Informationssikkerhedspolitik

for

Aarhus Kommune

Vedtaget af Aarhus Byråd den 2. december 2020

Indhold

1. Indledning

Informationssikkerhedspolitikken er den overordnede ramme for beskyttelse af Aarhus Kommunes informationer, herunder personoplysninger og andre fortrolige oplysninger fx økonomiske forhold, og følger principperne i den internationale standard for informationssikkerhed ISO27001:2013.

Informationssikkerhedspolitikken og den tilhørende Informationssikkerhedshåndbog skal være tilgængelig for alle medarbejdere, der beskæftiger sig med personoplysninger.

1.1 Formål med informationssikkerhedspolitikken

Aarhus Kommune vil sikre, at borgerne kan bevare en høj grad af tillid og tryghed i forbindelse med kommunens behandling af deres personoplysninger. I denne forbindelse vægtes arbejdet med cyber- og informationssikkerhed højt i forhold til bl.a. at øge borgernes tillid til digitale løsninger.

Informationssikkerhedspolitikken skal være med til at sikre den nødvendige beskyttelse af samtlige ressourcer, der indgår i eller bidrager til Aarhus Kommunes behandling og kommunikation af informationer i elektronisk og fysisk form, og herunder særligt at informationerne bevarer deres fortrolighed, integritet og tilgængelighed.

Informationssikkerhedspolitikken fastlægger på baggrund af en risikobaseret tilgang det overordnede sikkerhedsniveau for Aarhus Kommunes beskyttelse af informationer. Herunder rammerne for de sikkerhedsforanstaltninger, som er nødvendige for, at kommunen kan opfylde gældende lov og relevante krav i relation til cyber- og informationssikkerhed.

1.2 Målsætninger for informationssikkerhed

Det er af væsentlig betydning for Aarhus Kommune, borgere og medarbejdere, at informationer behandles på en sikkerhedsmæssig forsvarlig måde, og at alle medarbejdere, der arbejder med personoplysninger, forholder sig til informationssikkerhed i det daglige arbejde.

Aarhus Kommunes mål for informationssikkerhed er:

- At overholde gældende lovgivning og relevante krav i relation til informationssikkerhed
- At forankre ledelsesansvaret for informationssikkerhedsområdet
- At understøtte medarbejdernes bevidsthed om, hvordan personoplysninger behandles sikkerhedsmæssigt forsvarligt
- At medvirke til et passende sikkerhedsniveau for beskyttelse af informationer
- At sikre og opretholde de nødvendige tiltag for at skabe modstandsdygtighed og forsvare kommunen mod cybertrusler

1.3 Omfang

Aarhus Kommunes informationssikkerhedspolitik gælder for:

- Alle medarbejdere, herunder eksterne konsulenter og servicemedarbejdere i Aarhus Kommune uanset ansættelsesform
- Alle systemer og IT-infrastruktur-komponenter som fx netværk, telefoni m.v.
- Alle leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til kommunens informationer, systemer og IT-infrastruktur-komponenter
- Alle informationer, der behandles i Aarhus Kommune

1.4 Vedligeholdelse af Informationssikkerhedspolitikken

Databeskyttelsesudvalget revurderer informationssikkerhedspolitikken en gang årligt eller efter behov for at sikre, at den er i overensstemmelse med de aktuelle mål og gældende lovgivning, som Aarhus Kommune arbejder efter. Digitaliseringsstyregruppen konsulteres om resultatet af revurderingen inden offentliggørelse.

2. Organisering og ansvar

Aarhus Kommune har det overordnede ansvar for, at behandlingen af personoplysninger sker på en sikkerhedsmæssig forsvarlig måde og er i overensstemmelse med informationssikkerhedspolitikken.

Dette sikres bl.a. ved en stærk ledelsesmæssig forankring samt en velfungerende informationssikkerhedsorganisation.

2.1 Ledelsesansvar

Det følger af kommunens styrelsesvedtægt, at Aarhus Byråd er ansvarlig myndighed, og at borgmesteren har det overordnede ledelsesansvar for informationssikkerhedspolitikken.

Rådmænd og direktører har ledelsesansvaret for udmøntningen af informationssikkerhedspolitikken i de enkelte magistratsafdelinger.

Forvaltningschefer har ledelsesansvaret for informationssikkerhedspolitikken i de enkelte forvaltninger.

Chefer for de enkelte afdelinger, områder, institutioner, centre mv. har normalt ledelsesansvaret for overholdelsen af Informationssikkerhedspolitikken i deres egen enhed.

2.2 Informationssikkerhedsorganisationen

Det er af stor betydning for overholdelse af informationssikkerhedspolitikken, at denne har en ledelsesmæssig forankring. Til støtte for dette har følgende en særlig rolle i informationssikkerhedsorganisationen.

Direktørerne er overordnede ansvarlige for, at magistratsafdelingerne overholder informationssikkerhedsreglerne. Digitaliseringscheferne fungerer som stedfortrædere for direktørerne i forhold til denne opgave.

De forvaltningsansvarlige og de afdelingsansvarlige (forvaltningschefer og afdelingschefer) er ansvarlige for, at forvaltningen/afdelingen overholder informationssikkerhedsreglerne og herunder, at der etableres en hensigtsmæssig sikkerhedsstruktur med et passende antal sikkerhedsområder (enhed eller samling af enheder) med dertilhørende informationssikkerhedsansvarlige i forhold til organisationens størrelse. De forvaltningsansvarlige udpeger de informationssikkerhedsansvarlige og stedfortrædere, der skal forestå de daglige sikkerhedsopgaver i sikkerhedsområderne.

Informationssikkerhedschefen er den øverste ansvarlige for, at informationssikkerhedshåndbogen, herunder politik, regler og procedurer er relevant, opdateret og kendt i kommunen. Herudover følger informationssikkerhedschefen op på, om magistratsafdelingernes informationssikkerhedsniveau er i overensstemmelse med informationssikkerhedssikkerhedspolitikken, og at de til enhver tid gældende kontroller gennemføres.

De informationssikkerhedsansvarlige er ansvarlige for udførelse af de daglige sikkerhedsopgaver i de respektive sikkerhedsområder, herunder at informere sikkerhedsområdets medarbejdere om informationssikkerhedsreglerne.

2.3 Aktører på informationssikkerhedsområdet

Til støtte for informationssikkerhedsorganisationen har følgende aktører en vigtig rolle på både det strategiske og operative plan på informationssikkerhedsområdet.

Digitaliseringsstyregruppen

Digitaliseringsstyregruppen er det strategiske organ for arbejdet med informationssikkerhed og referer til direktørgruppen.

Digitaliseringsstyregruppens opgaver på informationssikkerhedsområdet er at:

- Fastlægge strategi og risikoniveau for Aarhus Kommunes cyber- og informationssikkerhed
- Sætte mål, der er afstemt efter kommunens valgte strategi og risikoniveau. Dette skal ske årligt eller efter behov
- Udarbejde årlig overordnet risikovurdering for kommunen i samarbejde med relevante interessenter
- Følge op på status på:
    - Gennemførte risikovurderinger
    - Det overordnede trusselsbillede, herunder sikkerhedsvarslinger/ændringer i trusselsbilledet og mulige forbedringer
    - Bemærkninger fra it-revisionen og Datatilsynet
    - Sikkerhedsarbejdet/sikkerhedsprojekter i magistratsafdelingerne
    - Uddannelse/awareness
    - Resultatet af de periodisk afprøvninger af IT-beredskabsplanen
    - Databeskyttelsesrådgiverens rapport
    - Sikkerhedsbrud
    - Kommunens sikkerhedsniveau i forhold til andre (benchmarking)

Styregruppen skal videreformidle emner, der har særlig betydning for medarbejderne, til behandling i kommunens MED-system.

På informationssikkerhedsområdet består Digitaliseringsstyregruppen af magistratsafdelingernes digitaliseringschefer, informationssikkerhedschefen og databeskyttelsesrådgiveren (som rådgiver og uden stemmeret) og holder møde 2 gange om året eller efter behov.

Koordinerende direktører deltager i Digitaliseringsstyregruppens møder omhandlende informationssikkerhed bl.a. for at sikre, at der på informationssikkerhedsområdet skabes en ledelsesforankring på højeste niveau i kommunen.

Borgmesterens Afdeling står for sekretariatsbetjening af Digitaliseringsstyregruppen.

Databeskyttelsesudvalget

Databeskyttelsesudvalget er det operative organ for arbejdet med informationssikkerhed og referer til Digitaliseringsstyregruppen.

Databeskyttelsesudvalgets opgaver er:

- At udmønte og igangsætte tiltag, indsatser og forbedringer, som tilgodeser informationssikkerhedsstrategien og gennemfører de mål, som Digitaliseringsstyregruppen har fastlagt

- At behandle og træffe beslutninger om overordnede sikkerhedsspørgsmål
- At være rådgivende organ for informationssikkerhedsarbejdet i informationssikkerhedsorganisationen
- At have ansvaret for vedligeholdelse af informationssikkerhedshåndbogen, herunder fortolkning, ændring, sletning eller udarbejdelse af regler og procedurer

Databeskyttelsesudvalget består af informationssikkerhedschefen, som er formand, og informationssikkerhedskoordinatorer fra hver magistratsafdeling samt den tværgående informationssikkerhedskoordinator. Databeskyttelsesudvalget holder møde 6 gange om året eller efter behov.

Borgmesterens Afdeling står for sekretariatsbetjeningen af Databeskyttelsesudvalget.

Informationssikkerhedschef

Informationssikkerhedschefen er ansvarlig for, at indholdet i kommunens informationssikkerhedshåndbog, herunder politikker, retningslinjer m.v. er i overensstemmelse med databeskyttelseslovgivningen og kommunens sikkerhedsniveau.

Informationssikkerhedschefens opgaver er:

- At sikre, at informationssikkerhedshåndbogen, herunder politik, regler og procedure er relevant, opdateret og kendt i kommunen
- At følge op på, at magistratsafdelingernes informationssikkerhedsniveau er i overensstemmelse med informationssikkerhedspolitikken og databeskyttelseslovgivningen og at de til enhver tid gældende kontroller gennemføres
- At understøtte, samarbejde med og rådgive kommunens ledelse, systemejere og ansatte om it- og informationssikkerhed
- At igangsætte og gennemføre tiltag på it-sikkerhedsområdet sammen med relevante teknikere
- At holde kontakt med relevante myndigheder, herunder Datatilsynet, og andre eksterne samarbejdspartnere
- At varetage systemejerskaber indenfor informationssikkerhed fx kommunens Information Security Management System (ISMS)
- At skabe awareness om informationssikkerhed i organisationen gennem kampagner mv.

Tværgående informationssikkerhedskoordinator

Den tværgående informationssikkerhedskoordinator er placeret i Borgmesterens Afdeling og har en tværmagistratslig rolle i forhold til koordinering af informationssikkerheden på tværs af magistratsafdelingerne, herunder at være sekretær for Databeskyttelsesudvalget.

Den tværgående informationssikkerhedskoordinator er stedfortræder for Informationssikkerhedschefen.

Den tværgående informationssikkerhedskoordinators opgaver er:

- At deltage i planlægningen af indsatser i forhold til informationssikkerhed på tværs i organisationen
- At deltage i videreudvikling og vedligeholdelse af informationssikkerhedshåndbogen, politikker, regler og procedurer
- At bistå magistratsafdelingerne ved behov med udarbejdelse af risikovurderinger og eventuelle konsekvensanalyser

- At bistå magistratsafdelingerne ved behov for vurdering af informationssikkerhedskrav og besvarelser i forbindelse med anskaffelse af IT-systemer
- At yde rådgivning og vejledning om sikkerhedsspørgsmål
- At kontrollere anvendelsen af personoplysninger i den borgervendte service (Borgerservice)
- At udarbejde dagsorden og referater til Databeskyttelsesudvalget

Informationssikkerhedskoordinatorer

Informationssikkerhedskoordinatoren er magistratsafdelingens repræsentant i Databeskyttelsesudvalget og skal have de nødvendige faglige kompetencer til at varetage denne rolle.

Informationssikkerhedskoordinatoren varetager den overordnede daglige drift af informationssikkerhedsområdet i den enkelte magistratsafdeling. Informationssikkerhedskoordinatoren er udpeget af magistratsafdelingens digitaliseringschef.

Informationssikkerhedskoordinatoren fungerer som bindeleddet mellem magistratsafdelingens informationssikkerhedsorganisation og den overordnede tværmagistratslige koordinering på informationssikkerhedsområdet.

Informationssikkerhedskoordinatorens opgaver i egen magistratsafdeling er:

- At yde rådgivning og vejledning om sikkerhedsspørgsmål
- At bistå systemejerne med at sikre, at systemerne lever op til det fastlagte sikkerhedsniveau, herunder at der er udarbejdet de nødvendige retningslinjer og procedurer for brugen af systemerne
- At implementere de tiltag, indsatser og forbedringer, som er besluttet i Digitaliseringsstyregruppen
- At bistå ved registrering og rapportering af kritiske hændelser
- At vedligeholde informationssikkerhedsorganisationen
- At skabe opmærksomhed om informationssikkerhed blandt medarbejderne
- At informere relevante parter i organisationen om Digitaliseringsstyregruppens og Databeskyttelsesudvalgets beslutninger og sikre, at organisationen udfører opgaverne vedrørende informationssikkerhed
- At holde digitaliseringschefen orienteret om arbejdet i Databeskyttelsesudvalget
- Udføre relevante kontroller i egen magistratsafdeling og udarbejde dokumentation herfor

Informationssikkerhedsansvarlige

De informationssikkerhedsansvarlige har ansvaret for udførelse af de daglige sikkerhedsopgaver i de respektive sikkerhedsområder, herunder at informere sikkerhedsområdets medarbejdere om informationssikkerhedsreglerne.

De informationssikkerhedsansvarlige udpeges af de forvaltningsansvarlige.

Systemejere

Systemejeren har ansvaret for, at systemet lever op til det fastlagte sikkerhedsniveau, herunder at der er udarbejdet de nødvendige retningslinjer og procedurer for brugen af systemet.

2.4 Databeskyttelsesrådgiver

Databeskyttelsesrådgiveren skal understøtte kommunens overholdelse af databeskyttelseslovgivningen.

Det er et grundlæggende krav, at databeskyttelsesrådgiveren udfører sine opgaver uafhængigt. Dette betyder at databeskyttelsesrådgiveren ikke må modtage instrukser i forbindelse med udførelsen af sine opgaver og refererer til byrådet.

Databeskyttelsesrådgiverens opgaver er beskrevet direkte i forordningen, og omfatter følgende:

- Orientere og rådgive kommunens ledelse og ansatte om deres forpligtelser
- Overvåge at kommunen overholder forordningen
- Rådgive kommunen i forbindelse med udarbejdelse af konsekvensanalyser
- Holde kontakt med relevante myndigheder og andre eksterne samarbejdspartnere i forhold til databeskyttelseslovgivningen
- Samarbejde med og fungere som kontaktperson til tilsynsmyndigheden for databeskyttelse
- Fungere som kontaktperson for registrerede (borgere) angående spørgsmål om behandling af deres oplysninger
  Rapportere én gang årligt eller efter behov til det øverste ledelsesniveau, som i Aarhus Kommune er byrådet

Databeskyttelsesrådgiveren skal støtte og rådgive alle niveauer i Aarhus Kommune.

Databeskyttelsesrådgiveren har ingen ledelsesmæssig beslutningskompetence.

3. Risikobaseret tilgang

Risikovurdering

Aarhus Kommune foretager en afbalanceret overordnet risikovurdering under hensyntagen til relevante sikkerhedsforanstaltninger og gældende lovgivning for at sikre informationers fortrolighed, integritet og tilgængelighed.

Den overordnede risikovurdering opdateres årligt eller efter behov.

Informationssikkerhedsorganisationen gennemfører i samarbejde med informationssikkerhedskoordinatorerne et passende antal risikoanalyser i forbindelse med ibrugtagning af nye IT-systemer samt ved større rettelser af eksisterende IT-systemer eller ved væsentlige ændringer i risikobilledet.

Sikkerhedsniveau

Aarhus Kommunes sikkerhedsniveau fastlægges på baggrund af Statement of Applicability (SOA), jf. ISO-standarden og skal være medvirkende til, at kommunens håndtering af informationer foregår på en betryggende og tillidsvækkende måde.

Aarhus Kommunes sikkerhedsniveau skal tilgodese:

- Lovgivningsmæssige krav, herunder databeskyttelsesforordningen og databeskyttelsesloven
- De anerkendte standarder for databeskyttelse i form af ISO 27001
- Nationale strategier på cybersikkerhedsområdet

4. Personalesikkerhed

For at Aarhus Kommune kan fastholde et højt sikkerhedsniveau, er det vigtigt, at kommunens medarbejdere er bevidste om og lever op til deres informationssikkerhedsansvar. Medarbejderne oplyses, om informationssikkerhed i relation til deres jobfunktion ved hjælp af uddannelse og træning.

Regler for informationsansvar og -forpligtelser, som gælder både før og efter ansættelsen, skal fremgå af informationssikkerhedshåndbogen.

5. Styring af aktiver

Alle IT-aktiver, som indeholder personoplysninger, skal identificeres, klassificeres og der skal udpeges en ejer for hvert aktiv.

De enkelte magistratsafdelinger og Fælles IT skal vedligeholde en fortegnelse over disse aktiver.

Alle medarbejdere og eksterne brugere skal aflevere kommunens aktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.

6. Adgangsstyring

Adgangen til at udføre handlinger på Aarhus Kommunes netværk og netværkstjenester beskyttes af adgangskontrolsystemer for at forhindre uautoriseret adgang til systemer og tjenester.

Kommunens medarbejdere skal medvirke til beskyttelse af oplysningerne gennem korrekt brug af systemerne og tjenesterne.

7. Kryptografi

Implementering af foranstaltninger til beskyttelse af oplysningers fortrolighed, integritet og tilgængelighed sker på baggrund af risikovurderinger.

Aarhus Kommune kan beskytte oplysningers fortrolighed, integritet og tilgængelighed ved brug af kryptografi.

8. Fysisk sikring og miljøsikring

Aarhus Kommunes udstyr, aktiver, kontorer, lokaler og faciliteter skal på baggrund af risikovurderinger beskyttes mod uautoriseret fysisk adgang samt mod naturkatastrofer, ondsindede angreb eller ulykker.

Den uautoriserede fysiske adgang forhindres ved fysisk afgrænsning af områder, fysisk adgangskontrol, sikring af kontorer, lokaler og faciliteter, understøttende forsyningssikkerhed og sikker bortskaffelse eller genbrug af udstyr.

9. Driftssikkerhed

Der skal foreligge dokumenterede procedurer for drift, softwareinstallation samt ændringsstyring for at understøtte en korrekt og sikker drift af informationsbehandlingsfaciliteterne.

Aarhus Kommune sikrer, at der implementeres passende sikkerhedsforanstaltninger til beskyttelse mod fx malware, tab af data samt overvågning og registrering af brugeraktiviteter, undtagelser, fejl og informationssikkerhedssikkerhedshændelser for at opnå det fastlagte sikkerhedsniveau.

10. Kommunikationssikkerhed

Netværk og netværkstjenester skal styres og overvåges samt have installeret passende sikkerhedsforanstaltninger for at beskytte informationerne i systemer og applikationer.

Ved overførsel af informationer ved brug af alle former for kommunikationsudstyr internt i Aarhus Kommune eller til eksterne samarbejdspartnere skal informationerne beskyttes på passende måde, blandt andet ved indgåelse af aftaler om fortrolighed og hemmeligholdelse og brug af kryptering, når informationernes klassifikation kræver dette.

11. Anskaffelse, udvikling og vedligeholdelse af systemer

Det er vigtigt, at informationssikkerhed er en integreret del af processerne ved anskaffelse, udvikling og vedligeholdelse af systemerne samt applikationstjenester på offentlige netværk.

Aarhus Kommune sikrer, at der på baggrund af en dokumenteret risikovurdering sker identifikation af relevante sikkerhedskrav ved anskaffelse af nye systemer/applikationer eller forbedringer af eksisterende systemer/applikationer.

12. Leverandørforhold

Aarhus Kommunes leverandører/samarbejdspartnere skal mindst leve op til kommunens sikkerhedsniveau.

For at minimere risiciene forbundet med leverandørers/samarbejdspartneres adgang til kommunens aktiver skal der enten indgås en databehandleraftale, hvori sikkerhedskravene til behandlingen fastlægges eller underskrives en fortrolighedserklæring. Der skal desuden leveres relevante revisorerklæringer og gives mulighed for inspektion af informationssikkerheden som kontrol af de indgåede databehandleraftaler.

13. Styring af informationssikkerhedsbrud

Alle konstaterede informationssikkerhedsbrud skal dokumenteres og rapporteres til Aarhus Kommunes databeskyttelsesrådgiver og eventuelt Datatilsynet.

Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, skal anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.

Herudover skal alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester dokumenteres og rapporteres til informationssikkerhedsorganisationen.

14. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Aarhus Kommune er ansvarlig for, at informationer og systemer, der er kritiske for kommunens informationsbehandling, er omfattet af en IT-beredskabsplan, som sikrer den nødvendige informationssikkerhedskontinuitet i en kritisk situation.

På baggrund af en risikovurdering fastlægger, dokumenterer, implementerer og vedligeholder Aarhus Kommune en IT-beredskabsplan.

Der foretages periodisk afprøvning af IT-beredskabsplanen for at sikre, at den er tidssvarende og effektiv i kritiske situationer. Der skal foreligge dokumentation for afprøvningen og evalueringen heraf.

15. Overensstemmelse med lov- og kontraktkrav

Aarhus kommune er ansvarlig for, at alle relevante lov-, myndigheds- og kontraktkrav vedrørende informationsbehandling, herunder informationssikkerhedskrav identificeres, dokumenteres, efterleves og løbende vedligeholdes.

Herudover gennemgås kontroller, politikker, processer og procedurer for informationssikkerhed med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre, at informationsbehandlingen og informationssystemerne er i overensstemmelse med informationssikkerhedspolitikker og -standarder.