Greve Kommune

IT-sikkerhedspolitik

Indhold

1 Læsevejledning

Politikken er opdelt i 3 hovedafsnit:

1) Den overordnede sikkerhedspolitik, som beskriver de overordnede rammer og formål med Greve Kommunes sikkerhedspolitik.
2) Bilag 8.1a (IT-Sikkerhedspolitik – Retningslinjer) som er en beskrivelse af retningslinjerne for områderne politikken indeholder samt hvad der skal medtages i de konkrete instrukser.
3) Bilag 8.1b (IT-Sikkerhedspolitik – Instrukser) som konkret beskriver instrukserne ud fra rammer og krav beskrevet i Bilag 8.1a (IT-Sikkerhedspolitik – Retningslinjer).

I forhold til det fremadrettede arbejde, vil den overordnede sikkerhedspolitik være meget statisk i forhold til organisationen. Bilag 8.1a (IT-Sikkerhedspolitik – Retningslinjer) ændres i forhold til lovgivning og standarder. Bilag 8.1b (IT-Sikkerhedspolitik – Instrukser) ud fra konkret risikovurdering og trusselsbillede.

2 Informationssikkerhedspolitik

2.1 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 effektiv administration og til en hurtig og korrekt service.

For at sikre borgernes retssikkerhed er der udarbejdet en Informationssikkerhedspolitik, som skal medvirke til at minimere risikoen for at oplysninger om borgere falder i forkerte hænder eller misbruges, samt sikre at den kommunale sagsbehandling foregår hurtigt 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.

Greve Kommune har gennem tiden, i takt med udbygning af sin IT-anvendelse, haft en række retningslinjer og dokumenter omkring informationssikkerhed. Denne nye informations- sikkerhedspolitik er en præcisering og formalisering af disse eksisterende sikkerhedsmæssige retningslinjer, som er gældende i kommunen i dag.

Denne sikkerhedspolitik skal derfor ikke ses som en stramning af nuværende praksis, men derimod som en samling, dokumentation og præcisering af eksisterende retningslinjer, således at politikken kan håndtere nye problemstillinger. Den skal også fremadrettet, anvise metoder for auditering af sikkerheden.

2.2 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 i DS484:2005 samt 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.
- Pålidelighed: 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 systemejere og efterfølgende i forhold til ledelsen.

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

2.3 Holdninger og principper

Greve Kommune vil fastlægge sin politik 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 de berørte parter. Kommunen vil begrænse eventuelle skader mest muligt.

2.4 Hovedmålsætninger i informationssikkerhedspolitikken

For at konkretisere ovennævnte principper, er der opstillet følgende 7 hovedmålsætninger i arbejdet med informationssikkerhed.

2.4.1 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 borgerservice til tiden. Herigennem kan kommunen opnå og bibeholde et godt image over for kommunens borgere og offentligheden som helhed.

2.4.2 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.

2.4.3 FOREBYGGENDE SIKKERHED

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

2.4.4 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.

2.4.5 OVERHOLDELSE AF GÆLDENDE LOVGIVNING

Greve Kommune har over for borgerne et særligt ansvar for at beskytte oplysninger om personer mod uautoriseret anvendelse og mod fejl i oplysningerne. Sikkerhedsniveauet og IT-anvendelsen i Greve Kommune skal til hver en tid være i overensstemmelse med gældende lovgivning og kontraktuelle krav.

2.4.6 AFBALANCERET OG STYRET INFORMATIONSSIKKERHED

Informationssikkerheden er differentieret i forhold til de værdier og informationer, som skal beskyttes, og i forhold til et realistisk trusselsbillede. Sikkerhedsniveauet er derfor tilpasset disse faktorer og skal fastholdes igennem såvel tekniske som ikke-tekniske rammer. Dermed har såvel tekniske kontroller som organisationens og brugernes adfærd en væsentlig rolle i forhold til den samlede sikkerhed.

2.4.7 IKKE FUNKTIONALITETSBEGRÆNSENDE

Greve Kommune tilsigter, at anvendelsen af og funktionaliteten i kommunens IT-systemer ikke må forringes væsentligt som følge af sikkerhedsniveauet. Sikkerheden indgår i stedet som en integreret og ikke begrænsende del af arbejdsprocesserne i kommunen, hvad enten anvendelsen sker centralt på rådhuset, decentralt i de enkelte institutioner eller via hjemmearbejdspladser hos den enkelte medarbejder.

2.5 **Gyldighed og omfang**

Kommunens informationssikkerhedspolitik er gældende i alle af kommunens institutioner og centre, hvor der sker en anvendelse og bearbejdning af kommunens informationer. 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 niveau. Kommunen skal have mulighed for at sikre sig, at leverandører, herunder outsourcing leverandører, facility management centre o.l. reelt lever op til det påkrævede sikkerhedsniveau.

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.

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.

sikkerhedskrav, samt informeres om den forventede adfærd i relation til IT-anvendelsen.

Informationssikkerhedspolitikken skal uddybes med fornødne retningslinjer om konkrete anvendelsesområder og sikkerhedsforanstaltninger, herunder:

- Grundlæggende retningslinjer.
- Organisation og ansvar.
- Risikovurdering.
- Lovgivning.
- Klassifikation af data.
- Retningslinjer for fysisk og logisk sikkerhed.
- Fysisk sikkerhed.
- Logisk adgangskontrol til IT-ressourcer.
- Brugeradministration.
- Retningslinjer for drift og overvågning.
- Driftsafvikling og overvågning.
- Håndtering af sikkerhedsproblemer.
- Sikkerhedskopiering.
- Beskyttelse mod ondsindet programmel.
- Retningslinjer for håndtering af ændringer.
- Anskaffelse og udvikling.
- Håndtering af konfigurationsændringer.
- Øvrige retningslinjer.
- Samarbejdspartnere og leverandører.
- Beredskabsplanlægning.
- Medarbejdere.
- Logning og audit.

2.6 Ansvar for og godkendelse af sikkerhedspolitikken

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.

2.7 Sikkerhedsdokumentation og dokumenthåndtering

Informationssikkerhedspolitikken og de herudfra fastsatte retningslinjer er 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. Det skal til hver en tid være muligt for relevante medarbejdere at få adgang til retningslinjer og underliggende procedurer, hvis der måtte være brug for dette. Sikkerhedspolitikken og retningslinjer skal være tilgængelige på kommunens intranet.

2.8 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 daglige 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.

Informationssikkerhedsorganisationen skal indrettes således, at situationer med overtrædelse eller manglende overholdelse, samt forsøg på uautoriseret anvendelse, skal rapporteres til IT-chefen.