Informations-sikkerhedspolitik

FOR JAMMERBUGT KOMMUNE

JAMMERBUGT KOMMUNE

Versionsstyring

Version	Dato	Ændring	Ansvarlig	Godkendt af
03.02	22-12-2022	Tilføjelse af referencer til supplerende dokumentation	Morten Hedegaard	Chef for Digitalisering, Borgerservice og Indkøb
03.03	02-05-2023	Mindre gennemretning	Morten Hedegaard	Direktion
04.00	29-10-2024	Politikken er revideret i forhold til principperne i ISO 27001/2.	Jacob Holst Pedersen	Direktion

Indhold

1. Formål

Informationssikkerhedspolitikken fastsætter hovedprincipper, målsætninger og ansvaret for it-sikkerheden i Jammerbugt Kommune. Politikken tilstræber at gøre it-sikkerheden realistisk, operationel, logisk, acceptabel og kontrollerbar, og den skal overholde gældende lovgivning og standarder.

Politikken gælder for alle med adgang til kommunens it-systemer, herunder ansatte, politikere og samarbejdspartnere, der alle i det følgende betegnes som "medarbejdere". Alle medarbejdere med adgang til kommunens systemer skal kende og overholde politikken.

Politikken udmøntes i en Informationssikkerhedshåndbog, som følger ISO 27002 og fastlægger kommunens metode til at styre informationssikkerheden. Det samlede overblik over alle kommunens retningslinjer, procedurer mv. opdateres og vedligeholdes løbende i kommunens ledelsessystem for informationssikkerhed (ISMS).

Reglerne beskriver det ønskede niveau for informationssikkerheden i Jammerbugt Kommune og fastlægges af Sikkerhedsteamet. Ud fra Informationssikkerhedshåndbogen udarbejder Sikkerhedsteamet, fagchefer, system- og dataejere relevante procedurebeskrivelser, så det daglige arbejde med kommunens informationer sker i overensstemmelse med det ønskede sikkerhedsniveau.

Formålet med politikken er:

- At sikre data og informationers fortrolighed, pålidelighed, integritet og tilgængelighed for effektiv service til borgere, virksomheder og medarbejdere.
- At it-sikkerhedsniveauet altid overholder lovgivning, kontraktlige krav og god it-skik.
- At tilpasse it-sikkerheden til beskyttelsesbehov og trusler gennem løbende kontroller, uddannelse og information.
- At opretholde it-sikkerhedsniveauet gennem krav til adfærd og målrettet formidling af it-sikkerhed til medarbejderne.

Håndhævelse af it-sikkerhed kræver deltagelse fra alle it-brugere, og alle medarbejdere har ansvar for sikker it-anvendelse. Effektiv formidling af it-sikkerhedsmateriale skal øge brugernes opmærksomhed på it-sikkerheden. Der udarbejdes derfor kortfattet og overordnet håndbog for GDPR og It-sikkerhed med sigte på den brede og generelle sikkerhedsinformation til medarbejdere.

2. Organisation og ansvar

Rollerne og det medfølgende ansvar, som nævnes i informationssikkerhedspolitikken, er alene beskrevet i forhold til informationssikkerheden i Jammerbugt Kommune. Det betyder, at yderligere ansvar tildelt disse roller er beskrevet andetsteds.

Kommunalbestyrelse

Kommunalbestyrelsen har det overordnede ansvar for etablering og vedligeholdelse af en informationssikkerhed, der er tilpasset Jammerbugt Kommunes behov og opfylder krav til lovgivning og god forvaltningsskik. Kommunalbestyrelsen udpeger den øverste it-sikkerhedsansvarlige i Jammerbugt Kommune.

Direktion
Større ændringer til Informationssikkerhedspolitikken vedtages af Direktionen. Direktionen beslutter, hvorvidt ændringerne forudsætter politisk behandling og godkendelse.

Sikkerhedsteam
Der er nedsat et sikkerhedsteam, der på tværs af Jammerbugt Kommunes forvaltninger skal sikre overholdelsen af databeskyttelseslovgivningen. Sikkerhedsteamet er et besluttende organ, som på vegne af direktionen kan træffe beslutninger om implementering af databeskyttelseslovgivningen. Sikkerhedsteamet fastlægger kommunens overordnede kriterier for risikovillighed i forhold til accepterede økonomiske og politiske risici såvel som beslutning om eventuelle forsikringsniveauer med inddragelse af direktionen.

Sikkerhedsteamet består af følgende:

- Den øverste it-sikkerhedsansvarlig (chefen for Digitalisering, Borgerservice & Indkøb)
- Mandatgivne chefer fra hver forvaltning, der hver er ansvarlig for at understøtte egen forvaltning i overholdelsen af de gældende retningslinjer, implementering af sikkerhedsteamets vedtagne indsatser samt sikre udbredelse af de anbefalinger, som sikkerhedsteamet beslutter
- GDPR-koordinatorer fra hver forvaltning, der består af medarbejderrepræsentanter, som de respektive chefgrupper udpeger. I tilfælde af afbud fra de mandatgivne chefer overgår beslutningskompetencen til den pågældende GDPR-koordinator, så sikkerhedsteamet fortsat er beslutningsdygtige
- Sikkerhedsrådgiver
- Databeskyttelsesrådgiver (DPO)

It-sikkerhedsansvarlig
Chefen for Digitalisering, Borgerservice & Indkøb er den øverste it-sikkerhedsansvarlige, hvilket indebærer ansvar for den daglige ledelse og kontrol af informationssikkerhed. Den it-sikkerhedsansvarlige skal præcisere informationssikkerhedsniveauet, opstille procedurer og sikre overholdelse af gældende interne regler. Kommunaldirektøren er stedfortræder for den it-sikkerhedsansvarlige i forhold til dette ansvar.

Chefen for Digitalisering, Borgerservice & Indkøb er desuden ansvarlig for at vurdere de sikkerhedsmæssige og evt. kommunikative aspekter i forbindelse med it-investeringer, ændringer i den anvendte teknologi eller andre forhold, som har indflydelse på it-sikkerheden i kommunen.

De konkrete og operationelle opgaver med den daglige styring af informationssikkerhedsarbejdet er placeret i Digitalisering, Borgerservice & Indkøb og omfatter blandt andet:

- Den tekniske it-sikkerhed, herunder netværkssikkerhed, virusbeskyttelse, driftsstabilitet mv.
- Den administrative sikkerhed, herunder brugeradministration, dataklassifikation, systemejerskab mv.
- Den fysiske sikkerhed i alle bygninger, kommunen råder over, når det berører it-området
- Chefen for Digitalisering, Borgerservice & Indkøb er desuden ansvarlig for at rapportere fejl og afvigelser til kommunaldirektøren.

Databeskyttelsesrådgiver (DPO)
Jammerbugt Kommune har udpeget en databeskyttelsesrådgiver, hvis funktion består i at rådgive, vejlede og overvåge at de databeskyttelsesretlige regler overholdes. Årligt udarbejder

databeskyttelsesrådgiveren en rapport med status på kommunens overholdelse af de databeskyttelsesretlige regler, som fremlægges for Kommunalbestyrelsen.

På møder i sikkerhedsteamet informerer databeskyttelsesrådgiveren om ny lovgivning og praksisser inden for databeskyttelse og informationssikkerhed.

Systemejere

Rollen som systemejer fastlægges i forbindelse med indkøb og implementering af ethvert it-system. Rollen bør besættes af en leder i det fagområde, som har flest brugere af systemet, eller som ejer den opgave, der it-understøttes. Generelle og tværgående systemer ejes i udgangspunktet af chefen for Digitalisering, Borgerservice & Indkøb.

Systemejer har det samlede ansvar for et system. Herved forstås:

- Det økonomiske ansvar
- Det juridiske ansvar herunder det databeskyttelsesretlige ansvar:
- At sikre, at it-systemet overholder databeskyttelseslovgivningen og kommunens egne interne politikker og retningslinjer
- At sikre, at der er indgået en databehandleraftale for systemet
- At sikre håndtering af sikkerhedsbrud i it-systemet
- At sikre, at der udarbejdes en risikovurdering af systemet
- At sikre, at der gennemføres tilsyn med databehandlere
- At sikre, at kun brugere med et arbejdsbetinget behov har adgang til it-systemet, og at brugernes adgange kontrolleres halvårligt
- At sikre, at brugerne har kendskab til gældende regler og instrukser samt at føre tilsyn med, at disse overholdes og udføres.
- At sikre, at logningsniveauet er i overensstemmelse med kommunens retningslinjer og at rapportere fejl og afvigelser som sikkerhedsbrud.
- At sikre, at der halvårligt med vilkårlige mellemrum foretages stikprøver af loggen.
- At sikre, at der er fastsat slettefrister for personoplysninger behandlet i it-systemet, at sletning foretages, samt at der gennemføres kontrol af sletning.
- Ansvar for, at systemet drives på en effektiv og sikkerhedsmæssig forsvarlig måde
- Ansvar for, at systemet understøtter organisation og arbejdsgange, herunder at systemet udfases, når nytteværdien ikke står mål med omkostningerne ved at drive systemet

Systemejeren kan uddelegere opgaverne, men ikke ansvaret, til en systemforvalter, som varetager den daglige vedligeholdelse af systemet.

3. Medarbejdersikkerhed

Medarbejdernes korrekte håndtering af data og udstyr er afgørende for it-sikkerheden i Jammerbugt Kommune. Alle med adgang til kommunens data har ansvar for at beskytte disse mod uautoriseret adgang, ødelæggelse og tyveri.

Nye medarbejdere oprettes som brugere af deres leder og tildeles nødvendige autorisationer. Nærmeste leder orienterer nye medarbejdere om Informationssikkerhedspolitikken, som også findes på TRYK. Alle medarbejdere skal efterleve politikken. Overtrædelser kan medføre sanktioner og håndteres af nærmeste leder, som vurderer overtrædelsens karakter.

Kommunen sikrer løbende uddannelse i databeskyttelse og informationssikkerhed gennem årlige awareness-aktiviteter, som fastlægges af sikkerhedsteamet og udføres af sikkerhedsrådgiveren. Nærmeste leder sikrer medarbejdernes deltagelse og håndterer afdelingens specifikke risici.

Adgang til medarbejderes data og logoplysninger

Jammerbugt Kommune forbeholder sig ret til, med samtykke fra fagchef eller direktør, at foretage gennemgang af alle systemer og personlige/private områder, netværksdrev, mobiltelefoner, i e-mail og andre områder og enheder, som måtte indeholde data fra Jammerbugt Kommune, såfremt der forefindes berettigede interesser for dette. Dette kan være af driftsmæssige behov eller ved berettiget mistanke.

Driftsmæssige behov kan være, at en forvaltnings hensyn til at kunne foretage en kontinuerlig sagsbehandling eller på grund af potentielle alvorlige negative konsekvenser for borgere, fx manglende udbetaling af ydelser eller påvirkninger på fysisk helbred. Inden en medarbejders data tilgås, skal forvaltningen undersøge, om det er muligt at fremskaffe oplysningerne på anden vis. Derudover skal nærmeste ledelse forsøge at indhente samtykke hos den pågældende medarbejder. I de tilfælde, hvor en forvaltning gives adgang til en medarbejders oplysninger, orienteres den øverste it-sikkerhedsansvarlige.

I tilfælde af berettiget mistanke om kriminelle handlinger eller alvorlige brud på regler, kan en direktør eller fagchef anmode om adgang til data eller logoplysninger uden medarbejderens vidende. HR-chefenvurderer, om en anmodning kan imødekommes og sikrer, at adgang udelukkende gives til relevante data.

4. Adgangsstyring

Den logiske adgang til Jammerbugt Kommunes data og it-aktiver kan kun ske via Jammerbugt Kommunes administrative it-netværk. Dette netværk er logisk adskilt fra de øvrige netværk, der anvendes i kommunen, herunder den offentligt tilgængelige del af skolenetværket og andre eksterne net, som f.eks. Internettet.

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

Generelt skal adgang til data minimeres og afspejle et aktuelt arbejdsbetinget behov.

Det er medarbejderens nærmeste leder, der kan anmode om rettigheder til sin medarbejder efter konkret vurdering af behov. Ledere skal derfor have adgang til oplysninger, der er nødvendige for at kunne udføre løbende ledelsestilsyn med adgangene.

5. Styring af it-aktiver

Digitalisering, Borgerservice & Indkøb står for den løbende indkøb, vedligeholdelse og udskiftning af it-aktiver (it-udstyr) i Jammerbugt Kommune.

Al anskaffelse af it-udstyr finansieret af Jammerbugt Kommune skal ske gennem Digitalisering, Borgerservice & Indkøb.

Logiske it-aktiver (herunder alle data, som behandles på Jammerbugt Kommunes it-netværk) styres i forhold den gældende lovgivning. Det er den enkelte afdelings ansvar at klassificere de data, der behandles i afdelingen og sikre, at de er forsvarligt beskyttet. Digitalisering, Borgerservice & Indkøb bistår efter behov i klassificeringen.

Klassifikation af data og andre it-aktiver
Klassifikationen af data stiller forskellige krav til håndtering og opbevaring af data. Systemejeren skal ved introduktion af et nyt system og tilhørende hardware sikre, at sikkerheden i systemet er i stand til at beskytte de data, som systemet anvender i overensstemmelse med datas sikkerhedsklassifikation. Dette kan ske i samarbejde med Digitalisering, Borgerservice og Indkøb, men systemejeren har ansvaret for klassifikationen.

Vedligeholdelse af fysiske it-aktiver
Alle fysiske it-aktiver (it-udstyr) er underlagt løbende vedligeholdelse i form af softwareopdateringer og eventuelle fysiske reparationer for at sikre driftssikkerheden på it-netværket og integriteten i dataene.

Kassation af it-aktiver
Kassation foretages på en it-sikkerhedsmæssig forsvarlig måde, så det sikres, at GDPR-krav til sletning af data mm. overholdes.

6. Medarbejderes brug af it-udstyr

Generel brug
Medarbejdere skal sikre korrekt håndtering af data og udstyr for at beskytte kommunens it-aktiver.

Elektronisk udveksling af data
Brug af uautoriserede datamedier (f.eks. Dropbox og andre cloud-baserede datamedier) er ikke tilladt.

Brug af privat udstyr
Fortrolige oplysninger må ikke behandles på privat udstyr. Adgang fra ikke-kommunale enheder til kommunens netværk er forbudt. Private enheder kan dog anvende kommunens gæstenet via SMS-kode.

7. Risikovurdering og håndtering

Alle it-systemer og -arbejdsgange i Jammerbugt Kommune, som indebærer behandling af personoplysninger, eller som har en påvirkning på behandling af personoplysninger eller på kommunens evne til at levere sine myndighedsforpligtelser, risikovurderes. Det sikres desuden, at processerne håndteres, så it-brug altid foregår på den mest sikre og hensigtsmæssige måde, herunder at sikre overholdelse af gældende lovgivning.

Behandlingsaktiviteter
Kommunen har udarbejdet en fortegnelse over samtlige behandlingsaktiviteter indeholdende personoplysninger, jf. databeskyttelsesforordningens artikel 30. Fortegnelsen indeholder således en overordnet beskrivelse af samtlige arbejdsgange, hvor der behandles personoplysninger i Jammerbugt Kommune. Behandlingsaktiviteterne risikovurderes af den leder, der er ansvarlig for den givne arbejdsproces.

Systemer
Systemejeren har ansvaret for, at der udarbejdes en risikovurdering for det pågældende system. Chefen for Digitalisering, Borgerservice & Indkøb har som procesejer ansvaret for at risikovurdere på relevante tværgående it-arbejdsprocesser, fx central brugeradministration.

Logning af adgang
Adgang til og ændring af følsomme eller kritiske it-systemer eller data skal kunne spores til den medarbejder, der har foretaget en handling. Alle adgangsforsøg og anvendelser af systemer logges.

Stikprøver
Systemejerne er ansvarlige for at gennemføres stikprøver af logfiler i relevante it-systemer for at kontrollere uautoriserede logins og adgang til personoplysninger, samt om medarbejdere har tilgået personoplysninger uden et arbejdsbetinget behov.

8. Fysisk sikkerhed

Fysisk sikkerhed fokuserer på sikkerheden omkring de fysiske it-zoner og beskyttelse af it-aktiver i Jammerbugt Kommune. Dette område varetages af Digitalisering, Borgerservice & Indkøb, der står for drift og implementering af sikkerhedsforanstaltninger i form af henholdsvis overvågning, elektronisk låsesystem, UPS, brandsluknings- og alarmeringsudstyr mv.

Alle medarbejdere er ansvarlige for at opbevare fysiske dokumenter med personoplysninger forsvarligt. Det indebærer, at medarbejderne ikke efterlader personoplysninger ulåste, hvis lokalet forlades. Dokumenterne må godt efterlades, hvis de er under opsyn af en kollega, som har lov til at behandle personoplysningerne. Ellers skal dokumenterne låses inde enten i et skab eller ved at låse døren til lokalet.

9. Driftssikkerhed og netværk

Ansvar
Digitalisering, Borgerservice & Indkøb er ansvarlig for driften af it-infrastrukturen i samarbejde med eksterne leverandører. Samarbejdet sikrer stabil, sikker og tilgængelig drift samt kontrol af leverandørens medarbejdere.

Driftsnedbrud
Driftsproblemer løses primært inden for arbejdstid. Længerevarende nedlukninger bestræbes uden for arbejdstid. Nødprocedurer aktiveres ved kritiske nedbrud.

Redundans
Kritiske systemer er redundante for at modvirke nedbrud. En dobbelt driftscenterstrategi sikrer, at mindst 65% af systemerne fungerer, hvis et driftscenter svigter. Se it-beredskabsplanen for en liste over berørte systemer og prioritering ved nedbrud.

Netværk
Jammerbugt Kommunes it-netværk er segmenteret for at sikre de transmitterede data og infrastruktur. Digitalisering, Borgerservice & Indkøb står for driften.

Kommunikationsadskillelse kræver specifik godkendelse fra Digitalisering, Borgerservice & Indkøb.

It-netværket er segmenteret, hvilket forhindrer uhensigtsmæssig adgang.

Ny- og reetablering af it-lokationer kræver involvering af Digitalisering, Borgerservice & Indkøb, som også skal foreskrive udstyr, fx fiberetablering, tilkobling og andet teknisk udstyr.

10. 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 Informationssikkerhedspolitikken og databeskyttelsesloven. Ethvert nyt system skal risikovurderes inden ibrugtagning.

Nye systemer og konfigurationsændringer i eksisterende systemer skal planlægges, kvalitetssikres og godkendes i samarbejde med Digitalisering, Borgerservice & Indkøb.

11. Leverandørforhold

Eksterne serviceleverandører/samarbejdspartnere skal have minimum samme krav til informationssikkerhed som beskrevet i Jammerbugt Kommunes Informationssikkerhedspolitik samt tilhørende Informationssikkerhedshåndbog.

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

12. Styring af sikkerhedsbrud

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

13. It-beredskabsstyring

Jammerbugt Kommune har udarbejdet en it-beredskabsplan med en praktisk strategi for, hvordan man begrænser konsekvenserne af tab af data og it-systemer som følge af evt. katastrofer og sikkerhedsbrister.

14. Opdatering og godkendelse

Informationssikkerhedspolitikken opdateres minimum en gang årligt. Den øverste it-sikkerhedsansvarlige vurderer, hvornår der er behov for godkendelse i Direktion og evt. politisk behandling, og underretter MED-systemet hvis der ændres i personalerelaterede forhold.