Aarhus Kommune

Politik

1.22

20-09-2019

Indledning

IT-sikkerhedspolitikken blev vedtaget i byrådets møde den 24. juni 2009

Revisionsdato: 29. november 2018 (er lagt på hjemmesiden den 13. december 2018)

IT-sikkerhedspolitikken er den overordnede ramme for IT-sikkerheden i kommunens informationsbehandling generelt.

IT-sikkerhedspolitikken og den tilhørende IT-sikkerhedshåndbog skal være tilgængelig for alle medarbejdere/IT-brugere i Aarhus Kommune.

IT-sikkerhedspolitikken er udarbejdet på baggrund af den offentlige standard for informationssikkerhed DS 484:2005, lov om behandling af personoplysninger, Lov nr. 429 af 31. maj 2000 samt kommunens hidtidige IT-sikkerhedspolitik.

Formål

Det er af vital betydning for Aarhus Kommune, at informationer behandles sikkerhedsmæssigt forsvarligt, idet informationer og informationssystemer (herunder netværk og telefoni) er særdeles vigtige for kommunens virksomhed.

IT-sikkerhedspolitikken definerer en ramme for beskyttelse af kommunens informationer (herunder personoplysninger og andre fortrolige oplysninger f.eks. om økonomiske forhold) og sikrer hermed særligt, at følsomme og kritiske informationer bevarer deres fortrolighed, integritet og tilgængelighed.

IT-sikkerhedsniveauet vil være afstemt efter risiko, væsentlighed, lovkrav, Aarhus Kommunes IT-strategi og god IT-skik m.v.

IT-sikkerhedspolitikken skal være med til at forebygge sikkerhedsproblemer, begrænse skader samt sikre retablering af informationer og de forvaltningsprocesser, informationerne indgår i.

Politikkens omfang

IT-sikkerhedspolitikken omfatter alle informationer, der behandles i Aarhus Kommune, uanset i hvilken form de modtages, opbevares og formidles. Herunder omfatter politikken systemer, netværk, telefoni m.v.

IT-sikkerhedspolitikken gælder for alle medarbejdere/IT-brugere, uanset ansættelsesform samt selvejende institutioner eller andre samarbejdspartnere, som kommunen har indgået driftsoverenskomst med.

Ved udlicitering af opgaver samt hvor leverandører udfører opgaver for kommunen, skal systemejerne sikre, at kommunens IT-sikkerhedsniveau overholdes. Leverandøren skal således mindst leve op til kommunens IT-sikkerhedsniveau.

Ledelsesansvar

Det følger af kommunens styrelsesvedtægt, at Aarhus Byråd er ansvarlig myndighed og herunder, at Borgmesteren har det overordnede ledelsesansvar for IT-sikkerhedspolitikken.

Rådmænd og direktører har ledelsesansvaret for udmøntningen af sikkerhedspolitikken i den enkelte magistratsafdeling, herunder selvejende institutioner, som magistratsafdelingen har indgået driftsoverenskomst med. Forvaltningschefer har ledelsesansvaret for sikkerhedspolitikken i den enkelte forvaltning, og chefer for de enkelte enheder har ledelsesansvaret for sikkerhedspolitikken i den enkelte afdeling, område, institution m.v.

IT-sikkerhedsorganisationen

Det er af stor betydning for overholdelse af IT-sikkerhedspolitikken, at denne har en ledelsesmæssig forankring. Til støtte for dette har følgende en særlig rolle i IT-sikkerhedsorganisationen.

IT-sikkerhedschefener den øverste ansvarlige for administration, håndhævelse, tilsyn m.v. af IT-sikkerhedsreglerne i Aarhus Kommune og herunder godkendelse af sikkerhedsområder og sikkerhedsansvarlige. Det nærmere indhold af opgaverne fremgår af bilag 1 samt IT-sikkerhedshåndbogen.

Direktørerneer overordnet ansvarlige for, at magistratsafdelingen overholder sikkerhedsreglerne. IT-cheferne fungerer som stedfortræder for direktørerne i forhold til denne opgave.

De forvaltningsansvarligeog de afdelingsansvarlige (forvaltningschefer og afdelingschefer) er ansvarlige for, at forvaltningen/afdelingen overholder sikkerhedsreglerne og herunder, at der etableres en hensigtsmæssig sikkerhedsstruktur med et passende antal sikkerhedsansvarlige i forhold til organisationens størrelse. De forvaltningsansvarlige udpeger de sikkerhedsansvarlige og stedfortrædere, der skal forestå de daglige sikkerhedsopgaver i sikkerhedsområderne.
De sikkerhedsansvarligeer ansvarlige for udførelse af de daglige sikkerhedsopgaver i de respektive sikkerhedsområder, herunder at informere sikkerhedsområdets medarbejdere om sikkerhedsreglerne samt at medarbejderne alene autoriseres til oplysninger, der er relevante for vedkommendes arbejdsområde.

Databeskyttelsesudvalget

Databeskyttelsesudvalget består af en repræsentant fra hver magistratsafdeling, der har den fornødne beslutningskompetence og gerne en særlig interesse for IT-sikkerhedsområdet. Emner, der har særlig betydning for medarbejderne, skal også behandles i kommunens Med-system, jf. Lokalaftale om medindflydelse og medbestemmelse i Aarhus Kommune. Formandskabet for Databeskyttelsesudvalget varetages af databeskyttelsesrådgiveren. Sekretariatsfunktionen varetages af Borgmesterens Afdeling.
Databeskyttelsesudvalgets opgave er at behandle principielle sikkerhedsspørgsmål og være rådgivende organ for IT-sikkerhedsarbejdet i IT-sikkerhedsorganisationen. Digitaliseringsstyregruppen følger udvalgets særlige indsatser som følge af den tætte sammenhæng til Digitaliseringsstrategien for Aarhus Kommune. Der skal foreligge et kommissorium for Databeskyttelsesudvalgets arbejde.

IT-sikkerhedsniveau

Det er Aarhus Kommunes politik at beskytte informationer, sikre tilgængelighed og udelukkende tillade brug, adgang og offentliggørelse af informationer under hensyntagen til den til enhver tid gældende lovgivning.
På denne baggrund fastlægger Aarhus Kommune en afbalanceret risiko- og konsekvensvurdering under hensyntagen til de basale sikkerhedsforanstaltninger i DS 484, databeskyttelseslovgivningens bestemmelser samt Aarhus Kommunes IT-strategi. Den overordnede risikovurdering skal fremgå af IT-sikkerhedshåndbogen, der er gældende for kommunens informationsbehandling og har samme status som instrukser. Der skal foretages en årlig gennemgang af den overordnede risikovurdering.
IT-sikkerhedschefen gennemfører i samarbejde med magistratsafdelingerne et passende antal risikoanalyser i forbindelse med større forandringer i organisationen eller ved væsentlige ændringer i risikobilledet.

IT-sikkerhedshåndbogen

IT-sikkerhedshåndbogen indeholder de konkrete retningslinier om IT-sikkerhed. Det nærmere indhold af IT-sikkerhedshåndbogen fremgår af bilag 1.

IT-infrastruktur

Borgmesterens Afdeling skal sikre, at kommunen har en IT-infrastruktur, der understøtter de fastsatte sikkerhedsregler.

IT-drift

Systemejerne skal sikre, at driftsaftaler, der indgås, tilsvarende understøtter de fastsatte sikkerhedsregler.

IT-sikkerhedsbevidsthed

Det er vigtigt, at alle ansatte er bevidste omkring IT-sikkerheden i kommunen. Til brug for dette udarbejder IT-sikkerhedschefen i samarbejde med de øvrige magistratsafdelinger informations- og undervisningsmateriale, der vil blive publiceret til medarbejderne via IT-sikkerhedsorganisationen. IT-sikkerhedsorganisationen skal løbende følge op på, at medarbejderne er bevidste omkring IT-sikkerhedsreglerne.
IT-sikkerhedsorganisationen skal sikre, at alle medarbejdere er gjort bekendt med IT-sikkerhedsreglerne og kontrol f.eks. i forbindelse med brug af systemer, E-post, Internet, videoovervågning og øvrige kontrolforanstaltninger. Dette skal ske på en klar og utvetydig måde. Kontrolforanstaltningerne i forhold til

medarbejderne er i øvrigt omfattet af "Aftale om kontrolforanstaltninger OK-08".

IT-beredskab
IT-sikkerhedschefen skal sikre, at kommunens informationer, herunder data og systemer, der er kritiske for kommunens informationsbehandling, håndteres efter en særlig risikovurdering. Det skal også sikres, at kommunens driftsmiljø, kommunikationsforbindelser m.v. håndteres efter en særlig risikovurdering. Dette skal ske i sammenhæng med de kommunale Indsatsplaner for fortsat drift.

Brud på eller trusler mod IT-sikkerheden
Konstaterede IT-sikkerhedsmæssige brud på eller trusler mod IT-sikkerheden skal registreres og dokumenteres, og alle væsentlige brud skal rapporteres til databeskyttelsesrådgiveren til vurdering samt til den løbende opsamling af sikkerhedsproblemer til brug for revurdering af IT-sikkerhedsbestemmelserne.

Tilsyn og rapportering
Databeskyttelsesrådgiveren fører tilsyn med overholdelsen af IT-sikkerhedspolitikken og de herunder fastsatte IT-sikkerhedsbestemmelser.
Databeskyttelsesrådgiveren rapporterer løbende om IT-sikkerheden i Aarhus Kommune og herunder om eventuelle ændringer i IT-sikkerhedspolitikken via IT-sikkerhedsportalen. En gang årligt foretages en risikovurdering og herunder en vurdering af, om der skal ske ændring af de gældende IT-sikkerhedsregler og tilhørende procedurer. Aarhus Byråd orienteres om status for IT-sikkerhedsarbejdet i Aarhus Kommune via databeskyttelsesrådgiverens årlige rapport.

Vedligeholdelse
Som et led i den overordnede IT-sikkerhedsstyring samt på grundlag af den løbende overvågning og rapportering tages IT-sikkerhedspolitikken op til en årlig revurdering i Databeskyttelsesudvalget.
IT-sikkerhedshåndbogen vedligeholdes af IT-sikkerhedschefen i samarbejde med Databeskyttelsesudvalget.

Bilag 1 til IT-sikkerhedspolitik for Aarhus Kommune
Dette bilag definerer det nærmere indhold af IT-sikkerhedspolitikken, der anvendes som grundlag for de konkrete retningslinier om IT-sikkerhed i IT-sikkerhedshåndbogen.
Retningslinierne og deres operationalisering skal være med til at forhindre, at kommunens informationer, herunder særligt følsomme og kritiske, hændeligt eller ulovligt tilintetgøres, fortabes eller forringes eller kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.
Håndbogens opbygning skal følge den samme punktinddeling, som anvendes i standarden DS 484:2005 med tilføjelse af yderligere punkter til opfyldelse af regler på persondatalovens område.
IT-sikkerhedschefen er ansvarlig for udarbejdelse af de konkrete retningslinier om IT-sikkerhed.

1. IT-sikkerhedshåndbogen
Indeholder en beskrivelse af IT-sikkerhedshåndbogens opbygning og indhold.

2. Definitioner
Indeholder en beskrivelse af anvendte definitioner.

3. Særligt vedrørende databeskyttelseslovgivningens område
Indeholder en nærmere beskrivelse af databeskyttelseslovgivningens bestemmelser, som ikke direkte fremgår af DS 484, herunder regler for hvilke oplysninger, der er omfattet af databeskyttelseslovgivningen, fortegnelser, videregivelse af personhenførbare oplysninger, sammenstilling af personhenførbare oplysninger, kurser i brugen af systemer med personhenførbare oplysninger, opfyldelse af oplysningspligten og tv-overvågning.

4. Risikovurdering og -håndtering
Indeholder en overordnet risikovurdering, herunder konsekvens- og sårbarhedsvurdering. Den overordnede vurdering anvendes bl.a. i forbindelse med IT- beredskabet samt den årlige revurdering af IT-

sikkerhedspolitikken i Aarhus Kommune.
Det er målet, at kommunen har et forsvarligt sikkerhedsniveau for de aktiver, kommunen har ansvaret for at behandle set i forhold til mulige sikkerhedstruende hændelser.

5. Tilsyn med IT-sikkerheden

Indeholder en nærmere beskrivelse af kontrolprocedurer i forbindelse med tilsynet med overholdelse af kommunens IT-sikkerhedsregler.

6. Organisering af informationssikkerhed

Placering af ansvar er vitalt for at sikre kommunens informationer og informationssystemer. IT-sikkerhedschefen vedligeholder IT-sikkerhedsorganisationen, som skal varetage de IT-sikkerhedsmæssige opgaver, både i forhold til interne organisatoriske forhold og eksterne samarbejdspartnere/leverandører. Kontrakter med selvejende institutioner eller andre samarbejdspartnere og andre aftaler er ligeledes et område, der har indflydelse på informationssikkerheden.

Interne organisatoriske forhold:

Indeholder en nærmere beskrivelse af IT-sikkerhedsorganisationen og herunder Databeskyttelsesudvalgets samt databeskyttelsesrådgiverens opgaver.

Eksterne samarbejdspartnere/leverandører:

Systemejerne skal sikre, at IT-sikkerhedsniveauet hos eksterne samarbejdsparter/leverandører mindst er på niveau med kommunens IT-sikkerhedsniveau. Dette dokumenteres ved indgåelse af databehandlingsaftaler samt ved aflevering af relevante revisionserklæringer.

7. Styring af informationsrelaterede aktiver

Alle kommunens fysiske og funktionsmæssige informationsrelaterede aktiver skal beskyttes, uanset om det er fysiske aktiver som dokumenter, der er udskrevet, produktionsudstyr eller IT-systemer. Det er derfor nødvendigt at identificere, klassificere og placere ejerskab for alle aktiver.
De enkelte magistratsafdelinger samt Fælles IT skal vedligeholde fortegnelser over alle væsentlige aktiver, herunder IT-udstyr og informationssystemer. Der skal udpeges en ejer som ansvarlig for hvert aktiv.
Borgmesterens Afdeling udarbejder retningslinier for accepteret brug af kommunens informationsaktiver.

8. Medarbejdersikkerhed

Informationssikkerheden i kommunen afhænger i høj grad af medarbejderne. Medarbejdere skal derfor uddannes i IT-sikkerhed i relation til deres jobfunktion og modtage de nødvendige informationer. Endvidere er det nødvendigt med regler, der beskriver sikkerhedsforhold, når et ansættelsesforhold slutter.

IT-sikkerhedschefen udarbejder en nærmere beskrivelse af sikkerhedsprocedurerne.

Medarbejderne skal kvittere for at have set og forstået IT-sikkerhedsfilmen og at de vil overholde kommunens gældende IT-sikkerhedsregler.

Den enkelte magistratsafdeling vurderer behovet for baggrundscheck og straffeattest.

9. Fysisk sikkerhed

Kommunens IT-infrastruktur, lokaler, informationsbehandlingsudstyr og kommunikationsudstyr skal beskyttes mod uautoriseret fysisk adgang samt fysiske skader og uønskede hændelser.
IT-sikkerhedschefen beskriver retningslinjer for fysisk afgrænsning af områder, fysisk adgangskontrol, sikring af kontorer, lokaler og udstyr, beskyttelse mod eksterne trusler, forsyningssikkerhed, sikker bortskaffelse eller genbrug af udstyr m.v.

10. Styring af netværk og drift

Borgmesterens Afdeling beskriver operationelle procedurer og ansvarsområder. Herunder driftsafviklingsprocedurer, beskyttelse mod skadevoldende programmer og mobil kode, sikkerhedskopiering, netværkssikkerhed, databærende medier, informationsudveksling, elektroniske forretningsydelser samt overvågning og registrering af sikkerhedsrelaterede hændelser.

Systemejerne skal sikre en korrekt og betryggende driftsafvikling af kommunens informationssystemer.

11. Adgangsstyring

Adgangen til at udføre handlinger på kommunens IT-systemer beskyttes af adgangskontrolsystemer. Systemerne har til formål at sikre mod uautoriserede ændringer, ordrer, fejl og svindel. Kommunens medarbejdere skal medvirke til beskyttelse af informationsaktiverne gennem korrekt brug af systemerne.
IT-sikkerhedschefen beskriver retningslinjer for adgangsstyring, administration af brugeradgang, brugernes ansvar, styring af netværksadgang, styring af systemadgang, styring af adgang til brugersystemer og informationer samt mobilt udstyr og fjernarbejdspladser.

12. Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingssystemer

Det er vigtigt, at indkøb, udvikling og implementering af nye systemer foregår kontrolleret for at undgå unødvendige risici for kommunens informationsbehandling. Når løsninger implementeres skal sikkerhedsovervejelser altid indgå som en integreret del af processen. Systemejerne skal derfor sikre, at krav til sikkerhed bliver identificeret i forbindelse med udarbejdelse af kravspecifikationen ved anskaffelsen af et nyt system
IT-sikkerhedschefen beskriver sikkerhedskravene til informationsbehandlingssystemer, herunder korrekt informationsbehandling, kryptering, logning, styring af driftsmiljøet, sikkerhed i udviklings- og hjælpeprocesser og sårbarhedsstyring.

13. Styring af sikkerhedshændelser

Alle medarbejdere, samarbejdspartnere og øvrige brugere skal være bekendt med forretningsgangene for rapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden for kommunens aktiver. Væsentlige sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til IT-sikkerhedschefen.
Databeskyttelsesrådgiveren beskriver procedurer for rapportering af sikkerhedshændelser, svagheder, håndtering af sikkerhedsbrud og forbedringer.

14. Beredskabsstyring

Risikostyring og katastrofeplanlægning er nødvendige for at sikre mod uforudsete hændelser. Nødplanerne skal være med til at opretholde driften, således at skaderne for kommunen minimeres.
Borgmesterens Afdeling beskriver IT-beredskabet og herunder plan for periodisk afprøvning.

15. Overensstemmelse med lovbestemte og kontraktlige krav

Kommunens virke er omfattet af lovgivning og/eller påvirket af kontrakter eller eksterne parters rettigheder.
Borgmesterens Afdeling beskriver overensstemmelsen med lovbestemte krav, sikkerhedspolitik og retningslinier samt beskyttelsesforanstaltninger ved revision af informationsbehandlingssystemer.
Databeskyttelseslovgivningen gælder for behandling af oplysninger om identificerbare personer, når denne behandling helt eller delvis foretages ved hælp af elektronisk databehandling og ved ikke-elektronisk behandling af personoplysninger, der indeholdes i et register. I forhold til persondataloven skal ansatte i kommunen særlig være opmærksomme på: Hvornår en behandling er omfattet af persondataloven, Eventuel anmeldelsespligt, Den registreredes rettigheder (oplysningspligt, indsigtsret, indsigelsesret) og Aftaler med eventuelle leverandører.