Greve Kommune

Informationssikker-hedspolitik

Indhold

Informationssikkerhedspolitik

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.

Informationssikkerhedspolitikken skal medvirke til at sikre borgernes retssikkerhed, samt medvirke til at minimere risikoen for at oplysninger om borgere falder i forkerte hænder eller misbruges og sikre at den kommunale sagsbehandling foregår effektivt og ud fra valide data.

Sikkerhedspolitikken skal også hjælpe den enkelte medarbejder i dennes dagligdag, således at utilsigtede sikkerhedsmæssige hændelse kan minimeres eller helt undgås.

Sikkerhedsniveau

Ved udarbejdelsen af Greve Kommunes informationssikkerhedspolitik, er der taget udgangspunkt i god IT-skik, ”best practice” samt gældende lovgivning. Der er endvidere anvendt værktøjer og referencerammer, som beskrevet ISO 27001/27002:2013.

Sikkerhedsniveauet er fastlagt på baggrund af en risikovurdering, således at informationssikkerheden afspejler kritikalitet og klassifikation af data og systemer. Som udgangspunkt er det hensigten, at sikkerheden skal være på et sådant niveau, at det sikres den følger gældende lovgivning og anses for at være betryggende.

I forbindelse med fastlæggelsen af sikkerhedsniveauet er der taget udgangspunkt i følgende fire sikkerhedsmæssige begreber:

Fortrolighed: omfatter en sikring af, at information kun er tilgængelig for personer, som er berettigede hertil.

Integritet: omfatter sikring af, at systemer og data er korrekte og fuldstændige.

Tilgængelighed: omfatter sikring af nødvendig tilgang til systemer og data.

Ægthed: også kaldet autenticitet, omfatter en sikring af, at kommunikerende parter har vished for, hvem den anden part er.

Disse begreber er anvendt som værktøj i forbindelse med afdækning af risici i samarbejde med kommunens system- og dataejere og den efterfølgende fastlæggelsen af et ledelsesmæssigt godkendt sikkerhedsniveau.

Der gennemføres opfølgning på risikovurderingen mindst en gang om året – eller ved større tekniske eller organisatoriske ændringer, således at ledelsen kan holdes orienteret om det aktuelle risikobillede. Endvidere fungerer risikovurderingen i forhold til at ændre og tilrette de aktuelle procedurer, retningslinjer og audits, således at man opretholder det sikkerhedsniveau ledelsen har valgt.

For at følge op på at sikkerhedsniveauet er, hvor man fra ledelsen ønsker det skal være, vil der løbende blive gennemført opfølgning og audit på kommunes informationssikkerhed. Det skal sikre, at den fornødne dokumentation findes, men også at den følges i praksis. Ligeledes skal audit afdække eventuelle sikkerhedsbrud.

Resultatet af disse audits vil indgå i en samlet årlig afrapportering til direktionen.

Holdninger og principper

Greve Kommune informationssikkerhed politik skal ses som en afvejning af de ofte modstridende hensyn, ønsket om høj sikkerhed, hensynet til brugervenlig i IT-anvendelse, og omkostningerne ved investeringer i sikkerhed.

Herudover implementeres informationssikkerheden i overensstemmelse med følgende overordnede holdninger og principper:

Troværdigheden på sikkerhedsområdet over for omverdenen herunder borgere og samarbejdspartnere må ikke berettiget kunne drages i tvivl.

Sikkerhedsforanstaltninger skal søges tilrettelagt, så de opleves som en naturlig del af medarbejdernes daglige arbejde og ikke som en barriere.

Sikkerheden søges styret i overensstemmelse med almindelig anerkendte metoder og procedurer for datasikkerhed.

Udgifter til at tilvejebringe sikkerhed skal afvejes mod de udgifter, der er forbundet med mulige sikkerhedsbrud.

Såfremt borgere eller samarbejdspartnere berøres af sikkerhedshændelser, vil vi så hurtigt, konkret og præcist, som det er muligt, informere Datatilsynet og de registrerede som er berørt af sikkerhedsbristen. Kommunen vil søge at begrænse eventuelle skader mest muligt.

Hovedmålsætninger i Informationspolitikken

For at konkretisere ovennævnte principper, er der opstillet følgende 4 hovedmålsætninger i arbejdet med informationssikkerhed.

Sikre kommunens borgere adgang til en stabil og korrekt kommunal service

- Greve Kommune vil servicere kommunens borger og samarbejdspartnere på bedst mulige måde. Sikkerhedspolitikken har som mål at sikre en tilgængelighed og pålidelighed i kommunens IT-anvendelse, således at IT-anvendelsen understøtter en korrekt og effektiv digital forvaltning. Herigennem kan kommunen opnå og bibeholde et godt image over for kommunens borgere og offentligheden som helhed.

Fortrolighed i forvaltningen

- Vi vil i vores IT-anvendelse sikre, at behandlingen af data og informationer sker med fortrolighed og i overensstemmelse med god offentlig forvaltningsskik. Sikkerhedspolitikken skal derfor medvirke til, at informationer om borgerne holdes fortroligt for uvedkommende.

Forebyggende sikkerhed

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

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.

Gyldighed og omfang

Kommunens informationssikkerhedspolitik er gældende for alle uden undtagelse som har adgang til kommunens systemer, data eller informationer. Informationssikkerhedspolitikken skal derfor anvendes på alle kommunens institutioner og centre mv, hvor de foregår anvendelse og bearbejdning af borgernes og virksomhedernes data.

Sikkerhedspolitikken gælder tillige for byrådspolitikere og eksterne parter, ledere og medarbejdere, der fra eksterne lokaliteter (f.eks. supplerende IT-arbejdspladser i hjemmet eller andre lokaliteter uden for kommunen) 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 fører tilsyn med, at leverandører, herunder outsourcing leverandører, facility management centre o.l. reelt lever op til det påkrævede sikkerhedsniveau.

Endvidere gælder, at der vil blive indgået databehandleraftaler med leverandører af it-systemer og andre leverandører af tjenesteydelser som indebærer behandling af følsomme eller almindelige persondata. Via databehandleraftalerne regulere Greve kommune, som dataansvarlig myndighed hvilke data og behandling aktiviteter en leverandør må foretage på vegne af Greve Kommune.

Der vil blive udarbejdet tilrettede retningslinjer for de kommunale skolers undervisningsnet, offentlig tilgængelige IT systemer på bibliotekerne samt Borgerservice. Det vil løbende blive vurderet, om der skal implementeres særlige retningslinjer sikkerhedsmæssigt på andre områder, hvor risikoprofilen er anderledes i forhold til resten af kommunen.

Organisation og ansvar

Byrådet har det overordnede ansvar for informationssikkerhedspolitikken, og herunder fastlæggelse af de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger for overholdelse af sikkerhedsbestemmelser mm.

Kommunalbestyrelsen godkender sikkerhedspolitikken og skal have en årlig redegørelse for sikkerhedsarbejdet i kommunen.

Kommunaldirektøren er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.

Ledelsen på alle niveauer er ansvarlig for, at informationssikkerheden overholdes.

Informationssikkerhedskoordinatoren er ansvarlig for implementering og vedligeholdelse af Informationssikkerhedssystemet (ISMS), samt den generelle kontrol af sikkerhedsniveauet i kommunen.

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

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

Der er endvidere nedsat et informationssikkerhedsudvalg, som sikre den ledelsesmæssige forankring af sikkerhedsarbejdet.

Sikkerhedsdokumentation og dokumenthåndtering

Greve Kommunes informationssikkerhedspolitik beskriver vigtigheden af arbejdet med informationssikkerhed i kommunen og fastlægger det overordnede sikkerhedsniveau.

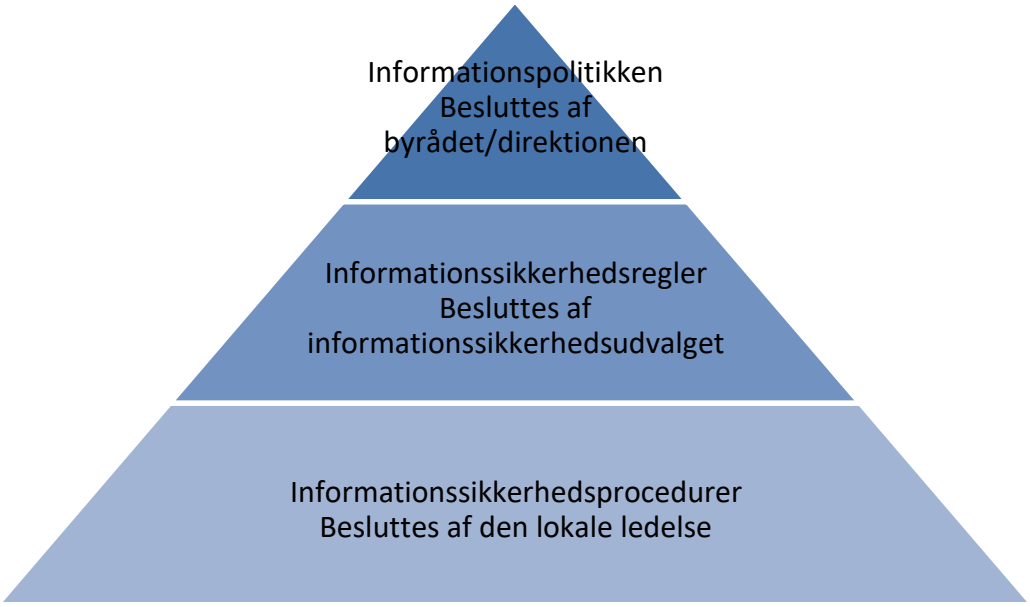
Informationssikkerhedspolitikken indeholder derfor de overordnede sikkerhedsmålsætninger og danner grundlag for udformningen af underliggende forretningsgange, retningslinjer og instrukser på informationssikkerhedsområdet.

Endvidere er informationssikkerhedspolitikken og de herudfra fastsatte retningslinjer grundlaget for det daglige sikkerhedsarbejde, inkl. de sikkerhedsadministrative opgaver.

Medarbejdere i kommunen med adgang til administrative systemer og data skal som nævnt i hovedmålsætningen have kendskab til sikkerhedspolitikken og de retningslinjer, der er relevante for deres arbejde i kommunen, herunder særlige IT-rettede funktioner.

Implementeringen af politik og retningslinjer kan medføre, at der udarbejdes underliggende procedurer, der på instruksniveau beskriver medarbejderens konkrete arbejdsopgaver.

Informationssikkerhedspolitikken og underliggende retningslinjer, arbejdsprocesser og instrukser retningslinjer skal være tilgængelige på kommunens intranet.



Overtrædelse af sikkerhedspolitikken og –retningslinjer

Bevidst eller ubevidst overtrædelse af sikkerhedsbestemmelserne kan medføre, at kommunens brugere, samarbejdspartnere, borgere mv. oplever ustabilitet, uregelmæssigheder og uhensigtsmæssigheder i anvendelse og bearbejdning af kommunens informationer. Dette kan medføre, dels økonomiske tab og dels forringelse af den kommunale service og kommunens image.

Overtrædelser af sikkerhedspolitikken håndteres af den nærmeste leder, for eksempel i form af kontakt til de involverede medarbejdere, med henblik på en nærmere afdækning af hændelsesforløb, baggrund og karakteren af overtrædelsen.

I alvorlige eller generelle tilfælde skal sagen behandles i direktionen. Overtrædelse af sikkerhedspolitikken kan få ansættelsesmæssige konsekvenser eller andre sanktioner.

Udarbejdelse og ikrafttrædelse

Håndteringen af ændringer i sikkerhedsdokumentationen foretages på følgende måde:

- Informationssikkerhedspolitikken: Godkendes af direktionen/byrådet.
- Retningslinjer: Godkendes af informationssikkerhedsudvalget.
- Instrukser: Kan fortages af den lokale ledelse under hensyntagen til de gældende retningslinjer

Informationssikkerhedspolitikken er godkendt af byrådet d. 19. marts og træder i kraft den 1 maj 2018.

Dato	*Redigeret af*	*Version og Ændring*
19-08 -15	Lene Elberg	Ver. 0.5 første udkast – afklaring af format, indhold og omfang
23-09 -15	Lene Elberg	Ver 0.8 udkast med rettelse og afklaring, og som informationssikkerhedspolitik
28-10 -15	Lene Elberg	Ver 1 med ind arbejdede kommentarer fra datasikkerhedsudvalgets møde
Feb. 2016	Lene Elberg	Vedtaget af kommunal bestyrelsen
Feb. 2017	Lene Elberg	Sikkerhedspolitik gennemgået på sikkerhedsudvalgsmødet
Jan. 2018	Lene Elberg	Udkast til ny version 1.95 som afspejler GDPR lovgivning
Jan. 2018	Lene Elberg	Ver 1.97 Endelig udkast sikkerhedspolitik efter høring og kommentarer (xx) skal erstattes med godkendelse dag
7. feb 18	Pernille Vestergaard	Ver. 1.97.1 Figur indsat efter ønske fra informationssikkerhedsudvalget
9. feb 18	Pernille Vestergaard	Ver. 1.97.2 Designmæssige ændringer