Greve Kommune

Informations-sikkerhedspolitik

Informationssikkerhedspolitikken beskriver hvordan Greve Kommune håndterer IT-sikkerhed i det daglige arbejde.

Version 2.1

Greve Kommune

Indhold

Indledning

Der er i dag et øget krav til digitalisering af det danske samfund. Derfor anvender Greve Kommune i dag også IT på de fleste områder for at leve op til de krav som borgere, samfundet og lovgivningen stiller til en moderne og effektiv administration, samt en hurtig og korrekt service.

Derfor behandler kommunens medarbejdere hver dag mange oplysninger om borgere og virksomheder, og det er essentielt for tilliden til kommunen, at vi til stadighed opretholder en sikkerhedsindsats som sikrer at borgere og virksomheder kan føle sig trygge ved at overlade informationer til kommunen.

Formålet med informationssikkerhedspolitikken er at fastlægge de overordnede principper for kommunens informationssikkerhed, således at data, informationer og informationssystemer beskyttes bedst muligt under hensyntagen til den aktuelle vurdering af risici. Informationssikkerhedspolitikken er udmøntet i operative sikkerhedsbestemmelser, procedurer og vejledninger, som er samlet i en informationssikkerhedshåndbog.

Informationssikkerhedspolitikken fungerer i sammenhæng med kommunens øvrige centrale politikker og retningslinjer.

Holdninger og principper

Greve Kommunes Informationssikkerhedspolitik bygger på fire grundlæggende principper:

1. **Kommunens borgere skal have adgang til en stabil og korrekt kommunal service**

   Greve Kommune vil servicere kommunens borgere og samarbejdspartnere på bedst mulig måde. Politikken har som mål at sikre en tilgængelighed og pålidelighed i kommunens IT-anvendelse, således at IT-anvendelsen understøtter en korrekt og effektiv digital forvaltning.

2. **Fortrolighed i forvaltningen og respekt for borgernes data**

   Vi vil i vores IT-anvendelse sikre, at behandlingen af data og informationer sker med den fornødne fortrolighed i overensstemmelse med god offentlig forvaltningsskik og efter gældende databeskyttelsesregler.

3. **Forebyggende sikkerhed**

   Informationssikkerheden implementeres gennem forebyggende tiltag og aktiviteter således at medarbejderne i kommunen, i størst muligt omfang, kan fokusere på service til borgerne i stedet for at rette op på sikkerhedsbrud.

4. **Informationssikkerhed via viden**

   Informationssikkerheden skal etableres og fastholdes gennem krav til brugeradfærd, samt en målrettet formidling af viden om sikkerhed til de medarbejdere og eksterne parter, der har kontakt med de kommunale IT-ressourcer.

   Det er Greve Kommunes politik, at informationssikkerhed bygger på tillid, sund fornuft og ansvarlighed hos kommunens medarbejdere og mindre på kontrol, overvågning og mistanke. Kommunen ønsker derfor også, at informationssikkerhedspolitikken fungerer adfærdsregulerende snarere end kontrollerende over for de ansatte.

   Det forventes at ledere på alle niveauer påtager sig et aktivt ansvar for at udmønte informationssikkerhed i alle kommunens opgaver, og at lederne understøtter og motiverer medarbejderne i at arbejde efter principperne i informationssikkerhedspolitikken.

Sikkerhedsniveau

Ved udarbejdelsen af Greve Kommunes konkrete informationssikkerhedsindsatser og procedureniveauer, tages der udgangspunkt i værktøjer og referencerammer, som beskrevet ISO 27001/27002:2017.

Ved fastlæggelsen af de givne sikkerhedsniveauer tages udgangspunkt i risikovurderinger der indbefatter kommunens konkrete og aktuelle behandlingsaktiviteter og aktuelle trusselsbilleder, samt gældende lovgivning.

Kommunens sikringsforanstaltninger kan rettes mod alle former for eksternt og internt identificerede trusler, hændelige fejl og uheld samt bevidst skadevoldende handlinger og misbrug. Gennem sikkerhedsindsatserne skal det sikres, at it-driftssikkerheden og brug af it-løsninger kan ske så effektivt som muligt, samtidigt med at konsekvenserne ved sikkerheds-brud reduceres til et acceptabelt niveau.

Informationssikkerheden fastlægges dels ud fra en afvejning af behovet for et tilstrækkelig højt sikkerhedsniveau, dels ud fra hensynet til enkle og smidige arbejdsgange. Kommunen har en målsætning om, at informationssikkerhedsindsatser er tilpasset de værdier og informationer, som skal beskyttes, samtidig med at det sikres at borgere, virksomheder og samarbejdspartnere kan være trygge ved kommunens håndtering af data - og at gældende lovgivning altid overholdes.

Organisation og ansvar

Kommunens Informationssikkerhedsudvalg (ISU) udarbejder informationssikkerhedspolitikken og kommunale retningslinjer, centrale indsatser og fastlægger gældende sikkerhedsniveau. Byrådet godkender informationssikkerhedspolitikken.

Kommunens informations-sikkerhedsgruppe (ISG) indstiller forslag til informationssikkerhedsudvalget, koordinerer og udmønter informations-sikkerhedsindsatser. Alle centre er repræsenteret i informations-sikkerhedsgruppen. Informationssikkerhedskoordinatoren er ansvarlig for at koordinere arbejdet i informationssikkerhedsgruppen.

Kommunaldirektøren er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Kommunaldirektøren er endvidere formand for kommunens informationssikkerhedsudvalg.

Ledelsen på alle niveauer er ansvarlig for, at informationssikkerheden overholdes og at der implementeres procedurer der skal sikre overholdelse af politikken.

Medarbejdere, samarbejdspartnere, institutioner og leverandører med fysisk eller logisk adgang til kommunens IT-systemer skal være bekendt med informationssikkerhedspolitikken og skal forpligte sig til at overholde reglerne, der følger af den.

Nye medarbejdere skal ved ansættelsen introduceres til de gældende IT-sikkerhedskrav, samt informeres om den forventede adfærd i relation til IT-anvendelsen.

Udmøntning og opfølgning

Informationssikkerhedspolitikken er omsat til operative sikkerhedsbestemmelser, procedurer og vejledninger, som er samlet i en informationssikkerhedshåndbog.

Informationssikkerhedspolitikken revurderes som led i den overordnede sikkerhedsstyring mindst én gang årligt, og altid ved større ændringer der måtte følge af nye strategier eller lovgivning, af informationssikkerhedsudvalget.

Der skal løbende gennemføres informationstiltag over for kommunens medarbejdere for at sikre et fornødent kendskab til politikken, ligesom nye medarbejdere ved ansættelsen skal informeres om de væsentligste IT-sikkerhedskrav og den forventede adfærd i relation til informationer og systemer i kommunen.

Gyldighed og omfang

Kommunens informationssikkerhedspolitik er gældende for alle, uden undtagelse, som har adgang til kommunens systemer, data eller informationer. Informationssikkerhedspolitikken gælder derfor på alle kommunens institutioner og centre mv, hvor der pågår behandling af borgernes og virksomhedernes data.

Sikkerhedspolitikken gælder tillige for byrådspolitikere (når de handler i deres hverv som politikere) og eksterne parter, ledere og medarbejdere, der fra eksterne lokaliteter ad elektronisk vej etablerer forbindelse til kommunens systemer og data.

For leverandører, som har adgang til kommunens systemer, gælder det, at de skal have defineret og implementeret et sikkerhedsniveau, der mindst svarer til kommunens sikkerhedsniveau. Kommunen skal føre tilsyn med, at leverandører, herunder outsourcing leverandører, facility management centre og lignende, reelt lever op til det påkrævede sikkerhedsniveau.

Endvidere indgås der databehandleraftaler med leverandører af it-systemer, og andre leverandører af tjenesteydelser, som indebærer behandling af følsomme eller almindelige personoplysninger. Via databehandleraftalerne instruerer Greve Kommune, som dataansvarlig, databehandleren i at behandle persondata på en måde der lever op til Greve Kommunes informationssikkerhedskrav.

Overtrædelse af sikkerhedskrav

Bevidst eller ubevidst brud på informationssikkerheden i Greve Kommune kan medføre alvorlige konsekvenser for borgere og virksomheder, økonomiske tab, ansvarspådragelse, bødestraf og at tilliden til Greve Kommune forringes.

Forudsætningen for at have et velfungerende sikkerheds-setup er kommunens evne til at kunne reagere rettidigt på risici og trusler imod informationssikkerheden. Hvis medarbejdere i Greve Kommune opdager en trussel mod, eller brud på, informations-sikkerheden, skal dette straks meddeles til de sikkerhedsansvarlige, som vurderer hvilke handlinger der bør igangsættes. Det er Greve Kommunes politik, at medarbejdere altid skal kunne stå frem og anmelde sikkerhedsbrud, gøre opmærksom på uhensigtsmæssigheder mv. Derfor skal sikkerhedsbrud og hændelser behandles resolut iht. procedurer, registreres og have et proaktivt læringsperspektiv for øje.

Medarbejdere der, bevidst eller ubevidst, peger på uhensigtsmæssigheder i arbejdsgange, systemer eller infrastruktur skal betragtes som nogle af kommunens vigtigste sikkerhedsaktiver.

Samtidig forventes det naturligvis at medarbejdere, i det daglige arbejde, overholder gældende informationssikkerhedspolitik, og øvrige retningslinjer og procedurer for informationssikkerhed. Forsætlige, eller groft uagtsomme, overtrædelser af kommunens sikkerhedskrav vil i alvorlige tilfælde kunne medføre ansættelsesmæssige konsekvenser eller andre sanktioner i henhold til gældende lovgivning.

Udarbejdelse og ikrafttrædelse

- Informationssikkerhedspolitikken indstilles af Informationssikkerhedsudvalget og godkendes af Byrådet

- Kommunale retningslinjer der vedrører informationssikkerhedsområdet udformes af Informationssikkerhedsgruppen (ISG) og godkendes af Informationssikkerhedsudvalget (ISU)

- Instrukser og lokale procedurer, der vedrører Informationssikkerhedsområdet, udarbejdes på centerniveau

Dato	Redigeret af	Version og Ændring
Feb. 2016	Lene Elberg	Version 1.0 Vedtaget af kommunalbestyrelsen
Jan. 2018	Lene Elberg	Ver 1.97 som afspejler GDPR lovgivning
07. feb 2018	Pernille Vestergaard	Ver. 1.97.1 Figur indsat efter ønske fra informationssikkerhedsudvalget
09. feb 2018	Pernille Vestergaard	Ver. 1.97.2 Designmæssige ændringer
16.marts 2022	Jaco Hansen	Version 2.0 Ny fuldt revideret version (design og indhold) af informationssikkerhedspolitik godkendt i Informationssikkerhedsudvalg
25.maj 2022	Jaco Hansen	Version 2.1 Ændringer af godkendelsesprocedure
17. juni 2022	Jaco Hansen	Version 2.1 Tilrettelser af sproglig karakter
08.juli 2022	Jaco Hansen	Version 2.1 Til forelæggelse for Byråd
11.december 2023	Dieter Carstensen	Version 2.1 Til årlig godkendelse for Informationssikkerhedsudvalget (Godkendt af ISU 11.12.2023)