Politik for informationssikkerhed i Hvidovre Kommune

Indhold

Politik for informationssikkerhed i Hvidovre Kommune

Denne politik er sammen med informationssikkerhedshåndbogen og databeskyttelsespolitikken grundlaget for brugen af informationsteknologi og håndtering af personoplysninger i Hvidovre Kommune.

Rammer og gyldighed

Politikken gælder for alle ansatte på alle arbejdspladser i Hvidovre Kommune, og den gælder ved al brug af programmer, systemer og kommunikation på alle platforme, dvs. både PC, smartphone, tablet osv.

Politikken udmøntes i informationssikkerhedshåndbogen og databeskyttelsespolitikken. Både politik og håndbog skal altid findes tilgængelig for alle medarbejdere i kommunen.

Alle medarbejdere i kommunen har en pligt til at sætte sig ind i kommunens informationssikkerhedshåndbog og databeskyttelsespolitik.

Målsætning

Hvidovre Kommune gennemfører alle nødvendige aktiviteter for at sikre tilstrækkelig sikkerhed i forhold til:

Fortrolighed
Dette dækker over fortrolig behandling, modtagelse, forsendelse og opbevaring af data, hvor det kun er autoriserede personer, der får adgang til oplysningerne.

Integritet
Kommunens systemer skal fungere pålideligt og korrekt, så vi mindsker risikoen for, at fejl i systemet, menneskelige fejl eller udefrakommende hændelser fører til et ukorrekt og/eller fejlbehæftet datagrundlag for kommunens sagsbehandling.

Tilgængelighed
Informationer og data skal være tilgængelige for de ansatte, som skal bruge dem i arbejdet med at servicere borgerne Derfor skal systemerne driftssikres og samtidig skal risikoen for nedbrud og tab af data mindskes.

Det er Hvidovre Kommunes mål at opretholde et niveau af informationssikkerhed, der overholder de til enhver tid gældende regler og ISO-standarder, og samtidig sikrer, at kommunens holdninger og principper efterleves i videst muligt omfang.

Vores holdninger og principper

Hvidovre Kommunes virke afhænger af håndteringen af informationer. Af denne grund betragter vi informationssikkerhed med samme alvor som andre spørgsmål om sikkerhed i kommunen.

Vi arbejder med informationssikkerhed for at understøtte kommunens opgaver og for at sikre kommunens troværdighed over for bl.a. borgere, virksomheder og offentlige samarbejdspartnere.

Vi sørger for, at alle medarbejdere har den nødvendige viden for at kunne arbejde med sikker behandling af informationer i kommunen.
Vi prioriterer undersøgelse af arbejdsgange og processer på de områder i organisationen, hvor medarbejderne håndterer de mest følsomme eller kritiske informationer. På den måde har vi mulighed for at sætte ind med de tiltag, der skal til for at opretholde et så højt sikkerhedsniveau som påkrævet.

Der skal være nedskrevne procedurer og arbejdsgange på de områder, hvor vi behandler personoplysninger. Formålet er at sikre, at informationssikkerhed og persondatabeskyttelse bliver en integreret del af driften og det daglige arbejde.

Hvis eksterne parter bliver berørt af brud på informationssikkerheden i Hvidovre Kommune, vil vi kommunikere åbent og så hurtigt som muligt til de berørte parter.

Databeskyttelse i Hvidovre Kommune

I Hvidovre Kommune følger de ansatte de seks principper fra den europæiske databeskyttelsesforordning og den supplerende danske databeskyttelseslov. De seks principper er:

Lovlighed, rimelighed og gennemsigtighed

Dette princip handler om, at personoplysninger kun må behandles med et lovligt og rimeligt formål. Samtidig skal personoplysninger behandles på en gennemsigtig måde i forhold til de registrerede, sådan at der altid er gennemsigtighed i forhold til hvem der er ansvarlig for behandlingen, og hvad lovgrundlaget og formålet med behandlingen er.

Formålsbegrænsning

Dette princip handler om, at personoplysninger kun må indhentes til specifikke og saglige formål, og herefter må oplysningerne ikke bruges til andre formål, der er uforenelige med det formål, oplysningerne oprindeligt blev indsamlet til.

Opbevaringsbegrænsning

Dette princip handler om, at personoplysninger skal slettes, begrænses eller anonymiseres, når vi ikke længere har behov for oplysningerne i forhold til det formål, de blev indsamlet til. Dette princip skal efterleves under hensyntagen til reglerne om notat- og journaliseringspligt samt reglerne arkivering efter arkivloven.

Rigtighed

Dette princip handler om, at de personoplysninger, kommunen gemmer, skal være korrekte og opdaterede. Hvis en oplysning er forkert, skal denne ajourføres eller berigtiges. Dette princip skal efterleves under hensyntagen til reglerne om notat- og dokumentationspligt.

Dataminimering

Dette princip handler om, at man kun må behandle de personoplysninger, der er nødvendige for at opnå det formål, oplysningerne er indsamlet til. En sagsbehandler skal dog som udgangspunkt gemme alle oplysninger, vedkommende modtager i forbindelse med sagsbehandlingen for at overholde notatpligten efter forvaltningsloven.

Integritet og fortrolighed

Dette princip handler om, at personoplysninger skal beskyttes mod ulovlig eller uautoriseret adgang og behandling. Det skal ligeledes sikres, at oplysninger ikke går tabt eller bliver ændret uberettiget.

Persondatabeskyttelse og hvordan Hvidovre Kommune håndterer personoplysninger er nærmere beskrevet i kommunes databeskyttelsespolitik, hvorfor der refereres til denne.

Opfølgning
Hvidovre Kommune måler, vurderer og følger op på informationssikkerheden på følgende måde:

1. Løbende registrering og opfølgning på brud eller uregelmæssigheder i forhold til informationssikkerheden.

2. Løbende registrering af alle tiltag inden for informationssikkerhed.

3. Opfølgning på medarbejdernes viden om informationssikkerhed i kommunen.

4. Gennemførelse af uafhængige revisioner af tredjepart og evalueringer af informationssikkerheden.

5. Gennemførelse af databeskyttelsesrådgiverens tilsyn og årlige rapportering om kommunens efterlevelse af reglerne i den europæiske databeskyttelsesforordning og den supplerende danske databeskyttelseslov.

Revision af Politik
Kommunens forum for informationssikkerhed (Sikkerhedsforum) har det overordnede ansvar for vedligeholdelse og revision af kommunens informationssikkerhedspolitikker, herunder nærværende politik for informationssikkerhed, informationssikkerhedshåndbogen og databeskyttelsespolitikken.

Der skal ske revision af kommunens informationssikkerhedspolitikker mindst hvert andet år eller ved væsentlige ændringer.

Godkendelsesproces for politik
Politikker for informationssikkerhed udarbejdes og vedligeholdes af Sikkerhedsforum, der indstiller til behandling og godkendelse i Chefforum og Direktion, før politikken endeligt behandles i Økonomiudvalget

Politikker for informationssikkerhed indstilles til fornyet godkendelse i Økonomiudvalget hvert fjerde år eller ved væsentlige ændringer. Gældende informationssikkerhedspolitikker skal mindst hvert andet år forelægges kommunens Sikkerhedsforum til fornyet behandling og godkendelse.

Denne politik for informationssikkerhed erstatter ”Hvidovre Kommunes Informationssikkerhedspolitik” behandlet og godkendt af kommunalbestyrelsen den 18. december 2012.

Denne politik er godkendt af Hvidovre Kommunes Økonomiudvalg d. 23.03.2022