INFORMATIONS-SIKKERHEDS-POLITIK

GLOSTRUP KOMMUNE

14. NOVEMBER 2012

Politik

Digital Forvaltning Glostrup

Nærværende informationssikkerhedspolitik er en generel administrativ opdatering af version 1.0 især på baggrund af organisationsændringen den 1. september 2011 og Datatilsynets tilsynsbesøg den 30. maj 2012.

Informationssikkerhedspolitikken er godkendt af direktionen 29. oktober 2012, Økonomiudvalget 6. november 2012 og kommunalbestyrelsen 14. november 2012.

Version 2.0.

INDHOLDSFORTEGNELSE

1. INDLEDNING

Denne informationssikkerhedspolitik er den overordnede ramme for informationssikkerheden i Glostrup Kommune.

Politikken understøtter Glostrup Kommunes vision og målsætninger – og den skal understøtte visionen og de strategiske pejlemærker i kommunens digitaliseringsstrategi.

Informationssikkerhedspolitikken skal vedtages af Kommunalbestyrelsen hvert fjerde år.

Informationssikkerhedspolitikken uddybes i en informationssikkerhedshåndbog inklusive en række bilag og øvrige dokumenter.
Informationssikkerhedshåndbogen godkendes af direktionen.
Direktionen har dog mulighed for at uddelegere beslutningskompetence vedrørende bilag og øvrige dokumenter til andre ledere.

Informationssikkerhedshåndbogen opbygges under anvendelse af sikkerhedsstandarden DS 484:2005 med henblik på at sikre, at alle relevante aspekter vedrørende informationssikkerhed belyses og vurderes.

1.1. Dokumenthistorik

Informationssikkerhedspolitikken blev sidste gang vedtaget i Økonomiudvalget den 2. juni 2009 og i kommunalbestyrelsen den 10. juni 2009.

Informationssikkerhedspolitikken er revideret som en konsekvens af organisationsændringen den 1. september 2011 samt Datatilsynets tilsynsbesøg den 30. maj 2012. Den reviderede informationssikkerhedspolitik er behandlet og godkendt i direktionen den 25. oktober 2012 og i Økonomiudvalget og kommunalbestyrelsen hhv den 6. november 2012 og 14. november 2012.

2. FORMÅL

Glostrup Kommune behandler dagligt og kontinuerligt informationer af vidt forskellig karakter, og det sker gennem brug af forskellige informationssystemer.
Informationssikkerheden har derfor vital betydning for Glostrup Kommunes troværdighed og funktionsdygtighed.

Formålet med informationssikkerhedspolitikken er at definere en ramme for beskyttelse af kommunens informationer og særligt sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

Information kan eksistere i mange former. Det kan være skrevet på papir, lagret elektronisk, transmitteret via kabler eller gennem luften, ligge på en film eller være fremført i tale. Uanset formen skal informationen beskyttes i henhold til dens betydning for kommunen.

Glostrup Kommune har besluttet at anvende et beskyttelsesniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav og indgåede aftaler.

Det skal tilstræbes, at informationssikkerhedspolitikken skal være realistisk, operationel, acceptabel og kontrollerbar – og der skal lægges vægt på reel sikkerhed frem for formel sikkerhed.

Det påhviler direktionen at oplyse kommunens medarbejdere om ansvarlighed i relation til kommunens informationer og informationssystemer.

Hensigten med informationssikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til kommunen, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

3. OMFANG

Politikken omfatter udelukkende administrativ information, dets tilhørende informationsaktiver og arbejdet dermed. Dette er den overordnede afgrænsning, og ordet ”information” vil således udelukkende omfatte ”administrativ information”.

Politikken omfatter inden for disse rammer Glostrup Kommunes informationer, dvs. enhver information, der tilhører kommunen, herunder også informationer, som ikke tilhører kommunen, men som kommunen kan gøres ansvarlig for. Dette inkluderer f.eks. alle informationer om personale, borgere, virksomheder og ejendomme – og alle informationer, som bidrager til administrationen af kommunen, herunder informationer, der er overladt til Glostrup Kommune af andre, samt interne informationer.

Informationssikkerhedspolitikken omfatter alle kommunens informationer, uanset hvilken form de opbevares på og formidles på.

Informationssikkerhedspolitikken gælder for alle ansatte uden undtagelse, dvs. både fastansatte og personer, som midlertidigt arbejder for kommunen gennem et ansættelses- eller andet kontraktforhold. Alle disse personer bliver betegnet som ”medarbejdere”.

Informationssikkerhedspolitikken gælder ligeledes for Kommunalbestyrelsens medlemmer.

Ved hel eller delvis udlicitering af it-drift skal det sikres i samarbejdet med serviceleverandøren, at Glostrup Kommunes sikkerhedsniveau fastholdes således, at serviceleverandøren og dennes medarbejdere, som har adgang til Glostrup Kommunes informationer, som minimum lever op til Glostrup Kommunes informationssikkerhedsniveau.

4. SIKKERHEDSNIVEAU

Det er Glostrup Kommunes politik at beskytte alle informationer og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med kommunens retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

Glostrup Kommune fastlægger på baggrund af en risikovurdering et sikkerhedsniveau, som svarer til betydningen af de pågældende informationer. Glostrup Kommune vil ligeledes basere sikkerhedsniveauet på en afbalanceret risiko- og konsekvensvurdering under hensyntagen til økonomiske forhold. Kommunen vil ikke sikre sig for enhver pris, men skal være derimod være bevidst om enhver risiko.

Direktionen vurderer derfor minimum hvert andet år, om der skal gennemføres en sårbarheds- og risikoanalyse.

Direktionen skal udvikle, administrere og vedligeholde et informationssikkerhedsniveau i overensstemmelse med ovenstående. Dette beskrives i en informationssikkerhedshåndbog, der følger opbygningen af standarden DS 484:2005.

Informationssikkerhedsniveauet svarer som udgangspunkt mindst til de basale beskyttelsesforanstaltninger i DS 484:2005, men der er i informationssikkerhedshåndbogen mulighed for at afvige dette, så længe det er i overensstemmelse med de overordnede principper i det i denne informationssikkerhedspolitik beskrevne sikkerhedsniveau og en risikovurdering i øvrigt.

Ansvaret for informationssikkerhedspolitikkens udførelse og den daglige styring ligger hos kommunaldirektøren, hvis opgave er at sikre, at ledere og medarbejdere gøres bekendt med, at de skal udøve, gennemføre og efterleve de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet i informationssikkerhedshåndbogen. En beskrivelse af kommunaldirektørens operationelle ansvar er anført i afsnit 7.1 ”Kommunaldirektøren”.

Ligeledes er det væsentligt, at informationssikkerhed integreres i forretningsgange, driftsopgaver og projekter.

5. SIKKERHEDSBEVIDSTHED

Informationssikkerhed vedrører kommunens samlede informationsflow, og gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at bidrage til at beskytte Glostrup Kommunes informationer mod uautoriseret adgang, ændring, ødelæggelse og tyveri. Alle medarbejdere skal derfor løbende informeres og uddannes i informationssikkerhed i relevant omfang.

Som brugere af Glostrup Kommunes informationer må alle medarbejdere følge informationssikkerhedspolitkken og de retningslinjer, der er afledt heraf. Medarbejderne må kun anvende kommunens informationer i overensstemmelse med det arbejde, de udfører i kommunen, og de skal beskytte informationerne på en måde, som er i overensstemmelse med informationernes følsomhed og natur.

6. BRUD PÅ INFORMATIONSSIKKERHEDEN

Såfremt en medarbejder opdager trusler mod informationssikkerheden eller brud på denne, skal dette straks meddeles til den nærmeste leder, anden relevant leder eller informationssikkerhedskoordinator med henblik på at få vurderet, om og i givet fald hvordan truslen skal reduceres eller elimineres.

Medarbejdere, der overtræder informationssikkerhedspolitikken, kan blive mødt med ansættelsesretlige konsekvenser såsom advarsel, uansøgt afsked eller bortvisning.

7. INFORMATIONSSIKKERHEDSORGANISATION

Sikkerheden defineres via informationssikkerhedsorganisationen.

7.1. Kommunaldirektøren

Kommunaldirektøren er den øverste sikkerhedsansvarlige, herunder også for informationssikkerheden og dermed også for informationssikkerhedspolitikken.

Kommunaldirektørens opgaver og operationelle ansvar omfatter:

- at sikre, at informationssikkerhedspolitikken forelægges og godkendes af kommunalbestyrelsen hvert fjerde år
- at træffe rimelige forholdsregler til beskyttelse af kommunens informationer, herunder anmode kommunalbestyrelsen om midler og ressourcer dertil
- at forebygge og begrænse risici til en for kommunen kendt og accepteret størrelse
- at vedligeholde informationssikkerhedsorganisationen i forbindelse med organisationsændringer
- at sikre, at informationssikkerhedspolitikken med tilhørende informationssikkerhedshåndbog, bilag og dokumenter implementeres samt løbende revideres og ajourføres
- at træffe de nødvendige forholdsregler for at sikre, at informationssikkerhedspolitikken og afledte retningslinjer bliver overholdt
- at sikre, at enhver sikkerhedsmæssig følsom informationsaktivitet kan henføres til den person, som har udført aktiviteten – samt at sikre gennemførelse af de fornødne kontroller til opdagelse af misbrug eller forsøg herpå
- at drøfte og vurdere sager om misbrug med centerchefer og it-chef[1]
- at sikre den fornødne ledelsesrapportering af status for informationssikkerheden
- at sikre, at kommunens implementering af systemer udføres under iagttagelse af betryggende sikkerhedsforanstaltninger
- at sikre, at kommunens leverandører overholder de sikkerhedsforskrifter, som er gældende for komunens informationer og medarbejdere i samarbejdet med leverandørerne
- at udpege systemejere for samtlige informationssystemer

[1] *It-chefen er centerchefen for Center for It og Udvikling.*

- at udarbejde en brugbar plan til at retablere daglig drift, såfremt informationer eller informationssystemer ødelægges
- at definere regler for arkivering af informationer, så disse kan genskabes senere i et kendt og accepteret omfang

Kommunaldirektøren har mulighed for at uddelegere disse opgaver mod at sikre sig, at de derved udpegede ansvarlige har en informationspligt over for kommunaldirektøren.

7.2. Informationssikkerhedsleder

Centerchefer, funktionsledere og institutionsledere er informationssikkerhedsledere for deres respektive centre, afdelinger og institutioner, dvs. ledere med personaleansvar fungerer som informationssikkerhedsledere.
Informationssikkerhedslederen har ansvaret for overholdelse af informationssikkerhedspolitikken som en del af sit almindelige ledelsesmæssige ansvar inden for eget område.

Informationssikkerhedslederens opgaver omfatter:

- Godkende autorisation af brugere på domæneniveau, dvs. oprette og nedlægge brugere samt ændre deres rettigheder på domæneniveau
- Tilrettelægge informationssikkerheden og informationen herom inden for eget center, afdeling eller institution
- Træffe de nødvendige forholdsregler for at sikre, at informationssikkerhedspolitikken og afledte retningslinjer bliver overholdt
- Udpege og uddanne lokale informationssikkerhedsmedarbejdere
- Sikre, at it-udstyr mærkes og tyverisikres i henhold til forskrifterne
- Godkende og sikre dokumentation af egenudviklede programmer, herunder databaser og regneark, samt anmelde disse til Datatilsynet på linje med opgaverne for en systemejer (se afsnit 7.6), hvis de er omfattet af Persondataloven.

Institutionsledere har desuden som opgave at sikre lokal fysisk sikkerhed vedrørende krydsfelter, netværk, eventuelle servere, pc'er, smartphones, mobiltelefoner, printere og andre digitale enheder.

7.3. Informationssikkerhedsmedarbejder

Derudover har hver informationssikkerhedsleder udpeget en informationssikkerhedsmedarbejder, hvortil de praktiske opgaver vedrørende informationssikkerhed er uddelegeret.

Informationssikkerhedsmedarbejderens opgaver omfatter:

- Udføre brugeradministration, dvs. klargøre autorisation af brugere og forelægge disse for sikkerhedslederen (på domæneniveau) eller systemejeren (på systemniveau) til godkendelse. Ved autorisation af brugere forstås det at oprette og nedlægge brugere samt ændre deres rettigheder
- Vejlede og instruere nye medarbejdere om informationssikkerhed, herunder om behandling af personoplysninger
- Løbende overvåge informationssikkerheden i bred forstand i centret, afdelingen eller institutionen – og rapportere dette til informationssikkerhedslederen
- Rapportere informationssikkerheden efter behov og anmodning til informationssikkerhedskoordinatoren

Det vil være muligt for en informationssikkerhedsleder selv at påtage sig opgaven som informationssikkerhedsmedarbejder, hvilket kan være relevant på mindre institutioner.

Det vil ligeledes være muligt for en informationssikkerhedsleder at udpege en informationssikkerhedsmedarbejder uden for egen afdeling. Det vil derved være muligt for eksempelvis flere afdelinger i et center at anvende samme informationssikkerhedsmedarbejder.

7.4. Informationssikkerhedskoordinator

Kommunaldirektøren skal udpege en særlig informationssikkerhedskoordinator, der har ansvaret for at kontrollere informationssikkerheden og overholdelse af retningslinjer som defineret i informationssikkerhedspolitikken med tilhørende informationssikkerhedshåndbog, bilag og dokumenter.

Informationssikkerhedskoordinatorens opgaver omfatter:

- at sikre udarbejdelse af en ny informationssikkerhedsstrategi efter behov, herunder at der udpeges kommende indsatsområder for arbejdet med informationssikkerhed
- at sikre udarbejdelse af en informationssikkerhedspolitik hvert fjerde år
- at sikre ajourføring af informationssikkerhedshåndbogen og dens tilhørende bilag og dokumenter
- at sikre godkendelse af informationssikkerhedshåndbogen i direktionen
- at kontrollere informationssikkerheden, dvs. at undersøge, om retningslinjerne i informationssikkerhedshåndbogen efterleves i organisationen – og efterfølgende rapportere dette til kommunaldirektøren
- at bistå med faglig viden til centrene om udarbejdelse af anmeldelser til Datatilsynet jf. Persondataloven

- at sikre at centre og institutioner er informeret om forhold vedrørende Persondataloven, herunder lovændringer, bekendtgørelser, fortolkninger etc.
- at bistå med faglig viden til informationssikkerhedsledere, -medarbejdere og systemejere i varetagelsen af deres informationssikkerhedsopgaver
- at sikre, at dokumenter og information vedrørende informationssikkerhed er tilgængelige for kommunens medarbejdere via Globen

7.5. It-chefen

It-chefen er centerchefen for Center for It og Udvikling.

It-chefen er ansvarlig for at påse, at der til stadighed er etableret arbejdsgange og procedurer, som understøtter overholdelse af it-sikkerheden defineret i informationssikkerhedspolitikken. It-chefen er ansvarlig for de tekniske og sikkerhedsmæssige it-driftsopgaver i forbindelse med informationssikkerhedspolitikken.

It-chefens opgaver omfatter:

- at sikre sikkerhed vedrørende kommunens servere og øvrige centrale maskinpark i kommunens serverrum
- at sikre sikkerhedskopiering (backup) af kommunens data i det beskrevne omfang
- at vedligeholde kommunens sikkerhedssystemer, herunder firewall, antivirusbeskyttelse etc.

Derudover har it-chefen på ledelsens vegne initiativpligten over for informationssikkerhedskoordinatoren til at påpege behov for gennemgang, andre initiativer eller konkrete ændringer i informationssikkerhedspolitikken.

7.6. Systemejer

Systemejeren for det enkelte informationssystem har ansvaret for, at systemet på betryggende vis bidrager til at løse den forretningsmæssige opgave, systemet er indkøbt til.
Systemejeren har det økonomiske ansvar for informationssystemet, herunder køb, licenser, drift, vedligeholdelse, support mv.
Systemejeren har ansvaret for at udarbejde en risikovurdering for systemet.
Systemejeren har ansvaret for med passende mellemrum og mindst hvert femte år at vurdere, om informationssystemet til stadighed opfylder behovet.
Systemejeren har ansvaret for om nødvendigt at undersøge markedet for alternativer, og hvis ønsket at indkøbe og implementere et nyt informationssystem til løsning eller understøttelse af opgaven.

Systemejeren har ansvaret for, at informationssystemet overholder Persondataloven, herunder dens bestemmelser om beskyttelse af personhenførbare data og logning.
Systemejeren har ansvaret for, at informationssystemets informationssikkerhed opfylder de retningslinjer, der er anført i informationssikkerhedshåndbogen og dens tilhørende bilag og dokumenter.
Systemejeren har ansvaret for at kontrollere informationssikkerheden vedrørende informationssystemet, dvs. at undersøge, om retningslinjerne i informationssikkerhedshåndbogen med tilhørende bilag og dokumenter efterleves for systemet.

Systemejerens opgaver omfatter:

- Godkende autorisation af brugere på systemniveau, dvs. oprette og nedlægge brugere samt ændre deres rettigheder på systemniveau, på baggrund af en indstilling fra en informationssikkerhedsleder
- Foretage anmeldelser til Datatilsynet i overensstemmelse med Persondataloven
- Udarbejde planer til brug i nødsituationer grundet eksempelvis systemnedbrud
- Fastlægge procedurer og ansvar for intern kontrol med brug af system og informationer, dvs. oprettelse og vedligeholdelse af betryggende arbejdsgange og kontroller
- Styre indkøb og vedligeholdelse af licenser mv. til systemet
- Bidrage til kommunens it-beredskabsplan for det pågældende system, såfremt systemet er beskrevet heri

7.7. Arkivkoordinator

Direktionen udpeger det center, der har det overordnede administrative ansvar for arkivområdet. Opgaven varetages i praksis af en arkivkoordinator, der har en overordnet og koordinerende rolle vedrørende kommunens arkiver.

Hver centerchef har ansvaret for, at centrets arkiver, digitale og fysiske, lever op til bestemmelserne i Glostrup Kommunes gældende arkivinstruks.

7.8. Øvrige medarbejdere

Alle ansatte i kommunen skal overholde informationssikkerhedspolitikken under iagttagelse af "almindelig sund fornuft". Informationssikkerhedshåndbogen indeholder en beskrivelse af de informationssikkerhedsområder, der er relevante for Glostrup Kommune.