KØBENHAVNS KOMMUNE

It-sikkerhedspolitik for Københavns Kommune

Mål

Københavns Kommune ønsker, at København skal være et attraktivt sted at bosætte sig og en attraktiv by at investere i. Dette skal blandt andet opnås gennem effektivitet og kvalitet i kommunens serviceydelser og skabelse af et solidt grundlag for tillid fra borgerne såvel som fra virksomhederne. En vigtig forudsætning herfor samt for efterlevelse af kommunens it-strategi er, at kommunen har et passende og tilstrækkelig højt it-sikkerhedsniveau. It-sikkerhedsniveauet skal leve op til lovgivningens krav, herunder kravene i persondataloven og være i overensstemmelse med den til enhver tid værende gængse praksis i Danmark for offentlige myndigheder inden for dette område. Fastlæggelsen af it-sikkerhedsniveauet skal samtidig hermed ske under hensyntagen til den teknologiske udvikling og behovet for effektiv borgerbetjening.

For Københavns Kommune er det vigtigt at sikre:

- **Fortrolighed**
  Målet er at etablere en fortrolig behandling, herunder transmission og opbevaring af person- og værdioplysninger, hvor kun autoriserede og autentificerede brugere har adgang, og hvor brugernes adgang er begrænset til det nødvendige. Hensyn til effektivitet og fleksibilitet i sagsbehandlingen skal altid afvejes mod hensynet til borgernes personlige integritet.
- **Integritet**
  Det er målet at opnå en pålidelig og korrekt funktion i kommunens it-systemer med minimeret risiko for ukorrekt datagrundlag og datatab, for eksempel som følge af menneskelige eller systemmæssige fejl, forsøg på svindel eller bedrageri samt udefrakommende hændelser.
- **Tilgængelighed**
  Målet er en høj tilgængelighed, således at kommunens it-systemer er tilgængelige for brugerne og for borgerne og virksomhederne, når de har behov for det. Det er endvidere målet at minimere risikoen for systemnedbrud. It-systemernes tilgængelighed og kapacitet skal afspejle kommunens, borgernes og virksomhedernes behov for adgang til de oplysninger, der er nødvendige for en effektiv sagsbehandling, som udføres til tiden.

Kommunens it-sikkerhedsniveau skal fastlægges ved brug af periodisk gennemførte risikovurderinger samt ved risikovurderinger, der gennemføres ved anskaffelser og ændringer af it-systemer samt ved ændringer i det it-miljø, systemerne opererer i.

Anvendelsesområde

It-sikkerhedspolitikken gælder for elektronisk databehandling af personoplysninger og værdioplysninger i kommunen, det vil sige oplysninger, der har en væsentlig økonomisk eller forvaltningsmæssig betydning for kommunen.
Herudover gælder it-sikkerhedspolitikken for kommunens manuelle behandlinger af personoplysninger i kommunen, når oplysningerne indgår i eller senere skal indgå i et register.

It-sikkerhedshåndbog

It-sikkerhedsreglerne i Københavns kommune er samlet i en it-sikkerhedshåndbog, som indeholder:

- It-sikkerhedspolitikken
- It-sikkerhedsregulativ for Københavns Kommune.
- En række uddybende It-sikkerhedsregler for Københavns Kommune.

It-sikkerhedshåndbogen gælder for hele kommunen.
It-sikkerhedshåndbogen publiceres elektronisk på kommunens intranet.
It-sikkerhedsregulativet og de uddybende It-sikkerhedsregler skal tage udgangspunkt i ISO 27001 - 2.

ISO 27001 – 2 beskriver at It-sikkerhedsarbejdet består i risikoanalyse, planlægning, udførelse(fastsættelse), og efterlevelse af It-sikkerhedsreglerne på følgende områder:

- Sikkerhedspolitik.
- Organisering af it-sikkerhed.
- Styring af aktiver.
- Medarbejdersikkerhed.
- Fysisk sikkerhed.
- Styring af kommunikation og drift.
- Adgangsstyring.
- Anskaffelse, udvikling og vedligeholdelse af informationssystemer.
- Styring af it-sikkerhedshændelser.
- Beredskabsstyring.
- Overensstemmelse med krav og politikker.

Ansvar og organisering
Dette skal være beskrevet i Københavns Kommunes Regulativ for It-sikkerhed

Løbende vedligeholdelse
It-sikkerhedspolitikken er forankret i It-sikkerhedsfunktionen, som er ansvarlig for udarbejdelse, vedligeholdelse og revurdering af politikken.

Vedligeholdelsen skal omfatte en vurdering af mulighederne for at tilpasse it-sikkerheden og sikkerhedsstyringen ved ændringer af organisatorisk, lovgivningsmæssig, teknisk eller anden karakter.

Bevidsthed om it-sikkerhed
En høj it-sikkerhedsbevidsthed og hensigtsmæssig adfærd hos medarbejderne er blandt de vigtigste sikkerhedsforanstaltninger. Det er således kommunens mål, at der overalt er en høj bevidsthed om it-sikkerhed.

Derfor skal It-sikkerhedspolitikken, It-sikkerhedsregulativet og de it-sikkerhedsregler der uddyber dette kommunikeres til alle relevante interessenter - herunder samtlige af kommunens medarbejdere.

Medarbejderne skal endvidere ved ansættelse og løbende gennem ansættelsesforholdet uddannes og bevidstgøres om forhold, der relaterer sig til fastholdelse af et for kommunen passende og tilstrækkelig højt it-sikkerhedsniveau.

It-beredskab
It-systemer, der er vitale for kommunens betjening af borgerne og virksomhederne, og som således er kritiske for kommunens drift, skal identificeres, og der skal fastsættes maksimalt acceptable tider for utilgængelighed for så vidt angår disse it-systemer. Der skal endvidere udarbejdes, vedligeholdes og

afprøves beredskabsplaner, der sikrer nøddrift, eskalering, retablering og genoptagelse af normal drift i tilfælde af større nedbrud, ulykker eller katastrofer i forhold til kritiske it-systemer.

Opfølgning på it-sikkerhed
Københavns Kommune ønsker at måle, vurdere og følge op på it-sikkerheden i kommunen og at opfølgningen skal ske ved anvendelse af fælles metoder i alle forvaltningerne.

Det er kommunens mål, at løbende risikovurderinger viser en stadig faldende tendens for så vidt angår områder med en tidligere påvist uacceptabel høj risiko.

Herudover skal der måles vurderes og følges op på følgende måde:

- Ved løbende at registrere og følge op på hændelser inden for it-sikkerhedsområdet
- Ved at behandle it-sikkerhedshændelser og tiltag i relevante fora med henblik på løbende forbedring af it-sikkerheden og vidensdeling
- Ved løbende at følge op på vidensniveau inden for it-sikkerhedsområdet i kommunen
- Ved løbende at gennemføre revisioner og evalueringer af it-sikkerheden
- Ved mindst en gang hvert 2. år at revurdere it-sikkerhedspolitikken
- Ved mindst en gang årligt at revurdere it-sikkerhedsregulativet

Godkendt af Borgerrepræsentationen den