Hillerød Kommunes Informationssikkerhedspolitik

Indledning
Det er af afgørende betydning, at borgere, virksomheder, samarbejdspartnere og den øvrige offentlige sektor har tillid til, at kommunen passer på deres informationer og den nødvendige sikkerhed bliver opretholdt samt at lovgivning bliver overholdt. Informationssikkerhedspolitikken i Hillerød Kommune udgør den overordnede ramme for kommunens informationssikkerhed.

Informationssikkerhed
Informationssikkerhed betyder:

- Beskyttelse af kommunens informationer i alle former for it-systemer, digitale løsninger og digital kommunikation.
- Beskyttelse af fysisk udstyr som lagre og behandler informationer.
- Beskyttelse af kommunens papirer og lokaler der indeholder informationer

Informationssikkerhed udmønter sig i:

- Organisatoriske sikkerhedsforanstaltninger, som fastsættes via regler og procedure for hvorledes kommunens ledelse og ansatte skal beskytte kommunes informationer
- Tekniske sikkerhedsforanstaltninger som beskytter informationer i kommunens digitale løsninger, it-udstyr og netværk.

Formål og principper
Formålet med Hillerød Kommunes informationssikkerhedspolitik er at definere og fastlægge de overordnede principper for kommunens informationssikkerhed.
Politikken skal resultere i relevante sikkerhedsforanstaltninger og løsninger, som skal beskytte kommunens information med udgangspunkt i tre centrale begreber:

- **Tilgængelighed**: at kunne have adgang til, og bruge information, når der er behov for det.
- **Integritet**: at information forbliver pålidelig, korrekt og fuldstændig.
- **Fortrolighed**: at information ikke kommer til uvedkommendes kendskab.

Sikkerhedsforanstaltninger skal rettes mod alle former for eksterne og interne trusler, hændelige fejl og uheld og bevidst skadevoldende handlinger og misbrug.

Hillerød Kommune implementerer informationssikkerheden ud fra følgende principper:

- Der skal være troværdighed på sikkerhedsområdet over for borgere, samarbejdspartnere og omverdenen.
- Sikkerhedsløsninger skal være tilrettelagt, så medarbejderne oplever det som en naturlig del af det daglige arbejde og så vidt muligt ikke som en barriere. Løsninger skal følge anerkendte standarder eller "Best Practice".
- Kommunen styrer informationssikkerheden i overensstemmelse med almindeligt anerkendte metoder og procedurer for informationssikkerhed.

Omfang

Informationssikkerhedspolitikken omfatter alle informationer som Hillerød Kommune er dataansvarlig for. Informationssikkerhedspolitikken gælder for alle personer undtagelse – både fastansatte og midlertidigt ansatte, praktikanter, vikarer, politikere og eksterne konsulenter, mv. - som arbejder i eller for kommunen (under ét betegnet som medarbejdere). Ved en evt. serviceleverandør af kommunens opgaver (databehandlere), skal kommunen sikre, at kommunens sikkerhedsniveau bliver fastholdt ved serviceleverandørens behandling af persondata

Sikkerhedsniveau

Hillerød Kommunes informationssikkerhedspolitik skal til enhver tid beskytte kommunens informationer i forhold til fortrolighed, tilgængelighed samt integritet på et acceptabelt sikkerhedsniveau. Sikkerhedsniveauet bliver fastlagt på baggrund af en risiko- og konsekvensvurdering ud fra vigtigheden af informationerne for kommunens virke, type af informationer, samt økonomi.

Organisering og ansvar

Informationssikkerhed er **byrådets** ansvar og informationssikkerhedspolitikken vedtages af byrådet. Byrådet delegerer ansvaret for at administrere og implementere informationssikkerheden til kommunaldirektøren**.**

Kommunaldirektøren er øverste sikkerhedsansvarlig med ansvar for den overordnede styring af informationssikkerhedsindsatsen, samt sikre den fornødne prioritering og ressourcetildeling. Kommunaldirektøren kan delegere dele af opgaven til en eller flere i organisationen – ansvaret kan ikke delegeres.

Afdelingschefer skal sikre, at kommunens gældende informationssikkerhedsregler og procedurer bliver implementeret og forvaltet korrekt i afdelingens procedure og daglige arbejde, herunder behandling af persondata i henhold GDPR og Databeskyttelsesloven. Afdelingschefer er systemejer for de enkelte it-systemer.

Systemejeren er ansvarlig for it-systemet og dets data. Dette medfører at systemejer er ansvarlig for:

- driftsafvikling, vedligeholdelse, IT-serviceleverandør (databehandlere), samt anskaffelse og afvikling af it-systemet.
- at it-systemet, understøtter kommunens informationssikkerhedsregler, -procedure og gældende lovgivning, herunder GDPR og databeskyttelsesloven.
- at sikre at udarbejdes vejledning og procedure til systemets brugere, så systemet anvendes på korrekt vis, samt at føre kontrol og tilsyn med brugerne.

Systemejer kan uddelegere opgaven – men ikke ansvaret – til en leder eller medarbejder.

I det tilfælde hvor to eller flere afdelinger anvender det samme it-system, sikre kommunaldirektøren at der udpeges en systemejer. Hvor systemejer og afdelingschef ikke er den samme person, er afdelingschefen ansvarlig for at afdelings medarbejdere efterlever systemejerens vejledning og procedure for anvendelse af it-systemet.

Alle **medarbejder**e i Hillerød Kommune har et personligt ansvar for, at informationssikkerhedspolitikken og dertil hørende regler og procedure bliver fulgt i forbindelse med udførelse af deres arbejdsopgaver og deres behandling af informationer.

Informationssikkerhedsudvalget er ansvarlig for at udarbejde, revidere og godkende kommunens informationssikkerhedsregler og procedure. Informationssikkerhedsudvalget orienteres af Digitalisering og IKT-drift om aktuelle problematikker, informationssikkerhedstiltag og træffer beslutninger herom.

Databeskyttelsesrådgivere (DPO) skal bl.a. understøtte og rådgive kommunen i databeskyttelsesforordningen samt føre kontrol i overholdelsen heraf. Borgerne kan desuden rette henvendelse til DPO vedr. spørgsmål om kommunens behandling af persondata. DPO skal rapportere herom en gang årligt til byrådet.

Informationssikkerhedsbevidsthed

Ledere og medarbejdere har et fælles ansvar for at beskytte kommunens informationer mod uautoriseret adgang, ændring, ødelæggelse og tyveri. Den nødvendige viden og kompetence omkring informationssikkerhed kommunikeres til alle medarbejdere og der bliver løbende arbejdet med holdninger og viden omkring informationssikkerhed. Alle medarbejdere skal derfor løbende have uddannelse i informationssikkerhed i relevant omfang. Information om regler og procedure vedr. informationssikkerhed findes på kommunens Intranet.

Brud på informationssikkerheden

Alle medarbejdere i Hillerød Kommune er forpligtiget til at efterleve den til enhver tid gældende informationssikkerhedspolitik, -regler og –procedurer. Kommunens intranet er opdateret med regler og procedure for, hvorledes medarbejderne skal forholde sig i tilfælde af overtrædelse (hændeligt som bevist) af kommunens informationssikkerhed.

Afvigelser
Hvis der opstår situationer, hvor kravene i informationssikkerhedspolitikken, regler eller procedure ikke kan efterleves, skal der skriftligt anmodes om dispensation af Lederen af Digitalisering og IKT. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikkerhedsforanstaltninger. Der kan ikke dispenseret for lovgivningen som f.eks. Databeskyttelsesforordningen (GDPR).

Opfølgning
Informationssikkerhedsudvalget revurderer Informationssikkerhedspolitikken minimum hvert 4. år og altid ved væsentlige ændringer i kommunen eller omverdenen.

Offentliggørelse
Informationssikkerhedspolitikken er tilgængelig på kommunens hjemmeside og intranet. Øvrige Informationssikkerhedsregler og -procedure er intern forbeholdt kommunens medarbejdere.

Hillerød Kommunes informationssikkerhedspolitik er godkendt af Hillerød Byråd den 25.09.2019.