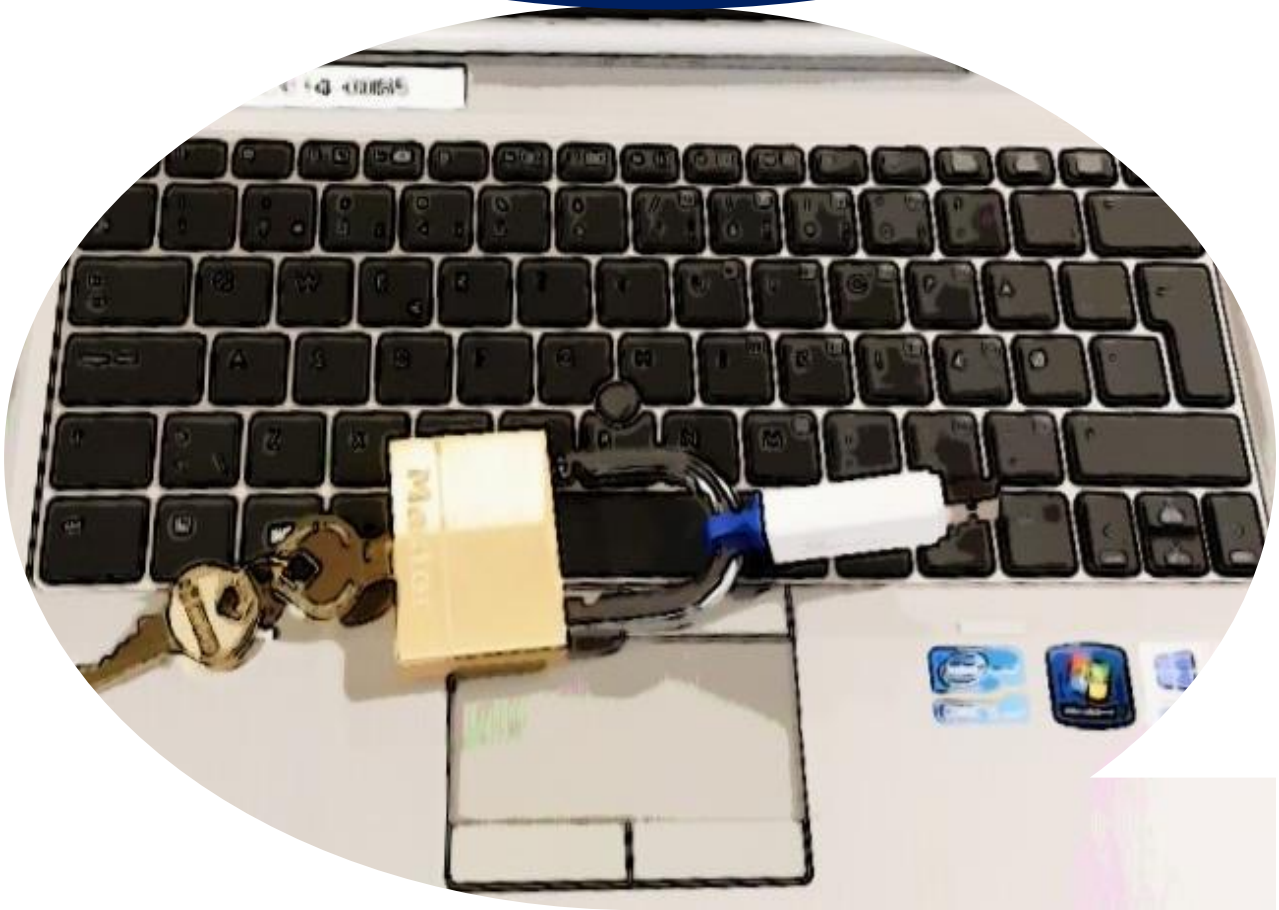
GLOSTRUP
KOMMUNE

Politik for informationssikkerhed



Informationssikkerhedspolitik Glostrup Kommune

Glostrup Kommunes informationssikkerhedsindsats

Glostrup Kommune er i besiddelse af en mængde data og informationssystemer, som er afgørende for varetagelsen af kommunens opgaver og forpligtelser. Kommunen behandler som led heri ofte følsomme oplysninger om borgere og virksomheder, hvilket derfor kræver særlig beskyttelse.

Beskyttelse af data, herunder personoplysninger og informationssystemer er et vigtigt fokusområde, som håndteres gennem kommunens informationssikkerhedsindsats.

Målsætningen med informationssikkerhedsindsatsen er at beskytte data og informationssystemer mod uautoriseret eller utilsigtet adgang, herunder bl.a. anvendelse, videregivelse, driftsforstyrrelse, ændring eller ødelæggelse. Formålet med informationssikkerhedsindsatsen er ligeledes at undgå sikkerhedsbrud, og i tilfælde af sikkerhedsbrud sikre en hurtig og effektiv håndtering, herunder sikring af informationerne.

Indsatsen består bl.a. i en række sikringsforanstaltninger, som etableres med henblik på at beskytte data og informationssystemer mod at blive kompromitteret, awareness i organisationen samt udarbejdelse af retningslinjer for håndteringen af informationer mm. Indsatsen tager sit naturlige udgangspunkt i informationssikkerhedspolitikken.

Formålet med informationssikkerhedspolitikken

Formålet med Glostrup Kommunes informationssikkerhedspolitik er at definere og fastlægge den overordnede ramme og principper for beskyttelse af kommunens data og informationssystemer.

Politikken skal udmøntes gennem implementering af sikkerhedsforanstaltninger på baggrund af risikovurderinger med henblik på at sikre et passende sikkerhedsniveau for de behandlede personoplysninger, og således at der med udgangspunkt heri udarbejdes interne retningslinjer, som skal beskytte data og informationssystemer med udgangspunkt i tre centrale begreber:

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

Følgende indsatsområder er centrale:

- Kommunens it-infrastruktur skal til stadighed være driftssikker og effektivt opretholdt for at beskytte mod interne og eksterne trusler, herunder 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 eller menneskelige fejl, hændelige uheld eller forsætlige handlinger, herunder skadevoldende handlinger og misbrug.
- God sikkerhedsskik, herunder at principper og normer for adfærd i anvendelsen af kommunens informationssystemer skal være klart formuleret og formidlet til medarbejderne.
- Konsekvenser af sikkerhedsbrud reduceres til et niveau, hvor konsekvenserne er mindst mulige.

Fastlæggelse af informationssikkerhedsniveauet i Glostrup Kommune

Glostrup Kommune skal til enhver tid beskytte data forsvarligt og udelukkende tillade brug, adgang til og offentliggørelse af data i overensstemmelse med gældende lovgivning samt kommunens sikkerhedsregler.

Kommunen skal til enhver tid leve op til:

- Sikkerhedsmæssige krav, der følger af den til enhver tid gældende lovgivning. 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.

Informationssikkerhedsniveauet I Glostrup Kommune er fastlagt ud fra en ambition om et højt sikkerhedsniveau og på baggrund af de konkrete risiko- og konsekvensanalyser .

Tiltag til forbedring af informationssikkerheden implementeres i overensstemmelse med følgende overordnede 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.
- Informationssikkerhedsniveauet skal fastsættes ud fra lovgivningsmæssige krav.
- Kommunen holder sig orienteret i KL's udmeldinger og efterlever udmeldinger, afgørelser mv. fra bl.a. Datatilsynet.
- De it-sikkerhedsansvarlige følger arbejdet i Den Storkøbenhavnske Digitaliseringsforening (DSD), og bruger vejledninger og rådgivning fra DSD som inspiration til indholdet af kommunens egne interne vejledninger, arbejdsgange, koncepter mv. samt fortolkninger i forbindelse med konkrete problemstillinger.
- Databeskyttelsesrådgiveren inddrages i nødvendigt omfang, herunder ved anskaffelse af it-systemer, udarbejdelse af vejledninger samt ved risiko- og konsekvensanalyser.
- De it-sikkerhedsansvarlige rådfører sig med kommunens egne jurister og ved intern tvivl og lignende behov med databeskyttelsesrådgiveren (DPO) vedrørende spørgsmål om beskyttelse af personoplysninger.
- Kommunen fastlægger på baggrund af risikovurderinger et sikkerhedsniveau, som svarer til betydningen af de pågældende data og informationsrelaterede aktiver. Risikovurderingerne gennemføres løbende under hensyntagen til ressourcer og de økonomiske forhold, herunder ved større organisationsændringer og ændringer i informationssystemer.
- 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.

Hvem skal efterleve informationssikkerhedspolitikken

Informationssikkerhedspolitikken omfatter enhver form for data, som ejes, opbevares eller behandles af kommunen og kommunens databehandlere, uanset hvilket medie, informationen er lagret på og uanset hvordan data fremstår, f.eks. – elektronisk, papirbaseret, i tale, transmitteret eller filmisk form mv.

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

- Medarbejdere – både fastansatte, midlertidigt ansatte, frivillige ol.
- Medlemmer af kommunalbestyrelsen i det omfang de ikke er undtaget, jf. styrelseslovens § 8b
- Eksterne samarbejdspartnere, herunder men ikke begrænset til:
    - Institutioner med driftsoverenskomst.
    - Personer og virksomheder, der udfører opgaver for kommunen.
    - Nævn, som kommunen udøver sekretærbistand til.

Sikkerhedsbevidsthed

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

For at sikre, at der til stadighed er et tilstrækkeligt bevidsthedsniveau i kommunen, skal medarbejderne løbende uddannes i emner indenfor informationssikkerhed.

Sikkerhedsorganisering og -ansvar

- Kommunalbestyrelsen har det overordnede ansvar for, at kommunens informationssikkerhed styres hensigtsmæssigt og på betryggende vis, samt ansvar for nærværende informationssikkerhedspolitik.
- Kommunaldirektøren er den øverst ansvarlige for den administrative styring af informationssikkerhedsindsatsen og skal sikre den fornødne kontrol med efterlevelsen af informationssikkerhedspolitikken, herunder godkende interne retningslinjer/vejledninger.
- Digitaliserings- og porteføljerådet (DPR) skal i samarbejde med kommunens jurister hjælpe it-sikkerhedskoordinatoren med at vurdere, hvorvidt der er behov for ændringer i den gældende informationssikkerhedspolitik og udmøntningen af politikken. Det er DPR, som udgør kommunens tværorganisatoriske samarbejdsfora for digitalisering, herunder rådgivning og anbefalinger ifm. anskaffelser af it-systemer.
- Digitaliserings- og Porteføljerådet (DPR) har ansvar for at sikre en central styring, koordinering og kvalitetssikring af anskaffelser ift. valg af teknologisk platform, sammenhæng til eksisterende it-infrastruktur og arkitektur, og kobling til organisationens strategiske målsætninger; porteføljestyring; gevinstrealisering; anskaffelse, udvikling og vedligeholdelse af program- og projektværktøjskassen; initiering af digitale kompetenceløft; samt kvalificering af gode ideer og innovationsdriver.
- It-sikkerhedskoordinatoren og it-chefen har ansvaret for udarbejdelse og vedligeholdelse af informationssikkerhedspolitikken, sikkerhedsregler, retningslinjer/vejledninger, handlingsplaner og beredskabsplaner, der er omfattet af informationssikkerhedspolitikken.
- Kommunens jurister bistår med relevant rådgivning af relevante parter om gældende ret indenfor det persondataretlige område.
- Databeskyttelsesrådgiveren (DPO) skal udføre en række opgaver i overensstemmelse med databeskyttelsesforordningens artikel 39, stk. 1
- Centercheferne har ansvaret for implementering og overholdelse af gældende ret og interne retningslinjer indenfor it-sikkerhed i deres egne centre.
- Alle ansatte med lederansvar har ansvaret for den daglige ledelse af informationssikkerhedsindsatsen i de enkelte afdelinger, institutioner og enheder, samt at

udarbejde aktivitetsfortegnelser og holde disse ajour samt tilhørende nødvendige risikovurderinger.
- Alle medarbejdere og kommunalpolitikere har ansvar for at følge informationssikkerhedspolitikken i sammenhæng med de konkrete ansvarsområder.
- De enkelte systemejere har ansvaret for at godkende oprettelse og ophør af autorisation af brugere; indgå og føre tilsyn med databehandleraftaler på it-systemer; det økonomiske ansvar for indkøb og vedligeholdelse af licenser og drift af it-systemer.
- Glostrup Kommunes IT afdeling er ansvarlig for intern kontrol med betryggende arbejdsgange og kontroller af kommunes IT-systemer.

Sikkerhedsbrud

Såfremt en trussel mod informationssikkerheden eller brud på denne opdages, skal dette straks meddeles til nærmeste leder, der skal kontakte it-sikkerhedskoordinatoren og it-chefen iht. den procedure, der er beskrevet i den til enhver tid gældende "Handlingsplan for håndtering af brud på Glostrup Kommunes IT-sikkerhed".

Udmøntning af informationssikkerhedspolitikken

Principperne i informationssikkerhedspolitikken skal omsættes til sikkerhedsregler, som omfatter organisatoriske, fysiske og tekniske sikringsforanstaltninger. Udmøntning af reglerne sker i form af procedurer, retningslinjer/vejledninger, handlingsplaner, aftaler med kommunens leverandører, kontrolforanstaltninger og uddybende it-sikkerhedsregler mv.

Med godkendelsen af denne informationssikkerhedspolitik, tildeles direktionen ligeledes kompetencen til at fastsætte sådanne retningslinjer mv., så længe disse er i overensstemmelse med den overordnede informationssikkerhedspolitik.

Ændring af informationssikkerhedspolitikken

Som et led i den overordnede sikkerhedsstyring skal direktionen påse, at informationssikkerhedspolitikken revurderes, når det findes nødvendigt.

Det er kommunalbestyrelsen, der har beslutningskompetencen til at godkende informationssikkerhedspolitikken.

Politikken skal formidles til alle relevante interessenter, herunder samtlige medarbejdere i kommunen, og offentliggøres på www.glostrup.dk.

Ikrafttræden

Denne informationssikkerhedspolitik afløser den hidtidige politik, træder i kraft i forbindelse med godkendelse i kommunalbestyrelsen.