række specifikke opgaver.
- Indsamler og videreformidler information, som er påkrævet for intern og ekstern kommunikation
- Informerer om situationen og de løbende fremskridt til interessenter i henhold til IT-Beredskabsledelsens anvisninger
- Beslutter kommunikationskanal i samarbejde med IT-Beredskabsledelsen og muligheder i øvrigt
- Udarbejder meddelelser til ekstern kommunikation
- Udsender intern og ekstern kommunikation ved nærmere faste intervaller, beskrevet i kommunikationsplanen
- Svarer på de mest kritiske spørgsmål jf. IT-Beredskabsledelsens anvisninger

4.1.5 Retableringsteams/Leverandører

Retableringsteams er teknisk orienterede medarbejdere, som forestår retablering af IT-systemer i henhold til de operationelle planer og detailplanerne, og desuden har ansvar for at sikre, at forløbet dokumenteres i Rød Mappe / Log. Dette inkluderer også leverandører

Dagligt ansvar

- Bidrager med teknisk input til opdateringer af relevante SRP

Ansvar i beredskabssituationen

I beredskabssituationen har Retableringsteams et særligt ansvar og skal udføre en række specifikke opgaver

- Evaluere omfanget af skaden og potentielle konsekvenser i samarbejde med de IT-Beredskabskoordinator.
- Sikre kontakt på det tekniske plan – både internt og med leverandører
- Gennemfører systemgenoprettelse i henhold til SRP'ere
- Aktiviteter dokumenteres sideløbende via en grundig ajourføring af fejlmeldingen i Rød Mappe / Log i Microsoft Teams, Sekundær på N: som henvist i afsnit "1.2 Relaterede dokumenter" (alternativt på papir). Ved enkelte undtagelser føres kun en intern log.
- Informerer løbende IT-Beredskabskoordinatoren om status på systemgenoprettelse, herunder tidsestimater for forventet genoprettelse, samt eventuelle ændringer og problemer undervejs

4.1.6 Andre roller: Digitalisering, IT og indkøb

Digitalisering, IT og indkøb dækker over Jammerbugt Kommunes forskellige Level 1 og Level 2 ressourcer og IT-ledelse. De er fordelt i mindre virtuelle teams relateret til deres speciale områder inklusive Servicedesk, som håndterer 1st line kald fra brugerne.

Dagligt ansvar

- Lokal IT Helpdesk service.
- Operationelt ansvar for servere og anden IT-infrastruktur på alle omfattede lokationer.
- Operationelt ansvar for klienter.
- Vedligehold og opgradering af IT-infrastruktur, servere, software og klienter.
- Planlægning og installation af nyt hardware i server rum.
- Vedligehold og test af nødstrømsanlæg og køling i serverrum.

Ansvar i beredskabssituationen

- Assisterer IT-Beredskabslederen og IT-Beredskabskoordinatoren med at vurdere omfang og konsekvenser af nedbrud, samt estimere tiden for recovery processen.
- Være udførende på System Recovery processen.
- Udføre test og øvelser
- Sikre at nødstrømsanlæg er funktionelle og har brændstof, hvis aktiveret.
- Løbende informere IT-Beredskabskoordinatoren om status på System Recovery processen og eventuelle ændringer og problemer.

4.1.7 Andre roller: Ejendomscenter Jammerbugt

Ejendomscenter Jammerbugt har det overordnede ansvar for kommunale bygninger i Jammerbugt Kommune.

Der henvises til Ejendomscenter Jammerbugt beredskabsplan

I "Service Ansvar og Kontaktliste" er medlemmer, roller og kontakt info for Ejendomscenter Jammerbugt beskrevet

Dagligt ansvar

- Sikre de korrekte procedurer overholdes i forbindelse med brandsluknings- og forsyningsanlæg + køleanlæg mv. ud over serverrummet, som er IT chefens ansvar
- Sikre at tekniske og logiske adgangskontroller til fysiske bygninger og lokaler løbende vedligeholdes, herunder adgangskoder, låse, nøgler, overvågningskontroller mv.

Ansvar i beredskabssituationen

Ansvarsfordelingen i dette afsnit er på nuværende tidspunkt ikke afklaret og godkendt. Nedenstående er udelukkende ment som input.

- Sikre de korrekte procedurer overholdes i forbindelse med brandslukningsanlæg.
- Evaluere eventuelle skader og sikkerhedsrisici ved bygninger og serverrum, og rapportere til IT-Beredskabskoordinator.
- Oprydning efter eventuelle skader.
- Koordinere og sikre midlertidige arbejdspladser ved større skader/nedbrud.

4.1.8 Leverandører

Hvis der er aftalt særlige roller med leverandøren, bør disse beskrives her. Det kan f.eks. være kontaktpersoner, koordinatorer m.v.

Dagligt ansvar

- Sikrer, at der opretholdes et passende IT-beredskab i forhold til den IT-løsning leverandøren leverer
- Sikrer, at både kerne- og/eller fagsystemer (afhængig af leverance) er tilstrækkelig beskyttet og sikkerhedsopdateret
- Sikrer, at der er den nødvendige kapacitet og de nødvendige ressourcer tilgængelige til at kunne understøtte Jammerbugt Kommune i en IT-Beredskabssituation
- Sikrer, at nødvendige processer for genetablering af kerne- og/eller fagsystemer er tilgængelige i tilfælde af en beredskabssituation

Ansvar i beredskabssituationen

I beredskabssituationen har leverandører et særligt ansvar og skal udføre en række specifikke opgaver

- Underretter Jammerbugt Kommunes IT-chef straks ved nedbrud, når det vurderes, at kerne- og/eller fagsystemet ikke kan retableres.
- Stiller tilstrækkelige ressourcer til rådighed for Jammerbugt Kommune i en IT-Beredskabssituation
- Deltager i Jammerbugt Kommunes IT-Beredskabsledelse på kommunens foranledning

- Koordinerer retableringsindsatsen i samarbejde med Jammerbugt Kommunes IT-Beredskabskoordinator
- Meddeler løbende status for retablering

4.1.9 Systemejere

Nødberedskabet for IT-anvendelsen skal skabe sikkerhed for, at Jammerbugt Kommune kan genskabe en normal driftssituation hurtigt, effektivt og sikkert – også selvom IT-understøttelsen ikke eksisterer. Endvidere skal relevante dele af nødberedskabet kommunikeres ud til kommunens it-brugere således, at der er synlighed omkring det sikkerhedsniveau, som er etableret. Udover det tekniske nødberedskab, som er forankret i IT-afdelingen, skal systemejere for alle systemer tage stilling til behovet for beskrivelser af manuelle forretningsgange. Hvis systemet har prioritet 1, skal der beskrives manuelle forretningsgange, som kan medvirke til at minimere konsekvenserne ved et egentligt katastrofescenarie eller et mere begrænset systemnedbrud.

Dagligt ansvar

- Sikrer, at alle systemer som systemejeren har ansvaret for, er listet i Systemoversigten og er prioriteret og klassificeret
- Identifikation, overvågning og styring af risici for de processer, systemet understøtter
- Udarbejdelse af uddybende systemdokumentation
- Beskrivelser af relaterede interne kontroller - elektroniske og manuelle
- Etablering af systemsupport
- Administration af leverandøradgang

Ansvar i beredskabssituationen

I beredskabssituationen har systemejerne et særligt ansvar og skal udføre en række specifikke opgaver

- Underrette relevante brugere om nødberedskabet
- Beskrive konsekvenser for berørte borgere, virksomheder og samarbejdspartnere, og orientere IT-Beredskabskoordinatoren herom
- Bidrage til udarbejdelse af materiale til ekstern kommunikation
- Holde sig orienteret om IT-Beredskabslederens løbende opdateringer

5 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, herunder frekvens for løbende opdatering af status.

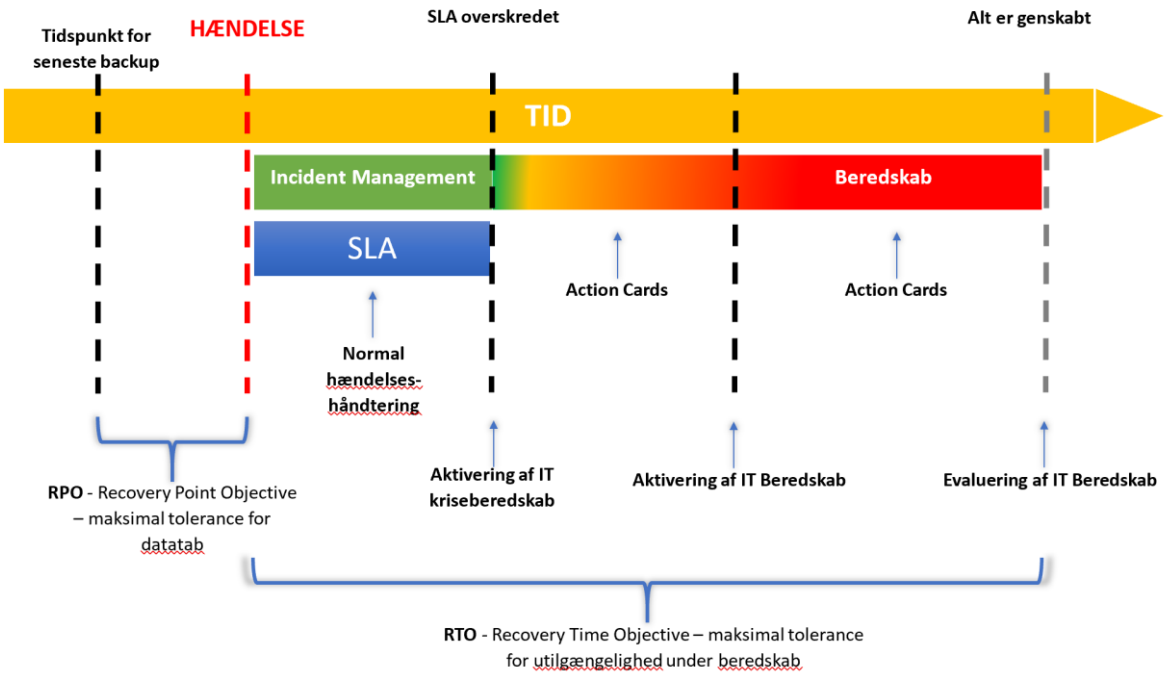
Det vil være beredskabsledelsen, der skal godkende kommunikationen.

Kommunikation og kommunikationsplan defineres i et særskilt dokument *"Kommunikationsplan ved IT relaterede hændelser"*, og tager udgangspunkt i nedenstående model:

Nr.	Handling
1	**Udarbejd tidsplan** Der udarbejdes en tidsplan for ekstern og intern kommunikation.
2	**Indsaml information** Al information, som er påkrævet for intern og ekstern kommunikation, samles hos den kommunikationsansvarlige.
3	**Beslut kommunikationskanal** For hver enkel intern og ekstern kommunikation fastlægges kommunikationskanalen.
4	**Udarbejd eksterne meddelelser** Udarbejd meddelelser til ekstern kommunikation, og få disse godkendt af beredskabsledelsen.
5	**Oversæt relevant dokumentation** Hvis der er behov for at vedlægge dokumentation, foretages eventuelt oversættelse heraf.
6	**Udsend information** Sørg for, at al intern og ekstern kommunikation udsendes samtidigt, hvis dette er påkrævet, og at budskaberne er ens.
7	**Responder på spørgsmål** Svar på eventuelle spørgsmål med fokus på de mest kritiske spørgsmål og interessenter.

6 Aktivering af IT-beredskabsplanen

Et hændelsesforløb gennemgår forskellige faser inden det egentlige IT-beredskab aktiveres. De tre faser fra en hændelse opstår til normal drift er genetableret er illustreret herved:



Første fase (grøn) efter en hændelse er almindelig incidenthåndtering, som håndteres af Jammerbugt Kommunes 1st og 2nd line support funktion. I denne fase kan hændelsen håndteres inden for rammerne af Jammerbugt Kommunes normale processer, arbejdsgange og problemløsning

Anden fase (gul) efter en hændelse er det tidsrum, hvor IT-understøttelsen ikke kan retableres indenfor den tid der er aftalt med forretningen, men hvor situationen endnu ikke er så kritisk, at IT-beredskabet skal aktiveres.

I **tredje fase (rød)** aktiveres og mobiliseres IT beredskabet, hvis der er sikkerhed for, at et af nedenstående kriterier er opfyldt eller vurderes i risiko for at blive opfyldt

Det er væsentligt at pointere, at en beredskabssituation (rød fase) erklæres af IT-beredskabsledelsen på grundlag af en konkret vurdering. Selvom hændelsen ikke umiddelbart opfylder kriterierne for at iværksætte det fulde IT-beredskab, kan dele af de operationelle handlingsplaner benyttes, f.eks. kommunikationsplanen af hensyn til håndtering af interessenter, herunder også anmeldelse af brud på persondatasikkerhed. En væsentlig del af aktiveringen og styringen/ledelsen vil i en sådan situation bestå i at afgrænse indsatsen i forhold til planernes fulde omfang.

Kriterier for aktivering af IT-beredskabet:

a. Tidsmæssig udstrækning af hændelsen

Hvis det står klart, at en hændelse ikke kan håndteres og løses inden for de ramte aktiveres serviceaftaler for almindelig udbedring af hændelser, kan det være en indikation af en krise, der kræver aktivering af IT-beredskabet.

Hvis der er risiko for, at en hændelse ikke kan håndteres og løses indenfor de ramte aktivers RTO, er der utvivlsomt tale om en krise, der kræver aktivering af IT-beredskabet.

b. Større datatab

Såfremt det står klart, at der efter en hændelse er risiko for datatab, der er større end tabstolerancerne, jf. RPO-værdierne, kan det være en indikation af en krise, der kræver aktivering af IT-beredskabet.

c. 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 IT-beredskabet.

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 IT-beredskabet. Dette afhænger af årsag til bruddet og alvoren af denne.

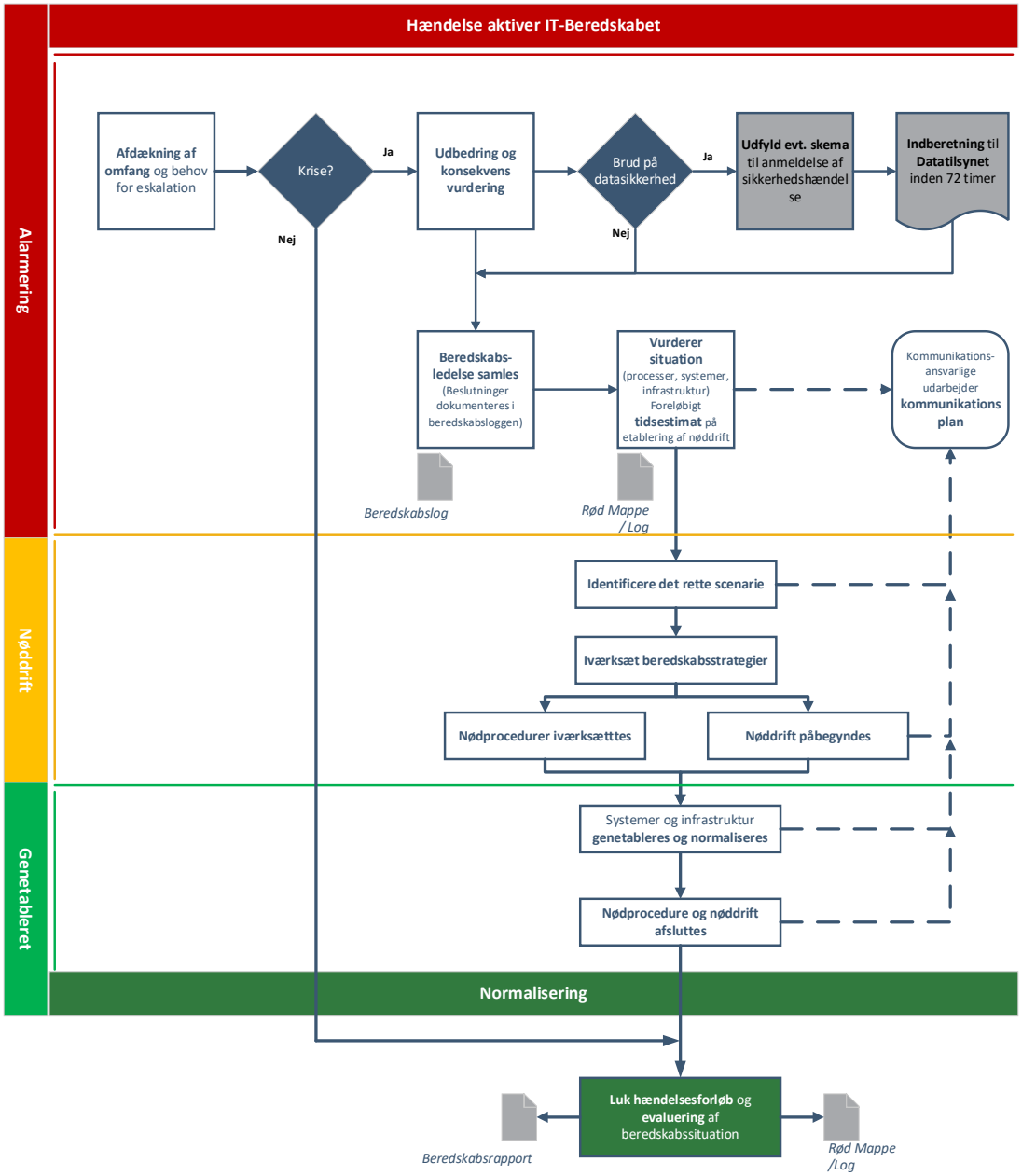
Uanset om beredskabet aktiveres eller ej vil scenariet Brud på persondatasikkerhed kunne anvendes som støtte til kommunikation.

d. Særlige hændelser

Særlige hændelser såsom:

- Naturkatastrofer (oversvømmelse, jordskælv, brand mv.) kan kræve umiddelbar aktivering af beredskabsplanen
- Brud i forsyningen af el, der går væsentligt ud over nødstrømskapaciteten
- Terrorisme, krig, sabotage, strejker

6.1 Vurdering af en hændelse



6.2 Beredskabsproces

Når IT-Beredskabsledelsen aktiverer IT beredskabet, skal der føres en *"Beredskabslog"* under beredskabsforløbet.

"Rød Mappe/Log" anvendes til registrering af hændelser og er et vigtige redskab til opfølgningsaktiviteter, fx erfaringsopsamling.

Når beredskabssituationen evalueres, skal der udarbejdes en *"Beredskabsrapport"* og Rød Mappe / Log skal ajourføres.

6.3 Alarmering

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

- Formanden for beredskabet, eller dennes stedfortræder, kan aktivere IT-Beredskabsplanen, og erklære en krise.
- Beredskabslederen, eller dennes stedfortræder, indkalder beredskabsledelsen.
- Beredskabslederen er nu styrende i forhold beredskabshændelsen, og styrer den efter beredskabsplanen.

Når beredskabsledelsen indkaldes, skal de mødes på:

- IT Leders kontor (I daglig tale Mortens Kontor), hvis det er muligt
- Alternativt findes der en anden passende lokation at mødes, afhængig af beredskabsledelsens nuværende lokation (Exvis War Room i kælderen)

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

- IT Leders kontor – (I daglig tale Mortens Kontor)
- *Mødelokale v/ K.DIR*, Toftevej 43, 9440 Aabybro
- Kantinen - Borgervænget 12, 9460 Brovst

6.4 Eskalering

Til at sikre struktureret initiering af beredskabsprocessen i forbindelse med en hændelse, anvendes nedenstående planer for eskalering.

Nr.	Handling
1	**Modtag notifikation** Når en notifikation om en potentiel katastrofe modtages, skal følgende oplysninger forsøges fremskaffet: • Typen af hændelsen • Eventuelle tilskadekomne personer • Omfanget af skaden • Hvilke eksterne leverandører er involveret
1.1	**Start Rød Mappe / Log** Brug kolonne i nærværende tabel, eller anvend tom skabelon
2	**Bekræft notifikation** Få notifikationen bekræftet hvis nødvendigt.
3	**Evakuer medarbejdere** Hvis evakuering er nødvendig, så følg planen for evakuering af bygningen.
4	**Kontakt Alarmcentralen** Kontakt Alarmcentralen hvis nødvendigt.
5	**Indledende vurdering af omfang**

Nr.	Handling
	Foretag en indledende vurdering af skadesomfanget. Skade på bygninger mv. bør vurderes af de bygningsansvarlige, mens skade på informationssystemer vurderes af IT-Beredskabskoordinatoren eller den leverandør, som har driftsansvaret.
5.1	**Vurder notifikation af øvrige beredskaber** Hvis IT-beredskabet er iværksat som det første, kan det være relevant at notificere andre dele af koncernens beredskab.
6	**Incident evaluering / eskalering til leverandør** Vurder situationen og undersøg hos leverandøren, hvor lang tid der skal bruges på at retablere skaderne, og bestem ud fra kriterierne, om IT-beredskabet skal aktiveres. Driftsleverandøren varsles om mulig beredskabssituation
7	**Aktivering af IT-beredskab** Aktiver IT beredskabet. Beslutningen om at aktivere IT beredskabet skal kommunikeres til beredskabsorganisationen. Informer om kendte udeståender
8	**Organisér beredskabsledelsen** Med udgangspunkt i den besluttede beredskabsorganisation mobiliseres beredskabsledelsen. Beredskabsledelsen vurderer situationen og igangsatte aktiviteter bekræftes eller tilpasses. Beredskabsledelsen konsolideres og fastholdes til beslutning om normalisering er truffet.
8.1	**Aktiver plan for driftsnedbrud hos leverandør** Udveksling af kontaktdetaljer, kommunikationsmønster og evt. aftaler for ekstern kommunikation i beredskabsforløbet. Aktivering foregår i henhold til aftaler.
9	**Information til interessenter** Øvrige relevante interessenter informeres om IT beredskabet.
10	**Fastlæg omfanget af skaden** Medmindre skadens omfang er åbenlys, f.eks. ved tab af en hel bygning, foretages en nærmere registrering af de berørte aktiver.
10.1	**Påbegynd planlægning af normalisering** For at minimere perioden med nedsat driftsfunktionalitet i beredskabssituationen og unødige omkostninger, igangsættes i relevant omfang planlægning af aktiviteter til normaliseret drift.

6.5 Plan for driftsnedbrud hos leverandør

Ved nedbrud hos en af Jammerbugt Kommunes driftsleverandører, skal det aftalte beredskab iværksættes så snart det vurderes nødvendigt. Nedenstående aktiviteter har til formål at varsko den konkrete leverandør og at sikre dialogen med leverandøren i hele beredskabssituationen.

Nr.	Handling
1	**Undersøg leverandørforhold** Det undersøges, hvilken leverandør den ramte IT-understøttelse er outsourcet til.
2	**Kontakt leverandør** Hvis ikke dette allerede er sket, fx i tilfælde af det er leverandøren der har konstateret og informeret om hændelsen, tages kontakt til leverandøren.
3	**Vurder situationen** Status gennemgås, og situationen vurderes i samarbejde med leverandøren. Hvis leverandøren har behov for adgang til organisationens lokation, aftales det, hvordan adgangen finder sted.
4	**Planlæg indsatsen** Planlæg indsatsen i samarbejde med leverandøren, og aftal det videre forløb.
5	**Kommunikation og kontakter** Planlæg hvordan kommunikationen med leverandøren skal foregå, og oplys kontaktoplysninger til eventuelle øvrige parter som leverandøren skal kommunikere med.

6.6 Ibrugtagning af alternativ driftslokation

Formålet med denne handlingsplan er at sikre en hurtig og effektiv overgang til en alternativ driftslokation. Der henvises til Ejendomscenter Jammerbugt beredskabsplan. Kommunikationen foregår mellem IT-Beredskabskoordinator og Ejendomscenter Jammerbugt.

Nr.	Handling
1	**Kontakt retableringsteam** Kontakt retableringsteamet, hvis det ikke allerede er sket. Retableringsteamet bør flytte til den alternative driftslokation.
2	**Kontakt alternativ driftslokation** Kontakt den alternative driftslokation og aftal flytningen.
3	**Flyt til alternativ driftslokation** Foretag flytningen til den alternative driftslokation.
4	**Fremskaf backup mv.** Fremskaf backup og øvrige nødvendige aktiver, som har været opbevaret på en ekstern lokation, f.eks. adgangskoder, nøgler mv.
5	**Vurdér om infrastruktur kan genbruges**

Nr.	Handling
	Foretag en vurdering af, om noget af den eksisterende infrastruktur kan genbruges på den alternative lokation.
6	**Viderestil telefonopkald** Foretag viderestilling af telefonopkald, så de kan modtages på den alternative lokation.
7	**Kontrollér driftsmiljø** Kontroller at driftsmiljøet på den alternative lokation er i overensstemmelse med behovet for det udstyr, der ønskes opsat.
8	**Vurder behov for yderligere udstyr mv.** Vurder om der er behov for at anskaffe yderligere udstyr eller foretage ændringer på driftslokationen, f.eks. hævning af gulve, adgangskontrol mv.

Planen omfatter følgende lokationer, som indeholder infrastrukturs komponenter relateret til omfattede services, eller af andre årsager kan forventes at tages i brug som følge af et site nedbrud:

Lokation	Adresse	Beskrivelse
Aabybro	Toftevej 43 9440 Aabybro	Serverrum
Brovst	Borgervænget 12 9460 Brovst	Serverrum
Fjerritslev	Danmarksgade 3 9690 Fjerritslev	Backup system

Adgang til bygning er dokumenteret i ”Alarm og koder til administrationsbygninger” på Microsoft Teams, Sekundær på N: som henvist i afsnit ”1.3 Relaterede dokumenter”

6.7 Hardwarerelaterede planer

I situationer, hvor det eksisterende hardware eller infrastruktur ikke kan genbruges, skal der fremskaffes nyt udstyr til at retablere IT driften. I de efterfølgende planer fremgår de respektive løsninger og afledte retableringsaktiviteter.

6.8 Servere

Nr.	Handling
1	**Anskaf og installer backup** Fremskaf backup og installer denne i udviklingsmiljøet.
2	**Fastlæg datatab og informer IT-Beredskabskoordinatoren** Fastlæg omfanget af datatabet (RPO) og informer systemejere og brugerne om, hvor stort et tidsrum, der mangler i systemet.
3	**Fastlæg forventede retableringstid og informer IT-Beredskabskoordinatoren** Fastlæg den forventede retableringstid og informer IT-Beredskabskoordinatoren. Hvis retableringstiden forlænges, skal IT-Beredskabskoordinatoren informeres STRAKS.
4	**Implementer almindelige driftskontroller** Implementer de almindelige driftskontroller og konfigurationer såsom backup, overvågning mv.
5	**Informer IT-Beredskabskoordinator** Informer IT-Beredskabskoordinatoren når systemet er retableret.

6.9 Netværk

Nr.	Handling
1	**Bestem hvilket områder der er ramt** Foretag en undersøgelse af, hvilke områder som er ramt af nedbrud.
2	**Kontakt eventuelle leverandører** Kontakt leverandøren og vurder situationen.
3	**Iværksæt undersøgelse af årsagen til nedbruddet** Assister leverandøren med at identificere årsagen til nedbruddet.
4	**Planlæg retableringen** Planlæg hvordan der retableres.
5	**Foretag retablering** Foretag den planlagte retablering, f.eks. udskiftning af defekt hardware.
6	**Informer IT-Beredskabskoordinator** Informer IT-Beredskabskoordinatoren og kommuniker til øvrige interessenter.

6.10 Plan for virus eller hackerangreb

Handlingsplanen for virus- eller hackerangreb skal sikre en effektiv indsats i tilfælde af virusangreb eller hackerangreb.

Nr.	Handling
1	**Vurder situationen** Hvis der er risiko for, at data kan blive kompromitteret, afbrydes internetforbindelsen. Vurder om der er behov for at lukke systemer for at undgå spredning af angrebet.
2	**Luk systemer** Vurder, om der er behov for at lukke systemer for at undgå spredning af angrebet. Informer relevante systemejere, brugere mv.
3	**Informer relevante systemejere, brugere m.v.**
4	**Iværksæt undersøgelse** Iværksæt en undersøgelse af angrebet. Vurder om der er behov for ekstern hjælp til afdækning og genetablering
5	**Skift adgangskoder** Det vurderes, om og hvilke adgangskoder der bør skiftes.
6	**Aktiver ekstra systemlogning** Det vurderes, om der bør iværksættes ekstra logning af systemer og netværk for at opklare og indsamle beviser om hændelsen.
7	**Kontakt leverandører** Hvis de ramte områder driftes eksternt, kontakt leverandørerne.
8	**Kontakt myndigheder** Det skal vurderes, om der skal foretages politianmeldelse, og om der er andre myndigheder, som bør kontaktes. Hvis der er sket brud på fortrolighed og integritet, skal dette anmeldes til Datatilsynet inden 72 timer (se scenarie for brud på persondatasikkerhed).
9	**Informer interessenter** Eventuelle øvrige interessenter informeres. Hvis der er sket brud på fortrolighed og integritet kan der være borgere, der skal informeres.

6.11 Plan ved brud på persondatasikkerhed

Scenarie for brud på persondatasikkerhed skal sikre den korrekte kommunikation til interessenter samt hindre en gentagelse.

Som udgangspunkt skal alle brud på persondatasikkerhed anmeldes til Datatilsynet. Kun hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal der ikke ske en anmeldelse.

Nr.	Handling
1	**Vurder situationen** • Hvilken type brud er der sket? Er der sket tab af oplysninger, brud på fortrolighed eller en integritetskrænkelse • Oplysningernes art og omfang • Risikoen for at den registrerede kan identificeres • Konsekvenserne for den registrerede • Omfatter bruddet særlige registrerede (børn eller særligt udsatte) • Antallet af berørte fysiske personer
2	**Opdater Rød Mappe / Log** Skabelon til Rød Mappe /½ Log, og kun ved store generelle brud. Enkeltmandsbrud håndteres ikke i dette forum, men som enkeltmands Datassikkerhedsbrud med log via DPO
3	**Anmeld brud til Datatilsynet** Anmeldelse skal ske uden unødig forsinkelse og senest 72 timer efter at bruddet er opdaget.
4	**Udarbejd kommunikationsplan** Orienteringen til borgeren bør som minimum: • ske uden unødig forsinkelse • ske i et klart og forståeligt sprog • beskrive karakteren af bruddet • beskrive kategorien af oplysninger, der er kompromitteret • beskrive sandsynlige konsekvenser af bruddet • beskrive hvad vi har gjort for at begrænse skaden • indeholde kontaktoplysninger på chef for området eller DPO, for yderligere oplysninger
5	**Risikovurdering** Gennemfør en risikovurdering på baggrund af bruddet eller revider den eksisterende risikovurdering for at forebygge at hændelsen gentages.

7 Normalisering

Hvilke planer, der er behov for ved genetablering, afhænger af den konkrete beredskabssituation samt kommunens organisering af IT-driften. Der henvises til relevante SRP'ere for genetablering af kernesystemer.

7.1 Genetablér processer

Forvaltningsprocesser genoptages som før hændelsen. Der skal tages højde for eventuelle ændringer, der måtte have påvirket processerne fremadrettet.

7.2 Afslut nødplaner

De manuelle nødplaner afsluttes og forretningens afdelinger bedes anvende it-systemerne fremadrettet.

7.3 Afslut beredskab

IT-Beredskabsleder og formanden for beredskabet beslutter, om beredskabet kan afsluttes, så snart normaldrift er blevet reetableret. Denne beslutning tages i samråd med systemejere og resten af beredskabsledelsen. I tilfælde af skade på udstyr eller lokationer, planlægges udbedring af disse, for at bringe miljøet tilbage til normale tilstande. Ledelsen og brugerne informeres om at situationen er normal.

Når beredskabet afsluttes, afsluttes beredskabsloggen

7.4 Evaluering af beredskab

Beslutninger og handlinger fra beredskabshændelsen diskuteres i beredskabsledelsen 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 og Rød Mappe / Log opdateres.

8 Forankring, vedligeholdelse og øvelse af IT-beredskabsplan

Løbende fokus på beredskabet er den bedste metode til forankring. Forankring omfatter

- Løbende øvelser/afprøvning af hele eller dele IT-beredskabsplanen og SRP
- Uddannelse og træning
- Vedligeholdelse

Eksempel på en enkel øvelse, som ikke kræver omfattende ressourcer, er en skrivebordstest / -øvelse. Denne type test/øvelse kan også benyttes til uddannelse. Kommunikationsplansøvelse er også enkel og sikrer, at de ansvarlige ved, hvem de skal kontakte.

Vedligeholdelse er med til at sikre, at recovery-kompetencer og -viden inden for de forskellige services som minimum er beskrevet. De nødvendige ressourcer og tid til opdateringer og vedligeholdelse af IT-beredskabsplan er absolut vigtige.

IT-beredskabsplanen eller udvalgte System Recovery Planerne skal mindst en gang om året øves, for at sikre, at den er faktuel, og at beredskabsorganisationen har kendskab til den. Foretages der væsentlige ændringer i organisationens it-anvendelse eller organisationen bør IT-beredskabsplanen desuden altid afprøves. "Disaster Recovery Test" dokumentet skal bruges til dokumentation for udførelse af test /øvelse.

8.1 Øvelse af IT-beredskabsplan

På Microsoft Teams afrapporteres og dokumenteres der samlet for den gennemførte øvelse og opfølgninger. Den samlede dokumentation for test / øvelse overføres til IT-beredskabslederen der har ansvaret for review og evalueringer. Der udarbejdes skrivebordstest/ -øvelse eller reelle øvelsesscenarier med målbare objektiver (hvis muligt).

Da mangelfulde kommunikationsprocesser ofte er kilde til fejl i beredskabsindsatsen, skal kommunikation øves samtidigt. Erfaringer med kommunikationsopgaverne tilsvarende: "hvad er der sket, "hvem er berørt", "hvornår forventes fejlen rettet", "hvornår udsendes ny information" skal bruges til forbedringer af IT-Beredskabsplanen.

Frekvens	Øvelses type	Omfang
Årligt	Skrivebordstest / Øvelse	Der foretages ikke afbrydelser i it-driften. Med udgangspunkt i et foruddefineret scenarie foretages et skrivebordsøvelse. Øvelsen afprøver bl.a. eskaleringsprocessen og sikre, at kontaktoplysninger mv. er korrekte. Der foretages en simulering af kommunikationsplanerne
Mininum Hvert 2 år	Real test / Øvelse	Der er afbrydelse it IT-driften Der foretages en fuld test /øvelse af IT-Beredskabsplan og en eller flere SRP, hvor et eller flere systemer retableres med udgangspunkt i leverandørens retableringsplaner. Kommunikationsplanerne afprøves også

8.2 Uddannelse og træning

Hvor ofte de faste periodiske test skal foregå, er en ledelsesbeslutning. Det bør dog minimum være hvert år ved kritiske it-services, samt ved ændringer i organisationen og udskiftning af nøglepersoner i beredskabsplanen. Dette er også afhængige af, hvor godt de involverede personer forventes at kende beredskabsplanen. Der bør være kalender påmindelser når det er tid til at opdatere eller teste beredskabsplanerne.

Ved at teste beredskabsplanen er en god måde at oplære på. Endvidere er det vigtigt at sikre, at de udpegede medarbejdere har de nødvendige beslutningskompetencer.

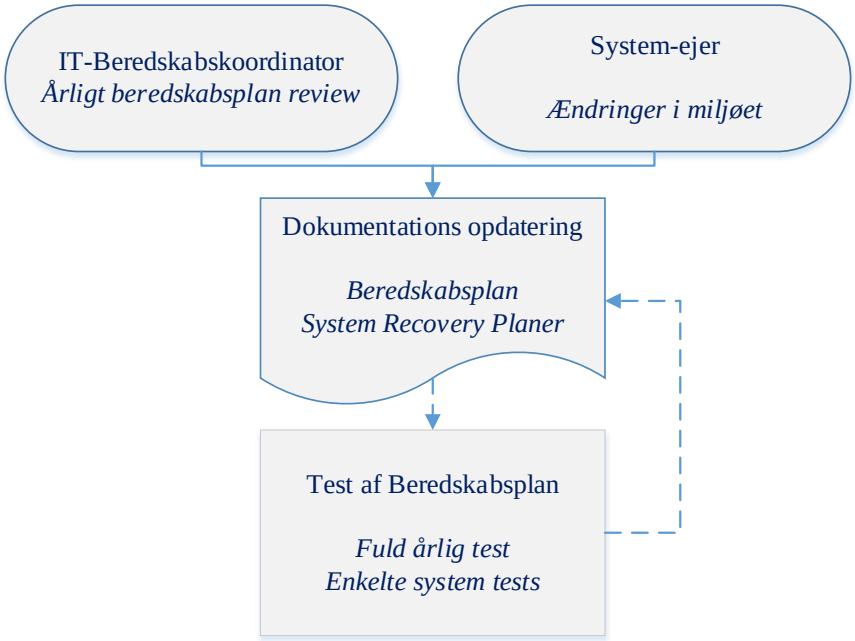
8.3 Planlægning af test

Testskema	Frekevens	Varighed	IT-Beredskabskoordinator	IT-Beredskabsleder	Reetableringsteam/ leverandører	Kommunikationsansvarlig e	Alle medarbejder	IT Nyansatte
Forankring af IT-beredskab								
Uddannelse vedr. beredskabplan	Årligt	1 time		X	X	X		X
Uddannelse vedr. IT-beredskabplan (evt. eksternt)	Årligt	½ dag	X					
Beredskabsplan								
Gennemgang af beredskabsplan	Årligt	2 timer	X	X	X			
Test								
SRP 1 (valgfrit)	Årligt	3 timer	X	X	X	X		
SRP 2 (Valgfrit)	Årligt	3 timer	X	X	X	X		
Test af kommunikationsplan	Årligt	2 timer	X	X	X	X		
Fuld test	Hvert 2 år	1-5 timer	X	X	X	X	X	

9 Vedligehold og opdatering af IT-Beredskabsplan

9.1 Vedligehold af IT-Beredskabsplan

IT-beredskabsplanen skal som et minimum evalueres årligt inklusiv godkendelse af ledelsen. Alle System Recovery Planer samt teknisk relateret dokumentation bør løbende vedligeholdes af serviceejerne inklusiv gennemgang af en kollega eller Level 3 support.



9.2 Opdatering af planer

IT-beredskabsplanen skal opdateres mindst en gang om året i forlængelse af den årlige afprøvning. Planen bør desuden opdateres, hvis der sker væsentlige ændringer i IT-anvendelsen (f.eks. en ny leverandør), beredskabsorganisationen m.v.

9.3 Ordforklaring

Det er nyttigt at definere en række centrale begreber. Definitionerne er opstillet med det formål at klarlægge begrebsanvendelsen, som er anvendt i dette dokument.

Begreb	Uddybning
Genopretningsplaner - SRP	SRP – System Recovery Plan er et teknisk dokument, der beskriver hvordan et givent system eller enhed skal genoprettes eller geninstalleres helt fra bunden. Hensigten er, at ressourcer uden forhåndskendskab til systemet eller enheden,skal kunne genoprette eller geninstallere.
RTO / Recovery Time Objective	Recovery Time Objective er et udtryk for den tid, der maksimalt må gå, fra en hændelse er opstået, til IT-understøttelsen igen skal være mulig. Med andre ord: hvor lang tid kan Jammerbugt Kommune tåle at være nede, før der iværksættes nødplaner andre steder
RPO / Recovery Point Objective	Recovery Point Objective er et udtryk for det maksimalt tolererede datatab – dvs. tiden fra seneste backup til hændelsen indtræffer, så alle de data, der er indtastet i dette mellemrum er gået tabt.
Beredskabslog skabelon	Skabelonen anvendes til brug for den log, der skal føres under en beredskabssituation. Loggen føres for at dokumentere forløbet af bredskabssituationen.
Beredskabsrapport skabelon	Skabelonen anvendes til brug for udarbejdelse af en beredskabsrapport i forbindelsen med en hændelse, der har aktiveret beredskabet eller en test af beredskabet. Sker der en hændelse bør beredskabsrapporten indeholde en beskrivelse af hændelsen samt en evaluering af denne.
Disaster Recovery Test	Skal bruges ved test af beredskabsplanen eller SRP
Kommunikationsplan	Service Level Agreements er de aftaler der er indgået mellem ”brugerne” og ”leverandørerne” af en service. Formålet er at sikre en gensidig forståelse mellem de 2 parter.
Action Cards	I et action card beskrives de konkrete arbejdsgange ned på funktionsniveau og med kontaktoplysninger på de personer, der skal inddrages.
Risikoanalyse	Risikoanalyse er en risikovurdering for alle væsentlige systemer og data i Jammerbugt Kommune
Incident	En hændelse der sker, som skal registreres og udbedres
Rød Mappe / Log	Jammerbugt Kommunes journal og registrering omkring en hændelse/incident

10 Godkendelse og kendte problemstillinger

Her dokumenteres kendte mangler i IT-beredskabsplanen:

- IT-beredskabsplanen og alle relaterede dokumenter er placeret på interne servere og Microsoft Teams. Microsoft Teams er afhængige af funktionel on-premise Active Directory og ADFS og Jammerbugt Kommune skal sikre bagdør adgang såfremt Active Directory og ADFS ikke er funktionel.
- IT-Beredskabslederen og IT-koordinatoren har flere ansvarsområder og man bør have en sekundær mulighed, hvis de ikke kan kontaktes.

10.1 Optimeringsmuligheder

Herunder er der opridset mulige optimeringsmuligheder, som kan forbedre processen i forbindelse med en beredskabssituation:

- Få dokumenteret forretningsnødplaner for kritiske forretningsprocesser
- Skabelon for Ekstern kommunikation kan udarbejdes, således den hurtigt kan udfyldes.
- FAQ med forventelige spørgsmål og svar i en beredskabssituation kan udarbejdes på forhånd.
- Få beskrevet Actions Cards for systemerne
- Få beskrevet Actions Card for beredskabsplan som helhed i slutning af dette dokument. Beskrivelse af generel gennemgang af hele planen samt opdatering af bilag hertil.

10.2 IT-beredskabsplan godkendelse

Dato for godkendelse: _____ Lokation: _____

_____

<Ansvarlig>, <Titel>