FREDERIKSBERG
KOMMUNE

December 2019

Informationssikkerhedspolitik

Frederiksberg Kommune

Indledning
Informationssikkerhedspolitikken er den overordnede ramme for beskyttelse af information i Frederiksberg Kommune.

Kommunen behandler oplysninger om borgere og virksomheder, som ofte er af sensitiv karakter og kræver særlig beskyttelse. Endvidere har kommunen en mængde information og informationssystemer, som er afgørende eller vigtige for varetagelse af kommunens opgaver og pligter.

Derfor er beskyttelse af information og informationssystemer et vigtigt fokusområde, som håndteres gennem kommunens informationssikkerhedsindsats. Indsatsen består overordnet i en mængde sikringsforanstaltninger, som etableres med henblik på at beskytte information og informationssystemer, som har betydning for kommunens virksomhed.

Målsætningen med informationssikkerhedsindsatsen er mere specifikt at beskytte information og informationssystemer mod uautoriseret eller utilsigtet adgang, anvendelse, videregivelse, driftsforstyrrelse, ændring eller ødelæggelse.

Uanset fysiske og tekniske sikringsforanstaltninger spiller den menneskelige faktor, dvs. den måde ledelse, medarbejdere og samarbejdspartnere handler og agerer på, en afgørende rolle i forhold informationssikkerheden. Det er derfor vigtigt, at der i kommunens informationssikkerhedsindsats i høj grad er fokus på de ledelsesmæssige, organisatoriske og menneskelige dimensioner.

Formål
Formålet med informationssikkerhedspolitikken er at definere og fastlægge de overordnede principper for kommunens informationssikkerhed.

Politikken skal udmøntes gennem implementering af relevante sikringsforanstaltninger, som skal beskytte information og informationssystemer med udgangspunkt i tre centrale begreber:

- **Fortrolighed,** at information ikke kommer til uvedkommendes kendskab.
- **Integritet,** at information forbliver pålidelig, korrekt og intakt.
- **Tilgængelighed,** at relevant information kan tilgås og anvendes, når der er behov for det.

Sikringsforanstaltningerne skal rettes mod alle former for trusler, interne og eksterne, hændelige fejl og uheld, samt bevidst skadevoldende handlinger og misbrug. Det skal sikres, at it-driftssikkerheden og effektiviteten kan opretholdes, samt at konsekvenser af sikkerhedsbrud reduceres til et acceptabelt niveau.

I den forbindelse er især følgende indsatsområder centrale:

- Kommunens it-infrastruktur skal til stadighed være effektivt beskyttet mod eksterne trusler og angreb på it-systemer, som f.eks. hacker- og virusangreb.
- De oplysninger om borgere og virksomheder som kommunen er ansvarlig for, skal til enhver tid beskyttes mod uberettiget videregivelse som følge af tekniske og menneskelige fejl eller forsætlige handlinger.
- God sikkerhedsskik, principper og normer for adfærd i anvendelsen af kommunens informationssystemer skal være klart formuleret og formidlet til medarbejderne, så uberettiget og retsstridig anvendelse kan forebygges og undgås.

Holdninger og principper
Informationssikkerhedsniveauet i Frederiksberg Kommune skal fastlægges som en afvejning af ofte modstridende hensyn, nemlig ønsket om høj sikkerhed og hensynet til enkle og smidige arbejdsgange.

Tiltag til forbedring af informationssikkerheden implementeres i overensstemmelse med følgende overordnede holdninger og principper:

- Kommunens troværdighed på informationssikkerhedsområdet må ikke kunne drages i tvivl.
- Sikringsforanstaltninger skal søges tilrettelagt, så de opleves som en naturlig del af medarbejdernes daglige arbejde og ikke som en barriere.
- Informationssikkerheden søges styret i overensstemmelse med anerkendte standarder og ”best practice” for informationssikkerhed.
- Informationssikkerhedsniveauet skal fastsættes ud fra lovgivningsmæssige krav og på grundlag af en afvejning mellem risiko og udgifter til sikringsforanstaltninger

- Såfremt borgere eller samarbejdspartnere berøres af sikkerhedshændelser hos Frederiksberg Kommune, vil kommunen så hurtigt, konkret og præcist, som det er muligt, informere de berørte parter. Kommunen vil gøre, hvad der står i dens magt for at begrænse eventuelle skader mest muligt.

Omfang og afgrænsning
Politikken omfatter principielt enhver information, som ejes, opbevares eller behandles af kommunen og kommunens databehandlere, uanset hvilket medie informationen er lagret på – elektronisk eller i anden form (herunder papirbaseret).

Det primære fokusområde er oplysninger om borgere, virksomheder, kommunens finansielle og økonomiske forhold, dokumentation af arbejdsgange, informationssystemer, samt andre typer information, som kræver særlig beskyttelse eller har væsentlig betydning for kommunens virksomhed.

Politikken er gældende for alle, der udfører opgaver eller hverv for kommunen, herunder:

- Medarbejdere – fast og midlertidigt ansatte
- Medlemmer af kommunalbestyrelsen
- Eksterne samarbejdspartnere, herunder:
    - Institutioner med driftsoverenskomst.
    - Personer og virksomheder der udfører opgaver for kommunen.

Sikkerhedsniveau
Det er kommunens politik at beskytte information og udelukkende tillade brug, adgang til og offentliggørelse af information i overensstemmelse med kommunens sikkerhedsregler og ud fra den til enhver tid gældende lovgivning.

Politikken tager udgangspunkt i ISO 27001 international standard for informationssikkerhed, der afløser den nu udgåede standard DS 484. ISO 27001 betragtes som en referenceramme, der anvendes som rettesnor og redskab for tilrettelæggelse og styring af informationssikkerheden i kommunen. Overgangen til ISO 27001vil være glidende og medfører på nuværende tidspunkt ikke yderligere ændringer i informationssikkerhedspolitikken.

Kommunen skal til enhver tid leve op til:

- Sikkerhedsmæssige krav, der følger af lovgivningen. Da kommunen har omfattende opgaver med behandling af personoplysninger, er især EU's databeskyttelsesforordning og den danske databeskyttelseslov samt arkivloven væsentlige.

- De sikkerhedsmæssige krav, som er fastsat i forbindelse med aftaler med andre myndigheder.
- Kommunen skal gennem beredskabsstyring sikre, at konsekvenserne af alvorlige sikkerhedsmæssige hændelser kan imødegås og begrænses bedst muligt. Beredskabsstyringen omfatter vedligeholdelse af formelle beredskabsplaner og den organisatoriske tilrettelæggelse af krisehåndtering i forbindelse med kritiske sikkerhedshændelser.

Eksempler på kritiske sikkerhedshændelser kan være omfattende nedbrud i it-systemer og andre sikkerhedshændelser, som har alvorlige konsekvenser for kommunens virksomhed og som ikke kan håndteres inden for de normale rammer for daglig driftsafvikling.

Beslutning om hvilke konkrete sikkerhedshændelser, der skal udarbejdes beredskabsplaner for, skal ske på grundlag af en systematisk vurderings- og afklaringsproces.

Sikkerhedsbevidsthed
Kommunens medarbejdere, kommunalbestyrelsesmedlemmer og samarbejdspartnere har alle et medansvar for, at kommunens informationer og informationssystemer beskyttes.

For at sikre at der til stadighed er et tilstrækkeligt bevidsthedsniveau, skal medarbejderne løbende uddannes i emner vedrørende informationssikkerheden.

Uddannelse inden for informationssikkerhed skal tilrettelægges målrettet, således at de forskellige medarbejdergrupper får netop den viden, som er relevant for deres arbejdsområde.

Organisering og ansvar

- *Kommunalbestyrelsen* har det overordnede ansvar for, at kommunens informationssikkerhed styres hensigtsmæssigt og på betryggende vis.
- *Kommunaldirektøren* er den øverste ansvarlige for den administrative styring af informationssikkerhedsindsatsen og skal sikre den fornødne kontrol med efterlevelsen af informationssikkerhedspolitikken.
- *Direktionen* skal sikre, at der er etableret et tværorganisatorisk forum, der bl.a. skal hjælpe projektlederen for databeskyttelse med at vurdere, hvorvidt der er behov for ændringer i den gældende informationssikkerhedspolitik og udmøntningen af politikken. Det er it-styregruppen suppleret af it-koordinatorgruppen, som begge udgør kommunens tværorganisatoriske samarbejdsfora for it-drift.
- *Projektlederen for databeskyttelse* refererer til it-chefen og varetager den overordnede styring af informationssikkerhedsindsatsen i praksis. *Projektlederen for databeskyttelse* har ansvaret for udarbejdelse og vedligeholdelse af informationssikkerhedspolitikken, sikkerhedsregler, handlingsplaner, risikovurderinger og beredskabsplaner, der er omfattet af informationssikkerhedspolitikken.

- Databeskyttelsesrådgiveren har med henvisning til databeskyttelsesforordningens artikel 37, stk. 6 følgende opgaver: Løbende rådgivning af kommunen og kommunens ansatte, rådgivning om kommunens projekter og konsekvensanalyser samt årlig overvågning af kommunens efterlevelse af databeskyttelsesforordningen og databeskyttelsesloven. DPO'en refererer i henhold til Datatilsynets vejledning til kommunalbestyrelsen, men via direktionen.
- *Områdedirektørerne* har ansvaret for, at informationssikkerhedspolitikkens krav og udmøntningen heraf i form af sikkerhedsregler og -procedurer m.v. implementeres og forvaltes korrekt.
- *Organisationens ledere* har ansvaret for den daglige ledelse af informationssikkerhedsindsatsen i de enkelte afdelinger, institutioner og virksomheder.
- *Medarbejdere og kommunalpolitikere* har ansvar for at følge informationssikkerhedspolitikken i sammenhæng med de konkrete ansvarsområder og arbejdsopgaver.
- *Systemejerne* har ansvaret for varetagelsen af aktiver, som relaterer sig til og er væsentlige for kommunens informationsbehandlingen. Ansvarsopgaverne omfatter driftsafvikling, vedligeholdelse og udfasning af aktiverne.

Brud på informationssikkerheden
Såfremt en trussel mod informationssikkerheden eller brud på denne opdages, skal dette straks meddeles til kommunens projektleder for databeskyttelse, som rapporterer sikkerhedsbrud til DPO'en og øvrige relevante parter.

Hvis medarbejdere overtræder politikken, sikkerhedsregler og procedurer, kan det medføre ansættelsesretslige konsekvenser.

For samarbejdspartnere vil overtrædelse af politikken, sikkerhedsregler og procedurer blive betragtet som aftalebrud og kan have konsekvenser derefter.

Såfremt der foreligger mistanke om strafbare forhold, f.eks. overtrædelse af tavshedspligt, vil der blive indgivet politianmeldelse.

Udmøntning
Principperne i politikken skal omsættes til sikkerhedsregler, som omfatter administrative, fysiske og tekniske sikringsforanstaltninger. Reglerne skal godkendes af Direktionen. Udmøntning af reglerne sker i form af procedurer, vejledninger, aftaler med kommunens leverandører, kontrolforanstaltninger samt uddybende it-sikkerhedsregler.

Opfølgning
Som et led i den overordnede sikkerhedsstyring skal politikken revurderes en gang årligt. Projektlederen for databeskyttelse skal sikre, at revurderingen gennemføres.
Kommunen fastlægger på baggrund af risikovurderinger et sikkerhedsniveau, som svarer til betydningen af de pågældende informationer og informationsrelaterede aktiver.

Risikovurderingerne gennemføres under hensyntagen til ressourcer og de økonomiske forhold.

Risikovurderinger udføres som udgangspunkt en gang årligt, eller ved større organisationsændringer, ændringer i informationssystemer, eller hvis andre forhold nødvendiggør det.
Der skal løbende laves opfølgning på, om medarbejdere og kommunalbestyrelsesmedlemmer har tilstrækkeligt kendskab til politikken, sikkerhedsreglerne og gældende procedurer, vejledninger, mv.

Der skal regelmæssigt følges op på overholdelsen af politikken, sikkerhedsregler og -procedurer. Opfølgningen skal som udgangspunkt foretages en gang årligt og udføres af Databeskyttelsesrådgiveren i samarbejde med projektleder for databeskyttelse. Resultatet af opfølgninger rapporteres til Direktionen.

Offentliggørelse
Politikken skal formidles til alle relevante interessenter, herunder samtlige medarbejdere i kommunen. Politikken offentliggøres på kommunens hjemmeside.

Godkendelse
Politikken er første gang vedtaget af Magistraten d. 18. maj 2009 og træder i kraft per denne dato.

Versionshistorik

Version	Vedtaget af	Ændring	Dato
1.0	Magistraten	Første udgave	18. maj 2009
1.1	Årlig revision tiltrådt af direktionen	Faktuelle rettelser og indføjelse af fodnote vedr. overgang fra DS484 til ISO27001.	21.december 2010
1.1.1	Årlig revision tiltrådt af direktionen	Gennemgang med henblik på ajourføring - ikke fundet behov for ændringer.	5. marts 2013
1.2	Årlig revision tiltrådt af direktionen	Der er ikke fortaget ændringer.	7. januar 2014

1.3	Årlig revision tiltrådt af direktionen	Der er ikke fortaget ændringer.	2. december 2014
1.4	Årlig revision tiltrådt af direktionen	Der er foretaget få ændringer i forbindelse med udfasning af DS 484.	12. januar 2016
1.5	Årlig revision	Det er præciseret, at sikkerhedspolitikken også gælder for kommunens databehandlere	12. december 2016
1.6	Revision ift. EU-databeskyttelsesforordning	Ændringer i formalia ved EU-databeskyttelsesforordningens ikrafttrædelse samt fjernelse af kravet om at sikkerhedspolitikken også gælder kommunens databehandlere	22. maj 2018
1.7	Årlig revision	Der er ikke fortaget ændringer.	17. december