

IT-BEREDSKABSPLAN I JOBCENTER OG BORGERSERVICE - 2026



INDLEDNING

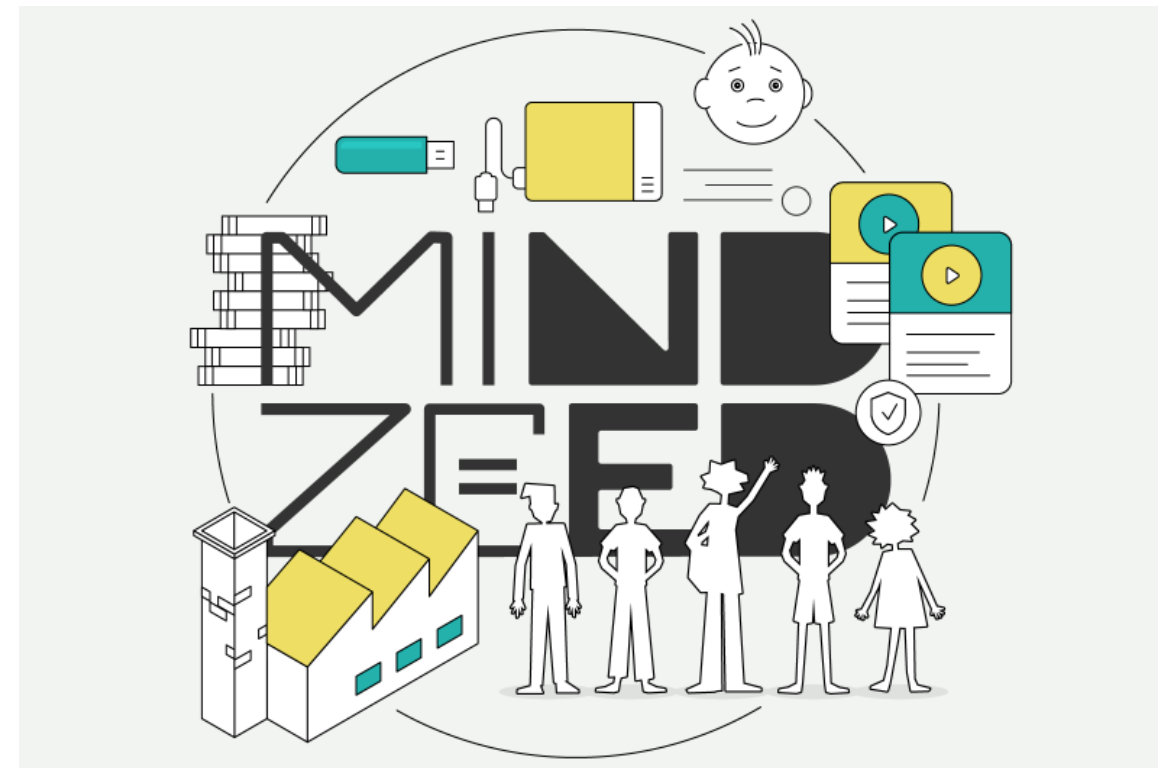
Informationssikkerhed på medarbejderportalen

- På Aabenraa Kommunes medarbejderportal findes en samlet side om [informationssikkerhed](#) . Her har medarbejdere adgang til gældende politikker og regler samt information om databeskyttelse, hændelseslog og håndtering af digitale trusler.
- Aabenraa Kommune har vedtaget en central informationssikkerhedspolitik med tilhørende regler, som fastlægger de overordnede rammer for informationssikkerhed og databeskyttelse. Siden indeholder desuden vejledning til medarbejdere om sikker brug af digitale løsninger, herunder håndtering af phishing og mobile enheder, samt initiativer for viden og uddannelse i beskyttelse af borgernes data.

Jobcenter og Borgerservice fremhæver følgende:

MINDZEED – E-LÆRING TIL INFORMATIONSSIKKERHED

- Det er vigtigt, at alle medarbejdere løbende uddanner sig inden for informationssikkerhed. Derfor har direktionen i Aabenraa Kommune besluttet, at alle ansatte med IT-adgang skal gennemføre et fælles onboardingmodul bestående af syv korte kurser.
- Efterfølgende vil forskellige medarbejdergrupper modtage kurser, der er målrettet deres specifikke arbejdsområder. Kurserne er obligatoriske for alle medarbejdere, og der udsendes ugentlige påmindelser, indtil kurserne er gennemført.
- Det er et fælles ansvar at gennemføre kurserne. De styrker os i forebyggelsen af cyberangreb og understøtter en sikker og korrekt håndtering af borgernes data.
- Du finder flere oplysninger om [Mindzeed](#) på medarbejderportalen.



CYBERANGREB, SIKKERHEDS- OG DATABRUD

Sikkerhedsbrud og sikkerhedshændelser

En hændelseslog er en registrering af alle sikkerhedshændelser – fra de helt små hændelser til større sikkerhedsbrud, som skal indberettes til Datatilsynet.

Du kan læse mere om håndtering af [Sikkerhedshændelser og -brud](#) på medarbejderportalen. På siden findes også et link til indberetning af en sikkerhedshændelse.

Beredskabsplan ved større databrud eller cyberangreb

IT-afdelingen har udarbejdet en central beredskabsplan ved større datalæk, databrud eller cyberangreb. Planen omfatter alle forvaltninger og afdelinger, herunder decentrale enheder som KIS i Jobcenter og Borgerservice.

Der findes et direkte link til kommunens beredskabsplan på medarbejderportalen.

Hvis en medarbejder i Jobcenter og Borgerservice får mistanke om, at der er sket et databrud eller cyberangreb, skal nærmeste leder og systemkoordinatoren kontaktes, som herefter kontakter kommunens eksterne DPO i samarbejde med IT-afdelingen. Lækkets omfang og alvor vurderes, og det afgøres, om der er grundlag for at nedsætte en taskforce.



IT- ELLER SYSTEMNEDBRUD

Hvis der sker et IT-nedbrud eller et system er utilgængeligt i kortere eller længere tid, vil det i perioden ikke være muligt at ajourføre borgersager. Der vil ikke være adgang til borgerens sag, kontaktoplysninger eller mulighed for at træffe afgørelser.

For alle IT-systemer er der foretaget risikovurderinger, som vurderer sandsynligheden for sikkerhedsbrud ud fra tre grundlæggende begreber:

- Fortrolighed
- Tilgængelighed
- Integritet

Ved systemnedbrud følges samme procedurer som ved databrud eller cyberangreb. Systemleverandøren kontaktes for information om tidshorisont for genetablering af systemet.



NEDBRUD PÅ EL-NETTET

Ved nedbrud på el-nettet vil mulighederne for drift i Jobcenter og Borgerservice være så begrænset, at almindelig betjening ikke kan opretholdes.

Ved el-nedbrud bortfalder adgangen til kablet og trådløst netværk samt strømforsyning til pc'er og andre enheder uden indbygget batteri. Der henvises til Bilag I, som skal betragtes som et dynamisk værktøj.

Sagsbehandling, journalisering og øvrige digitale tjenester vil ikke være tilgængelige, da hovedparten af betjeningen foregår digitalt, og systemer med on-site-løsninger ikke kan tilgås.

Flere løsninger vil dog fortsat være funktionelle, da de er webbaserede og kan tilgås uden for de berørte områder. M365-baserede apps kan anvendes, så længe der er netværksadgang, og data er gemt på SharePoint eller OneDrive. I visse tilfælde kræver adgangen, at den anvendte pc er tilsluttet VPN.

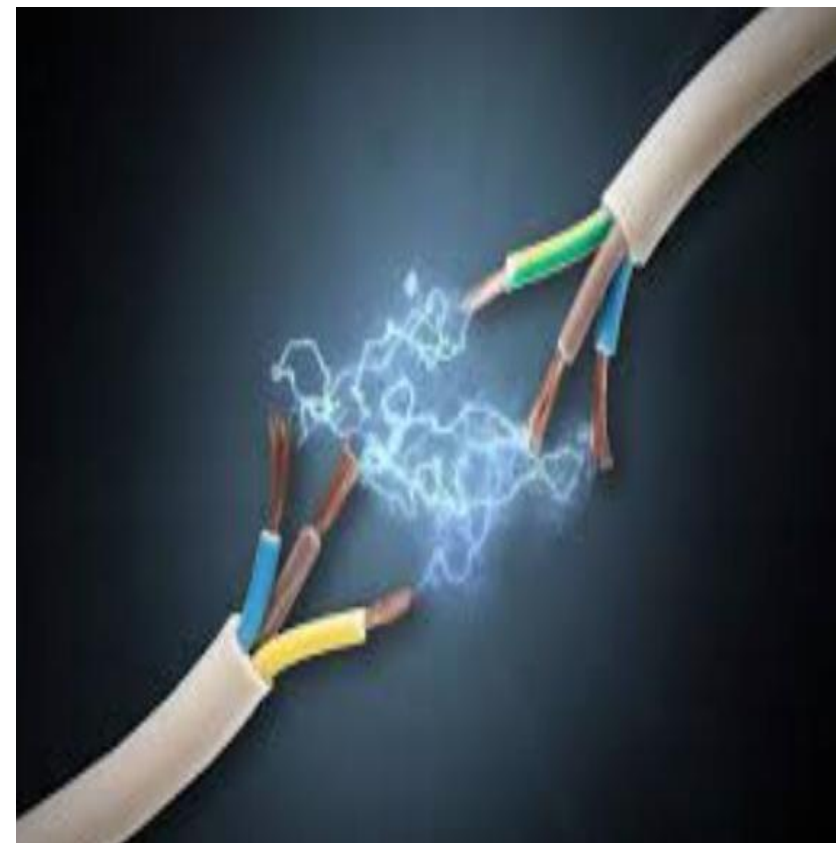
Bærbare enheder vil i nogen grad kunne anvendes, men batterilevetiden vil være begrænset. Alle ikke-nødvendige funktioner skal straks deaktiveres, og skærmens lysstyrke reduceres til et minimum for at forlænge batterilevetiden. Dette omfatter bl.a. WiFi, Bluetooth, NFC og ikke-kritiske apps.

Andre konsekvenser ved el-nedbrud er, at elektroniske døre samt brand- og overfaldsalarmer vil være ude af drift.

Der foreligger en oversigt med forslag til håndtering af situationen, som viser, at meget begrænsede dele af Borgerservice kan opretholdes ved el-nedbrud (Bilag I).

Borgere henvises til at gå hjem. Borgere med bookede tider kan aflyses via masse-SMS fra Frontdesk (da løsningen er off-site), og en dørvagt afviser nyankomne borgere, som ikke har modtaget beskeden.

Medarbejdere orienteres og sendes hjem, bortset fra en mindre beredskabsgruppe, der via mobiltelefoner, bærbare pc'er og mobilnet understøtter det generelle beredskab.



KONTAKTCENTERET



Kontaktcenteret består af to selvstændige systemer, som suppleres af intern telefoni via Microsoft Teams:

- Samwin/Jansson til omstilling og telefonhåndtering
- InDialog – en machine learning-baseret telefonrobot til grundlæggende hjælp og omstilling

Systemerne er uafhængige af hinanden og er placeret uden for kommunen. De er derfor underlagt separate el-net og netværk, hvilket betyder, at det ene system kan fungere, hvis det andet er ramt af nedbrud.

Ved lokalt el- eller netværksnedbrud vil kontaktcenteret blive berørt, og borgere, virksomheder m.fl. vil ikke kunne kontakte Aabenraa Kommune via hovednummeret, før medarbejdere har genetableret internetforbindelse via hotspot eller en ekstern forsyning, fx fra hjemmearbejdsplads.

Telefonrobotten kan i krisesituationer understøtte kommunen og kontaktcenteret ved at give borgere information om nedbrud, nød- og evakueringsplaner samt anden relevant information.

Ved nedbrud kan medarbejdere via hjemmearbejdsplads eller hotspot logge på VPN og Teams og besvare opkald via pc eller mobiltelefon – både på fastnet- og mobilnumre.

Beredskabsplanen indebærer, at forvaltningerne hurtigst muligt informeres, og at borgere orienteres via medierne, mens kontaktcenteret omplaceres til en lokation med strøm og netværk eller alternativt anvender batteridrevne hotspots. Kontaktcenteret vil herefter i begrænset omfang kunne hjælpe og vejlede borgere. Omstilling til medarbejdere forudsætter, at de pågældende selv har sikret, at de er kontaktbare under nedbrud.