Delplan for Sekretariat for Digitalisering til samlet beredskabsplan

1. Centrets opgaver og målgrupper

Sekretariat for Digitalisering er direktionens og kommunens sekretariat til varetagelse af den digitale udvikling. Vi udvikler strategier, mål, rammer og arkitektur for kommunens digitalisering. Desuden støtter og rådgiver vi forretningsenhederne i processer om udvikling, udbud og anskaffelser på det digitale område. S-DIG er bindeled til IT-Forsyningen, som varetager kommunens drift og support.

I beredskabssammenhæng er Sekretariat for Digitalisering ansvarlig for adgangs-styring, datavaliditet, databeskyttelse og herunder afværgeforanstaltninger og evt. genopretning.

IT-Forsyningen står for al teknisk drift og nødforsyning med IT i forbindelse med kriser.

I en situation, hvor beredskabet træder i kraft, er Digitaliseringssekretariatet koordinerende og styrende i forhold til IT-Forsyningen. Det betyder, at alle henvendelser skal gå igennem Digitaliseringssekretariatet.

2. Beskrivelse af centrets kritiske funktioner og situationer

Sekretariat for Digitalisering er ansvarlig for adgangsstyringen til Kommunens forretningskritiske systemer. Det vil sige de systemer, der styrer brugernavne, password og brugerrettigheder.

Sekretariat for Digitalisering er ansvarlig for at sikre, at data er valide og databehandlingen sker i overensstemmelse med den gældende lovgivning.

Hvis data bliver korrupte eller fx inficeres af virus, så er Sekretariat for Digitalisering ansvarlig for at få identificeret problemets årsag, omfang og efterfølgende sikre genoprettelse af datakvaliteten.

Hvis der sker datalæk, er Sekretariat for Digitalisering ansvarlig for at identificere, analysere, informere og evt. anmelde datalækket til Datatilsynet.

3. Beskrivelse af kritiske faktorer, der skal opretholde de kritiske funktioner

IT-Forsyningens drift af kommunens netværk, serverpark og data skal fungere. Det vil sige, at de digitale services vedvarende skal være tilgængelige på alle relevante lokationer i Ballerup Kommune.

4. Beskrivelse af risikofaktorer, der kan påvirke de kritiske funktioner?

Længerevarende strømsvigt og/eller netværksnedbrud kan resultere i manglende adgang til adgangsstyringen og herved adgangen til de forretningskritiske systemer.

Hvis ikke informationen om evt. virus angreb bliver kommunikeret ud til organisationen, kan der være risiko for yderligere spredning af vira.

5. Resumé af indsatsplaner

Sekretariatet udarbejder indsatsplanen "Sikring af forretningskritiske IT-systemer og kommunikation".

Indsatsplanen skal:

- sikre kommunikation for nødberedskabet og tydelige kommando- og handlingsveje i forhold til IT-Forsyningen.
  Den primære indsats består i etablering af nødtelefoner og procedure for hvem der gør hvad i henholdsvis IT-Forsyningen og S-DIG.

- skal sikre, at nødprocedurer for kritiske funktioner for forretningsenheder iværksættes.
  Indsatsen består fx i udprintning af livsvigtige lister over medicin, madudbringning m.m. samt etablering af backupsystemer.

- sikre at genetablering af de forretningskritiske IT-systemer prioriteres højest, herunder reetablering af adgangsstyring, muligheder for at tilgå systemer, samt genetablering af mails.
  Indsatsen består i ajourføring og kontrol af hvilke systemer der er forretningskritiske, samt planer for hvordan nødproceduren er for hvert enkelt system hvilket koordineres med IT-Forsyningen.

- sikre hurtig genetablering af den normale drift via iværksættelse af plan herfor.

6. Beskrivelse af, hvordan centret håndterer indkommende information om hændelser

Ved kritiske hændelser skal centrene henvende sig til sikkerhedskoordinatoren eller digitaliseringschefen via mail eller telefon.

Hvis disse er ude af drift skal centrene kontaktes på nødtelefonen.

7. Ressourceoversigt

Sekretariat for Digitalisering har udlånsbærbare computere og mobiltelefoner til rådighed ved kritiske hændelser.

I serverrummet vil der være mulighed for print af livsvigtige oplysninger.

8. Løbende sikring og forebyggende tiltag

Sekretariat for Digitalisering opdaterer listen over forretningskritiske systemer og sørger for, at de berørte centre rådgives i forhold til valg af nødløsninger ved systemnedbrud.

Sekretariat for Digitalisering søger for at alle centre løbende informeres om retningslinjer for IT-sikkerhed og holder løbende koordinerende møder med de lokale digitaliseringsledere.