

# Informations- sikkerhedspolitik



**Gentofte  
Kommune**

27. februar 2023  
Version 1.1

# Indholdsfortegnelse

1	Indledning.....	<b>3</b>
1.1	Formål og målsætning.....	3
1.2	Gyldighedsområde.....	3
1.3	Godkendelse.....	3
1.4	Gentofte Kommunes informationssikkerhedspakke.....	3
2	Politik.....	<b>4</b>
2.1	Generelle krav.....	4
2.2	Styring af sikkerhedskrav.....	4
2.2.1	Risikovurdering.....	4
2.2.2	Klassifikation.....	4
2.2.3	Overvågning af informationservices.....	4
2.2.4	Kontroller.....	4
2.3	Roller og ansvar.....	4
2.4	Sikkerhedskultur og -bevidsthed.....	5
2.4.1	Awareness.....	5
2.5	Sikker IT-drift.....	6
2.6	Adgang og rettigheder til data og systemer.....	6
2.7	Projekter og indkøb.....	6
2.8	Fysisk beskyttelse af data og systemer.....	6
2.9	Eksterne parter.....	6
2.10	Håndtering af sikkerhedshændelser.....	6
2.11	Evaluerings.....	7
3	Ikrafttrædelse og ændringer.....	<b>7</b>

# 1 Indledning

Gentofte Kommunes Kommunalbestyrelse fastlægger med denne politik kravene til informationssikkerhed i Gentofte Kommune. Politikken omfatter såvel IT-tekniske, som manuelle behandlinger 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, som eksempelvis National Standard for Identiteters Sikringsniveauer (NSIS), tekniske minimumsstandarder i kommuner, Databeskyttelses-forordningen (GDPR) mv. Herved opnår organisationen en fokuseret, optimeret og sammenhængende indsats med ensartet håndtering af samme 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 desuden 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.

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 kommunen. Alle informationer og informationsaktiver (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 Gentofte Kommunes informationssikkerhedspakke

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

Informationssikkerhedspolitik		
Operationelle Bestemmelser		
IT-retningslinjer for ledere	IT-retningslinjer for medarbejdere	IT-retningslinjer for leverandører
Fælles processer og (kontrol)foranstaltninger		
Afdelingsspecifikke processer og (kontrol)foranstaltninger		

**Informationssikkerhedspolitik** (dette dokument) beskriver rammer, mål, processer og overordnet organisering af informations-sikkerhedsindsatsen og godkendes i Kommunalbestyrelsen.

**De operationelle Bestemmelser** beskriver, hvordan indholdet af informationssikkerhedspolitikken organiseres og konkretiseres i forhold til drift, ansvar og roller. Disse godkendes af direktionen. De operationelle Bestemmelser tager afsæt i ISO27002, og beskriver hvordan det enkelte krav efterleves.

**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. Deciderede sikkerhedsprocesser og sikkerhedsforanstaltninger samt kontrolforanstaltninger dokumenteres.

**Afdelingsspecifikke processer og (kontrol)foranstaltninger** omfatter de processer, der ikke kan centraliseres på grund af særlige forhold eller behov. For eksempel skoleelevers anvendelse af skolens IT og eget IT-udstyr på skolen.

## 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 De operationelle Bestemmelser, der godkendes af direktionen.

#### 2.2.2 Klassifikation

Data skal klassificeres efter konsekvenser ved brud på fortrolighed, integritet og tilgængelighed og beskyttelsen skal tilpasses efter klassifikationsniveau. Informationsservices, herunder it-services, it-systemer, print, men også funktioner som fx postomdeling, skal klassificeres efter konsekvenser ved brud på fortrolighed, integritet og tilgængelighed og servicen skal tilpasses efter klassifikationsniveau. Leverandører skal klassificeres efter, hvor kritiske de er i forhold til fortrolighed, integritet og tilgængelighed og deres mulighed for at påvirke informationsikkerheden i kommunen.

#### 2.2.3 Overvågning af informationservices

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

#### 2.2.4 Kontroller

Der skal foretages regelmæssige kontroller til sikring af, at kritiske 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 De operationelle Bestemmelser, 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 og løbende under ansættelsen.

- 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 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. De operationelle Bestemmelser.
- 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 De operationelle Bestemmelser.
- 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 alle persondatabehandlinger udpeges på chefniveau, en **dataansvarlig**, 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 samt styring og projektledelse. Her sikres, at "Den gode IT-anskaffelse" følges, herunder at der foretages en sikkerhedsmæssig vurdering og test af løsninger, kvalificering af kravspecifikation, hvad angår IT-sikkerheden, ved anskaffelsen 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

Den enkelte medarbejder skal forholde sig til informationssikkerhed uanset niveau og opgave og føle medansvar for, at der træffes de nødvendige forholdsregler. Både ledere og medarbejdere skal være opdaterede i forhold til de risici, som de kan påvirke i deres rolle og opgaver. Ledere på alle niveauer skal have et overblik over risikoen i deres område og har ansvaret for den løbende dialog med medarbejdere om risici og nødvendige forholdsregler for at håndtere dem.

### 2.4.1 Awareness

Der er etableret et awareness-program, som løbende arbejder med at udbrede kendskabet til kommunens informationssikkerhedspolitik og de retlige krav i databeskyttelsesforordningen og databeskyttelsesloven. Programmet udvides løbende i forhold til det lokale- og nationale trusselsbillede. Effekten af de gennemførte awareness-aktiviteter måles og indgår ligeledes i den løbende udvikling af programmet.

Der fastsættes nærmere krav i De operationelle Bestemmelser.

## 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 IT-services, som anvendes i kommunen, skal tydeligt deklareres og godkendes af ledelsen.

## 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.

De ansvarlige ledere skal gives let adgang til oplysninger, der er nødvendige for at kunne udføre ledelsestilsyn. Hvis der gives adgang til fortrolige data uden for det etablerede sikkerhedsmiljø, kræves en forudgående direktionsgodkendelse. Adgangskontrolens 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 det fornødne sikkerhedsniveau og forbedrer og forenkler kommunens opfyldelse af lovgivningens krav til sikring af "de registreredes rettigheder".

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

Det skal sikres, at samarbejdet med eksterne parter ikke kompromitterer Gentofte Kommunes målsætning for informationssikkerhed. Kravene til eksterne parter skal fastlægges ud fra politikken og ud fra en risikovurdering af det konkrete samarbejde. Eksterne parter skal dokumentere efterlevelsen af kravene og der skal ske løbende opfølgning. Der udarbejdes særskilte retningslinjer herfor: 'IT-retningslinjer for leverandører'.

## 2.10 Håndtering af sikkerhedshændelser

Der skal opretholdes et beredskab, så sikkerhedshændelser kan håndteres effektivt. Ved alvorlige hændelser skal der foretages en efterfølgende evaluering af hændelsen.

Sikkerhedsniveauet omkring de enkelte systemer og data fastlægges på baggrund af en risikovurdering og under hensyn til lovbestemte og kontraktlige krav.

## 2.11 Evaluering

Afdelingschef for Digitalisering og IT leverer en årlig status og forslag til ny årsplan, herunder omfanget af evaluering og opfølgning, til behandling i direktionen. Direktionen skal orienteres om alvorlige informationssikkerhedsbrud. Ved væsentlige personalerelaterede brud på sikkerheden involveres HR-chefen.

# 3 Ikrafttrædelse og ændringer

Informationssikkerhedspolitikken skal godkendes af Kommunalbestyrelsen hver fjerde år.

Redigering af Informationssikkerhedspakken 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 De operationelle Bestemmelser udarbejdes med inddragelse af databeskyttelsesrådgiveren og godkendes af direktionen.
3. Informationssikkerhedspolitikernes 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.

