POLITIK FOR INFORMATIONSSIKKERHED

for
Brønderslev Kommune

Godkendt af Byrådet den 6. oktober 2021

BRØNDERSLEV KOMMUNE

5. revision – august 2021

Indhold

1. Målsætning/formål

Politik for informationssikkerhed skal til enhver tid understøtte Brønderslev Kommunes vision og de strategiske mål, samt sikre efterlevelse af databeskyttelsesforordningen (GDPR) og øvrig lovgivning, som er forbundet med offentlig forvaltning.

Hensigten med Politik for informationssikkerhed og Regulativ for informationssikkerhed er desuden at tilkendegive over for alle, som har en relation til Brønderslev Kommune, at anvendelse af informationer og informationssystemer er underlagt standarder og retningslinjer.

Brønderslev Kommune ønsker derfor at opretholde og løbende udbygge et sikkerhedsniveau på højde med de krav, som skitseres i 'Den fællesstatslige standard for informationssikkerhed' (ISO 27001 basale krav).

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Brønderslev Kommune fremstår troværdigt overfor borgere såvel som medarbejdere, kommunale og statslige instanser samt øvrige forretningsforbindelser.

IT-systemer betragtes, næst efter medarbejderne, som Brønderslev Kommunes mest kritiske ressource. Der lægges derfor vægt på driftssikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Målene er derfor, at:

- opnå høj driftssikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab - TILGÆNGELIGHED
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

Ovenstående mål konkretiseres i risikovurderinger i Brønderslev Kommune.

Regler og retningslinjer fra regulativet for informationssikkerhed skal løbende indarbejdes i de relevante gældende regler på personalepolitikkens område.

2. Omfang

Sikkerhedskonceptet omfatter følgende:

- En politik for informationssikkerhed, der godkendes af Byrådet på baggrund af indstilling fra Datasikkerhedsgruppen.
- Et regulativ for informationssikkerhed, der uddyber politik for informationssikkerhed, fastlægges af Datasikkerhedsgruppen.

- En kortfattet og overordnet informationssikkerhedshåndbog, med sigte på den brede og generelle sikkerhedsinformation til medarbejdere.

3. Gyldighedsområde

Politik for informationssikkerhed er gældende for alle Brønderslev Kommunes informationsrelaterede aktiviteter, uanset om disse udføres af ansatte i Brønderslev Kommune eller af samarbejdspartnere. Dette inkluderer alle data behandlet af og for Brønderslev Kommune.

Det har Brønderslev Kommunes bevågenhed at efterleve gældende lovgivning og krav til informationssikkerhed, derfor sker der en revidering af Politik og Regulativ for informationssikkerhed en gang årligt.

Byrådet vedtager kommunens politik for informationssikkerhed.

4. RISIKOVURDERING OG -HÅNDTERING

Et af de primære grundlag for sikkerhedsniveauet i Brønderslev Kommune er risikovurderinger. Væsentlige informations- og fysiske aktiver har en risikovurdering.

Der sker en årlig revurdering af risikovurderingerne, men flere hvis der måtte opstå behov herfor, f.eks. på grund af nye opdagede risici.

Risikovurderinger tager udgangspunkt i 2 faktorer. ”Sandsynligheden for at hændelsen optræder” samt ”Konsekvenser i form af tab hvis hændelsen indtræder”.

Med udgangspunkt i risikovurderingerne der ligger over det accepterede risikoniveau, fastsættes der håndtering af risikoen af systemejer/ledelsen.

5. ORGANISERING AF INFORMATIONSSIKKERHED

Informationssikkerhed skal være organiseret for at være effektivt.

Som udgangspunkt skal informationssikkerheden være indbygget i kommunens forretningsgange og procedurer.

Direktionen har det overordnede ansvar for informationssikkerheden, og lederforum sætter den strategiske retning i Brønderslev Kommune. Organisering og ansvar er beskrevet i tilhørende bilag.

6. MEDARBEJDERSIKKERHED

Alle medarbejdere skal senest på tiltrædelsestidspunktet og som en integreret del af ansættelsesaftalen være bekendt med, at vedkommende er underlagt reglerne om tavshedspligt, jfr. Gældende lovgivning på området. Regler for fx opbevaring, ansvar og sanktioner mv. er defineret yderligere i regulativet for informationssikkerhed.

7. STYRING AF AKTIVER

Der foretages styring af Brønderslev Kommunes aktiver som fx Computere, telefoner samt databærende medier.

8. ADGANGSSTYRING

Adgang til Brønderslev Kommunes it-systemer beskyttes af autorisationssystemer, som har til formål at sikre adgange. Brønderslev Kommune fastlægger ud fra lovmæssige, organisatoriske og tekniske forhold, hvordan de overordnede adgangskrav til systemet skal være.

9. FYSISK SIKRING OG MILJØSIKRING

Brønderslev Kommunes serverrum er knudepunkt for kommunens fysiske infrastruktur. Den fysiske infrastruktur er sikret ved redundans. Serverrummet er fysisk beskyttet mod brand og indtrængen af uvedkommende personer.

10. DRIFTSSIKKERHED

Stabil og sikker it-drift er afgørende for Brønderslev Kommune. En høj driftssikkerhed og pålidelig administration er væsentlig, og der bør være dokumenterede retningslinjer med angivelse af ansvar og vedligeholdelse. Driftsafbrydelser kan forekomme, hvorfor beskrevne beredskabsplaner skal medvirke til genetablering og sikring af normal drift.

Netværkets tilgængelighed, ydeevne, oppetid og driftsstabilitet sikres ved redundans.

10.1 Malwarebeskyttelse

IT-systemer er beskyttet af autoriseret produkter til beskyttelse mod malware og computervirus.

10.2 Backup

Der skal foretages en sikkerhedskopiering, som sikrer, at alle Brønderslev Kommunes essentielle data og programmer kan gendannes i tilfælde af fejl og uheld.

10.3 Logning og TV-overvågning

Hvor det er muligt, skal driftslogning etableres til kontrol og eftersporing af, hvad der sker i driftsafviklingsforløbet og netværksstyringen.

Der er udarbejdet retningslinjer for anvendelse af TV-overvågning.

10.4 Hændelseslogning

Hvor det er muligt logges sikkerhedshændelser, fejlhændelser og væsentlige brugeraktiviteter på Brønderslev Kommunes systemer.

10.5 Softwareinstallation i driftssystemer

Inden ibrugtagning af softwareinstallationer, skal driftsafviklingssystemer, netværk og brugersystemer afprøves. Der sker en løbende vurdere af tilgængelige sikkerhedsrettelser.

11. ANSKAFFELSE, UDVIKLING OG VEDLIGEHOLDELSE AF SYSTEMER

Indkøb, udvikling og implementering af nye systemer skal foregå kontrolleret for at undgå en unødvendig forøgelse af risiko for informationssikkerheden. Det skal sikres, at nyanskaffelser ikke giver anledning til konflikt med eksisterende bestemmelser i Politik for informationssikkerhed og databeskyttelsesloven. Ethvert nyt system skal risikovurderes inden ibrugtagning.

12. LEVERANDØRFORHOLD

Eksterne serviceleverandører/samarbejdspartnere skal have minimum samme krav til informationssikkerhed som beskrevet i Brønderslev Kommunes regulativ for informationssikkerhed.

Anvendelsen af ekstern databehandler skal ske med respekt for databeskyttelseslovens retningslinjer.

13. STYRING AF INFORMATIONSSIKKERHEDSBRUD

Der skal forefindes procedurer og beredskabsplaner, som kan sikre en effektiv og kort reaktion på hændelser, der kan true IT-sikkerheden.

14. INFORMATIONSSIKKERHEDSASPEKTER VED NØD-, BEREDSKABS- OG REETABLERINGSSTYRING

Risikostyring og beredskabsplanlægning er nødvendige for at sikre Brønderslev Kommune mod uforudsete hændelser. Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og IT-udstyr. Der sker en årlig revidering af Beredskabsplanen.

15. BILAGSOVERSIGT

Organisation og ansvar