Informations-sikkerhedspolitik

Gentofte Kommune

2. februar 2026

Version 2.0

Indholdsfortegnelse

1 Indledning

Gentofte Kommunes Kommunalbestyrelse fastlægger med denne politik kravene til informationssikkerhed i Gentofte Kommune.

Politikken omfatter såvel teknisk som manuel behandling af informationer, herunder informationer lagret på elektroniske medier, papir, bånd mv.

Politikken har sit afsæt i ISO27001, som er en international standard for styring af informationssikkerhed. ISO27001 udgør grundstenen for arbejdet med informationssikkerhed og er fundamentet til implementering af andre standarder og lovkrav inden for informationssikkerhed, herunder National Standard for Identiteters Sikringsniveauer (NSIS), EU's Net- og Informationssikkerhedsdirektiv nr. 2 (NIS2), tekniske minimumsstandarder i kommuner, Databeskyttelsesforordningen (GDPR), AI Act mv. Herved opnår organisationen en fokuseret, optimeret og sammenhængende indsats med ensartet håndtering af krav på tværs af organisationen.

1.1 Formål og målsætning

Informationssikkerhedspolitikken balancerer hensynet til driftssikkerhed på den ene side og muligheden for fortsat at udnytte digitaliseringsmulighederne til gavn for borgerne på den anden side.

Lovgivningen stiller en række specifikke krav til beskyttelse af personoplysninger og borgernes mulighed for at få indsigt i, hvad egne data anvendes til. Det betyder blandt andet, at kommunen skal beskrive uddybende bestemmelser for informationssikkerhed, hvilket håndteres inden for rammerne af informationssikkerhedspolitikken.

Politikken beskriver principperne for styring af informationssikkerhed i kommunen og, på overordnet niveau, de fysiske, tekniske og administrative processer, der beskytter fortrolighed, integritet og tilgængelighed af informationer. For en række processer og aktiver udarbejdes underliggende retningslinjer, som beskriver håndtering af konkrete risici.

1.2 Gyldighedsområde

Politikken er gældende for hele Gentofte Kommune. Alle informationer og informationsaktiver (data, informationer, systemer, netværk, it-udstyr mv.), som er i kommunens varetægt og som anvendes i kommunen, er omfattet.

1.3 Godkendelse

Politikken er en del af kommunens styringsgrundlag og godkendes af Kommunalbestyrelsen.

1.4 Styring og ledelse af informationssikkerhed

Gentofte Kommune arbejder med informationssikkerhed på flere niveauer, som illustreret ved nedenstående oversigt:

<table>
<tr><td colspan="3">Informationssikkerhedspolitik</td></tr>
<tr><td colspan="3">Ledelsessystem for informationssikkerhed (ISMS)</td></tr>
<tr><td>IT-retningslinjer for ledere</td><td>IT-retningslinjer for medarbejdere</td><td>IT-retningslinjer for leverandører</td></tr>
<tr><td colspan="3">Fælles processer og (kontrol)foranstaltninger</td></tr>
<tr><td colspan="3">Afdelingsspecifikke processer og (kontrol)foranstaltninger</td></tr>
</table>

Informationssikkerhedspolitik (dette dokument) beskriver rammer, mål, processer og overordnet organisering af informationssikkerhedsindsatsen og godkendes i Kommunalbestyrelsen.

Ledelsessystem for informationssikkerhed (ISMS) (tidligere kaldet de operationelle bestemmelser) konkretiserer, hvordan informationssikkerhedspolitikken implementeres i praksis gennem beskrivelse af processer, kontroller, ansvar og roller. ISMS'et godkendes af direktionen. ISMS'et er opbygget efter ISO 27001-standarden og dokumenterer, hvordan kommunen efterlever de nødvendige sikkerhedskrav gennem konkrete kontrolforanstaltninger og procedurer.

Retningslinjerne beskriver, hvordan man i den pågældende rolle skal forholde sig til informationssikkerhed i sit arbejde. Formålet med retningslinjerne er at forebygge at personoplysninger og forretningskritiske oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes eller kommer til uvedkommendes kendskab, misbruges eller behandles i strid med den lovgivning, der gælder for kommunerne. Retningslinjer godkendes af Informationssikkerhedsforum med inddragelse af opgaveområder og interessenter.

Fælles processer og (kontrol)foranstaltninger omfatter de centraliserede processer, herunder indkøb, projektstyring, rekruttering og IT-drift samt håndbog for system- og dataejere. Her udarbejdes som hovedregel ikke særskilte sikkerhedsbeskrivelser af processer, men hvor der findes beskrivelser af processer og foranstaltninger indarbejdes sikkerhedskravene i disse. Konkrete sikkerhedsprocesser og sikkerhedsforanstaltninger samt kontrolforanstaltninger dokumenteres.

Afdelingsspecifikke processer og (kontrol)foranstaltninger omfatter de processer og kontrolforanstaltninger, der ikke kan centraliseres på grund af særlige faglige eller tekniske forhold i afdelingen. Dette kan eksempelvis omfatte skoleelevers anvendelse af IT-udstyr, særlige adgangskrav i institutioner, eller håndtering af specialiserede fagsystemer. Den lokale leder har ansvaret for at fastlægge afdelingsspecifikke foranstaltninger i samarbejde med IT og informationssikkerhed.

2 Politik

2.1 Generelle krav

Der skal etableres en systematisk styring og koordinering af sikkerhed samt for identifikation og håndtering af risici og trusler, som opfylder følgende krav:

- Kontinuerlig identifikation af risici, trusler og sårbarheder
- Kontinuerlig vurdering af sikkerhedshændelser, alarmer og identificerede risici, trusler og sårbarheder i forhold til deres betydning for borgerne, opgavevaretagelsen og overholdelse af lovkrav.
- Identifikation og implementering af foranstaltninger, som minimerer sandsynlighed og konsekvens ved sikkerhedsbrud og som eliminerer uacceptable risici.

2.2 Styring af sikkerhedskrav

2.2.1 Risikovurdering

Der skal foretages løbende risikovurderinger, som identificerer trusler og sårbarheder i IT-systemer, behandlingsaktiviteter samt i øvrige identificerede scenarier. Der skal foretages opfølgende risikovurderinger med passende mellemrum, der sikrer, at kommunens risikovurdering ifm. behandling af persondata er ajourført.

De nærmere krav hertil fastsættes i ledelsessystem for informationssikkerhed (ISMS), der godkendes af direktionen.

2.2.2 Klassifikation

Data skal klassificeres efter konsekvenserne ved brud på fortrolighed, integritet og tilgængelighed. Beskyttelsesniveauet skal fastsættes i overensstemmelse med klassifikationen.

IT-systemer og IT-services skal klassificeres efter konsekvenserne ved brud på fortrolighed, integritet og tilgængelighed. Sikkerhedsniveauet skal tilpasses klassifikationen.

Leverandører skal klassificeres efter deres kritikalitet for kommunens informationssikkerhed samt deres potentielle indvirkning på fortrolighed, integritet og tilgængelighed. Leverandørstyringen skal tilpasses niveauet.

2.2.3 Overvågning af informationsservices

Kritiske informationsservices (systemer, netværk, opbevaring af data, arkiver mv.) skal kontinuerligt overvåges. Overvågningen skal beskyttes mod manipulation og utilsigtede afbrydelser af adgang.

2.2.4 Kontroller

Der skal foretages regelmæssige kontroller til sikring af, at kritiske it-services og foranstaltninger virker som forudsat. Hyppigheden af kontroller skal tilpasses risikoen. Kontroller skal dokumenteres.

De nærmere krav til kontroller og fastlæggelse af, hvem der udfører denne, skal fastsættes i kommunens ledelsessystem for informationssikkerhed (ISMS), der godkendes af direktionen.

2.3 Roller og ansvar

Den enkelte medarbejders ansvar og afdelingernes ansvar skal være præcist og entydigt beskrevet med udgangspunkt i nedenstående overordnede organisering:

- Alle medarbejdere har pligt til at sætte sig ind i Gentofte Kommunes informationssikkerhedspolitik og skal efterleve de til enhver tid gældende IT-retningslinjer for medarbejdere. IT-retningslinjerne underskrives digitalt ved ansættelse.

- Alle personaleledere har ansvar for, at kravene til system- og datasikkerhed i lederens ansvarsområde er klart kommunikeret til medarbejderne, og at medarbejderne overholder kravene, ligesom lederen selv skal være bekendt med, og overholde, kravene til informationssikkerhed, herunder efterleve gældende IT-retningslinjer for ledere.

- Afdelingschefer har ansvar for, indenfor eget opgaveområde, at informationssikkerheden implementeres og anvendes korrekt, samt at der i nødvendigt omfang bliver udarbejdet afdelingsspecifikke procedurebeskrivelser, arbejdsgangsbeskrivelser, instrukser mv.

- Databeskyttelsesrådgiveren (DPO) varetager de opgaver, der påhviler denne iht. EU-databeskyttelsesforordningens artikel 39.

- Informationssikkerhedsforum består af Økonomi- og Digitaliseringsdirektør som formand samt repræsentanter for organisationens fagområder. Forummet har ansvaret for styring af informationssikkerheden i samarbejde med den tværgående informationssikkerhedskoordinator. Forummet sætter mål for informationssikkerheden, der er afstemt efter kommunens valgte strategi og risikoniveau og sørger for at informationssikkerheden realiseres og efterleves i organisationen jf. kommunens ledelsessystem for informationssikkerhed (ISMS).

- Direktionen har det overordnede ansvar for informationssikkerheden og er ansvarlig for organisationens arbejde med informationssikkerhed på strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger.

- Kommunaldirektøren er øverste informationssikkerhedsansvarlige og godkender i samråd med direktionen ledelsessystem for informationssikkerhed (ISMS).

- Kommunalbestyrelsen godkender Informationssikkerhedspolitikken. De enkelte kommunalbestyrelsesmedlemmer er ligesom kommunens medarbejdere forpligtet til at følge kommunens informationssikkerhedspolitik i forbindelse med deres virke som kommunalbestyrelsesmedlemmer.

- Ekstern IT-revision - Kommunens håndtering af IT-området er underlagt en ekstern IT-revision, der årligt gennemgår de forskellige områder og udfærdiger en IT-revisionsrapport, der behandles i Direktionen.

For alle systemer udpeges på chefniveau, en **systemejer** med ansvar for sikkerheden omkring systemet.

For hvert system skal der desuden udpeges en **systemadministrator**, som har det tekniske ansvar for systemets drift, vedligeholdelse og konfiguration, herunder håndtering af adgangsstyring og sikkerhedsindstillinger.

For alle persondatabehandlinger udpeges på chefniveau, en **dataejer**, som har ansvaret for at sikre at behandlingen er lovmedholdelig.

Understøttende funktioner

- **JURA** - Kommunens juridiske kontor rådgiver organisationen om persondataretlige spørgsmål.

- **Digitalisering og IT** - Afdelingens opgaver omfatter drift, udvikling, support, styring og projektledelse samt informationssikkerhed. Her sikres, at "Den gode IT-anskaffelse" følges, herunder at der foretages en sikkerhedsmæssig vurdering og test af løsninger, kvalificering af kravspecifikation fsva IT-sikkerhed ved anskaffelse af nye systemer og programmer. Afdelingschefen har det overordnede ansvar for aktiviteterne i forbindelse med styring og ledelse af informationssikkerheden.

2.4 Sikkerhedskultur og -bevidsthed

Alle medarbejdere har pligt til at forholde sig til informationssikkerhed i deres daglige arbejde og til at træffe de nødvendige forholdsregler.

Ledere og medarbejdere skal holde sig ajour med de risici, der er relevante for deres rolle og opgaver.

Ledere på alle niveauer skal have overblik over risikoen i deres ansvarsområde og sikre løbende dialog med medarbejdere om risici og nødvendige sikkerhedsforanstaltninger.

2.4.1 Awareness

Der er etableret et awareness-program, som løbende arbejder med at udbrede kendskabet til kommunens informationssikkerhedspolitik samt de lovmæssige krav til informationssikkerhed, databeskyttelse og cybersikkerhed, herunder databeskyttelsesforordningen, databeskyttelsesloven, AI Act og NIS2-direktivet.

Programmet tilpasses løbende i forhold til det lokale og nationale trusselsbillede samt nye cybertrusler. Effekten af de gennemførte awareness-aktiviteter måles og indgår i den løbende udvikling af programmet.

Der fastsættes nærmere krav i ledelsessystem for informationssikkerhed (ISMS).

2.5 Sikker IT-drift

Der skal opretholdes et driftsmæssigt stabilt, sikkert, let tilgængeligt og funktionelt IT-serviceniveau. Opgaveområderne skal kunne stole på, at IT-services, der etableres og leveres af IT-afdelingen, er tilgængelige og beskyttet efter opgaveområdernes behov.

Sikkerhedsniveauet omkring de enkelte systemer og data fastlægges på baggrund af en risikovurdering og under hensyn til lovbestemte og kontraktlige krav, herunder krav i NIS2-direktivet, for kritiske systemer.

2.6 Adgang og rettigheder til data og systemer

Følsomme og kritiske systemer og data skal beskyttes mod uautoriseret adgang og ændring uanset, hvor de befinder sig. Adgang til og ændring af følsomme eller kritiske systemer eller data skal let kunne spores til personen, der foretog handlingen.

De ansvarlige ledere skal gives let adgang til oplysninger, der er nødvendige for at kunne udføre ledelsestilsyn.. Adgangskontrollens effektivitet skal efterprøves løbende for væsentlige og følsomme data og systemer.

Adgange til data skal minimeres og skal afspejle et aktuelt arbejdsbetinget behov. Kun en leder (eller en lederbemyndiget) kan anmode om ændrede rettigheder til sin medarbejder.

Der skal foretages stikprøver af anvendelse af adgange til personoplysninger. Omfanget af stikprøver skal tilpasses bredden af rettighederne og resultatet af tidligere stikprøver.

2.7 Projekter og indkøb

Digitaliseringsprojekter, herunder anskaffelse, udvikling og vedligeholdelse af IT-systemer skal udformes, så de sikrer et passende sikkerhedsniveau og forbedrer og forenkler kommunens opfyldelse af lovgivningens krav til sikring af de registreredes rettigheder.

Indkøb af IT-systemer og -tjenester skal omfatte sikkerhedskrav, der vurderes og dokumenteres som en del af leverandørvurderingen. Sikkerhedskravene skal fastlægges inden udbud og efterleves gennem hele kontraktperioden.

Projekter og ændringer skal følge en fast, dokumenteret projekt- og/eller ændringsstyringsproces. Sikkerhedsmæssig vurdering skal være en integreret del af projekt- og programstyringen, samt af udbudsprocessen.

Projekter, der har relation til behandling af personoplysninger, skal følge principperne for databeskyttelse gennem design og standardindstillinger.

2.8 Fysisk beskyttelse af data og systemer

De fysiske omgivelser for informationer og informationsudstyr, der anvendes af kommunen og som kommunen har ansvaret for, beskytter effektivt mod fysiske hændelser, eksempelvis brand, vandskade, tyveri, hærværk, skader forårsaget af menneskelige fejl mv.

På steder, hvor der opbevares og anvendes informationer, systemer, infrastruktur og data, skal der etableres et risikotilpasset niveau af fysisk sikkerhed. Placering og den fysiske sikring af udstyr, som IT-afdelingen har driftsansvaret for, skal forhåndsgodkendes af IT-afdelingen. Den fysiske sikkerhed på lokationer med vitale installationer og informationer, der kræver høj beskyttelse, skal løbende efterprøves.

2.9 Eksterne parter

Samarbejde med eksterne parter skal beskytte Gentofte Kommunes informationssikkerhed. Der skal foretages risikovurdering af samarbejdet, og sikkerhedskrav skal fastlægges og indarbejdes i kontrakter og aftaler.

Ved samarbejder med eksterne parter, hvor Gentofte Kommune og en partner i fællesskab fastlægger formål og hjælpemidler for behandling af personoplysninger (fælles dataansvar), skal der indgås en aftale om fælles dataansvar, som klart definerer og fordeler parternes ansvar, jf. GDPR artikel 26.

2.10 Håndtering af sikkerhedshændelser

Der skal opretholdes et beredskab, så sikkerhedshændelser kan håndteres effektivt. For kritiske IT-systemer omfattet af NIS2-direktivet skal der være etableret procedurer for håndtering af sikkerhedshændelser, herunder rapportering til relevante myndigheder inden for lovgivningens tidsfrister. Ved alvorlige hændelser skal der foretages en efterfølgende evaluering af hændelsen.

2.11 Evaluering

Afdelingschef for Digitalisering og IT leverer en årlig status til den politiske ledelse. Direktionen skal orienteres om alvorlige informationssikkerhedsbrud. Ved væsentlige personalerelaterede brud på sikkerheden involveres HR-chefen.

3 Ikrafttrædelse og ændringer

Informationssikkerhedspolitikken skal godkendes af Kommunalbestyrelsen hvert år.

Redigering foretages af afdelingschefen for Digitalisering og IT og godkendes på følgende måde:

1. Forslag til ændringer til denne Informationssikkerhedspolitik udformes i samarbejde med JURA og databeskyttelsesrådgiveren til godkendelse af Kommunalbestyrelsen.
2. Ændringer i ledelsessystemet for informationssikkerhed (ISMS) udarbejdes med inddragelse af databeskyttelsesrådgiveren (DPO). ISMS'et undergår en samlet gennemgang og godkendelse af direktionen hvert andet år.
3. Informationssikkerhedspolitikkernes forskellige IT-retningslinjer udarbejdes og ændres i samarbejde med berørte afdelinger, med inddragelse af databeskyttelsesrådgiveren og godkendes af Informationssikkerhedsforum.
4. Øvrige bilag omkring informationssikkerhedspolitikken er forankret i Informationssikkerhedsteamet, som forestår udarbejdelse og ændringer i samarbejde med berørte afdelinger. Ændringer forelægges Informationssikkerhedsforum.