It-sikkerhedspolitik for Københavns Kommune

Indledning

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 for virksomhederne. En vigtig forudsætning herfor samt for efterlevelse af kommunens it-strategi er, at kommunen har et passende og tilstrækkelig højt it-sikkerhedsniveau, som lever op til henholdsvis persondatalovens og sikkerhedsbekendtgørelsens krav, og som er i overensstemmelse med den til enhver tid værende gængse praksis i Danmark for offentlige myndigheder inden for dette område.

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.
- **Dataintegritet**
  Det er målet at opnå en pålidelig og korrekt funktion i kommunens it-systemer med minimeret risiko for ukorrekt datagrundlag, 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.

Københavns Kommunes it-sikkerhedspolitik skal – sammen med sikkerhedsbekendtgørelsen - danne rammen for it-sikkerhedsregulativets bestemmelser. Politikken og regulativet skal skabe grundlaget for en sikker anvendelse af it i kommunen.

It-sikkerhedspolitikken skal sammen med it-sikkerhedsregulativet publiceres i en it-sikkerhedshåndbog, som skal være tilgængelig elektronisk.

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.

Ansvar og organisering

Borgerrepræsentationen vedtager kommunens it-sikkerhedspolitik og it-sikkerhedsregulativ.

Økonomiudvalget fører det overordnede tilsyn med kommunens it-sikkerhed og koordinerer it-sikkerhedsarbejdet i kommunen.

Borgerrepræsentationens Sekretariat fører på vegne af Økonomiudvalget det daglige overordnede tilsyn med overholdelsen af kommunens it-sikkerhedsbestemmelser og koordinerer i praksis kommunens it-sikkerhedsarbejde på tværs af forvaltningerne.

Borgerrepræsentationens Sekretariat udarbejder en it-sikkerhedshandlingsplan, der skal sikre, at it-sikkerhedspolitikken udmøntes i praksis og forelægger denne for Økonomiudvalget til orientering.

Overborgmesteren og den enkelte borgmester har, jf. kommunens styreform, ansvaret for it-sikkerhedsarbejdet inden for hver deres forvaltningsområde.

Direktionerne har inden for eget område ansvaret for gennemførelse af risikovurderinger og for fastlæggelse af et passende it-sikkerhedsniveau for området. Direktionen for Koncernservice har desuden ansvaret for fastlæggelse af it-sikkerhedsniveauet i forhold til kommunens netværk samt netværksudstyr og servere m.v., som ejes af Koncernservice. Dette skal opnås ved at begrænse identificerede risici til et acceptabelt niveau gennem en styret etablering af forebyggende og korrigerende foranstaltninger.

Direktionerne skal inden for eget område iværksætte de foranstaltninger, der er nødvendige for at opnå en tilstrækkelig it-sikkerhed og tilse, at medarbejdere, som varetager it-sikkerhedsfunktioner, er i besiddelse af de nødvendige kompetencer. Foranstaltningerne skal iværksættes ud fra risiko og væsentlighed og på grundlag af såvel sikkerhedsmæssige som økonomiske betragtninger.

It-sikkerhedslederne skal inden for eget område føre tilsyn med it-sikkerhedsfunktionerne og med, at it-sikkerhedsarbejdet bliver udført i overensstemmelse med de til enhver tid gældende it-sikkerhedsbestemmelser.

Systemejerne skal være ansvarlige for it-systemernes funktionalitet, opbygning, anvendelse og sikkerhedsløsning samt for at iværksætte de nødvendige foranstaltninger til beskyttelse af it-systemet og de person- og værdioplysninger, der er indeholdt heri.

Den it-ansvarlige skal sikre, at opbygning og anvendelse af it-platform, arkitektur, driftsmiljø og kommunikationsforbindelser er i overensstemmelse med de it-sikkerhedsmæssige krav og den til enhver tid gældende it-strategi.

Herudover skal der etableres et udvalg for it-sikkerhed og et samarbejdsforum for henholdsvis it-sikkerhedsledere og systemejere bl.a. med henblik på at fremme det tværgående it-sikkerhedssamarbejde i kommunen og imellem de respektive it-sikkerhedsfunktioner.

Ledere skal på alle niveauer sikre, at det er muligt for medarbejderne at efterleve deres ansvar for at beskytte kommunens person- og værdioplysninger.

Alle medarbejderne skal medvirke til at beskytte kommunens person- og værdioplysninger og skal agere i henhold til kommunens it-sikkerhedspolitik og it-sikkerhedsregulativ.

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 offentliggøres og 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, 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

Denne opfølgning beskrives nærmere i it-sikkerhedshandlingsplanen.

It-sikkerhedsregulativ
It-sikkerhedspolitikken skal uddybes i et it-sikkerhedsregulativ for Københavns Kommune. It-sikkerhedsregulativet skal være udformet som et fælles sæt af regler, der gælder for hele kommunen.

Kommunens it-sikkerhedsregulativ skal opfylde sikkerhedsbekendtgørelsens krav om interne uddybende sikkerhedsbestemmelser for Københavns Kommune.

It-sikkerhedsregulativet skal tage udgangspunkt i Dansk Standard for informationssikkerhed, DS484:2005, og anvende standarden som skabelon og reference.

Der gælder ingen formelle krav om efterlevelse eller implementering af DS484:2005 i kommunen. Kommunens ønsker og behov har derfor forrang for DS484:2005 ved udarbejdelse og vedligeholdelse af it-sikkerhedsregulativet.

It-sikkerhedsregulativet skal være operationelt og realistisk, og det skal indeholde regler, der beskriver en klar ansvars- og opgavefordeling i forvaltningerne generelt og i forhold til Koncernservice.

It-sikkerhedsregulativet skal endvidere være tilskåret til det nødvendige suppleret med vejledninger o. lign. Lovtekster m.v. skal ikke gentages i it-sikkerhedsregulativet.

Sikkerhedsbrud
Manglende efterlevelse af it-sikkerhedspolitikken og it-sikkerhedsregulativet kan få særdeles store konsekvenser for kommunen, medarbejderne, borgerne og virksomhederne. Det kan dreje sig om store menneskelige omkostninger eller store økonomiske tab, som der ikke findes nogen erstatning for. Overtrædelse af it-sikkerhedspolitikken eller it-sikkerhedsregulativet skal derfor af kommunens ledelse betragtes med stor alvor.

Kommunens ledelse skal dog samtidig have et balanceret syn på sikkerhedsbrud, idet sikkerhedsbrud kan og vil ske. Det er vigtigt, at sikkerhedsbrud rapporteres, således at de kan opfanges og håndteres på en professionel og hensigtsmæssig måde. Formålet hermed er at minimere konsekvenser, undgå gentagelser og at drage læring.

Løbende vedligeholdelse
It-sikkerhedspolitikken er forankret i Borgerrepræsentationens Sekretariat, 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.

Denne politik er tiltrådt af Borgerrepræsentationen den: