

# Fredericia Kommunes Informationssikkerheds- politik 2018

---

# Indholdsfortegnelse

Indledning

Hvad og hvem er omfattet?

Ansvar og konsekvens

Vision, mission og formål

Fortrolighed, tilgængelighed og integritet

Principper

Opfølgning

Organisering

Godkendelse

# Indledning

---

# Indledning

**Dette dokument er informationssikkerhedspolitikken for Fredericia Kommune.**

**En politik der sætter rammerne for, hvordan Fredericia Kommune teknisk og adfærdsmæssigt håndterer informationer/persondata (personnummer, køn, adresse, e-mailadresse m.v.) fra borgere og medarbejdere.**

**Informationssikkerhedspolitikken er et strategisk styringsredskab, hvor Fredericia Kommunes mål, omfang, ansvarsplacering og rammer for styringen af informationssikkerhed fastsættes.**

**Hensigten med politikken er at tilkendegive over for alle, som har relation til Fredericia Kommune, at brugen af informationer og informationssystemer er omfattet af gældende lovgivning, standarder og regler.**

**Denne Informationssikkerhedspolitik er overordnet den nuværende it-sikkerhedspolitik, og vil løbende erstatte denne og bilag.**

# Om informationssikkerhedspolitikken

- Fredericia Kommunes styring af informationssikkerhed bygger på principperne i den internationale standard for informationssikkerhed, ISO 27001 og sikkerhedsbekendtgørelsen.
- Standarden stiller krav om, at topledelsen fastlægger informationssikkerhedspolitikken og målsætningerne for informationssikkerhed.
- Informationssikkerhedsudvalget (ISU) har ansvaret for, at informationssikkerhedspolitikken bliver udarbejdet og opdateret.
- Informationssikkerhedspolitikken godkendes af byrådet.
- Informationssikkerhedspolitikken offentliggøres på [www.fredericia.dk](http://www.fredericia.dk)
- Informationssikkerhedspolitikken skal revurderes årligt, eller hvis der sker væsentlige ændringer i den kommunale organisation, lovgivning eller trusselsniveau.

# Hvad og hvem er omfattet?

---

# Hvad er omfattet?

Fredericia Kommune definerer informationssikkerhed som værende den samlede mængde af foranstaltninger, der skal sikre beskyttelsen af informationer.

Informationssikkerhedspolitikken gælder for:

- Alle systemer og alle data i Fredericia Kommunes besiddelse.
- Tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af Fredericia Kommunes it-systemer og papirarkiver.

# Hvem er omfattet?

Informationssikkerhedspolitikken gælder for alle ansatte i Fredericia Kommune uanset ansættelsesform. Det vil i praksis sige:

- Fastansatte
- Midlertidigt ansatte, herunder praktikanter, studiemedarbejdere og ansatte med løntilskud
- Eksternt tilknyttede personer, herunder konsulenter og servicemedarbejdere
- Politikere og samarbejdspartnere med adgang til Fredericia Kommunes informationsaktiver



# Ansvar og konsekvens

---

# Politik, roller og ansvar

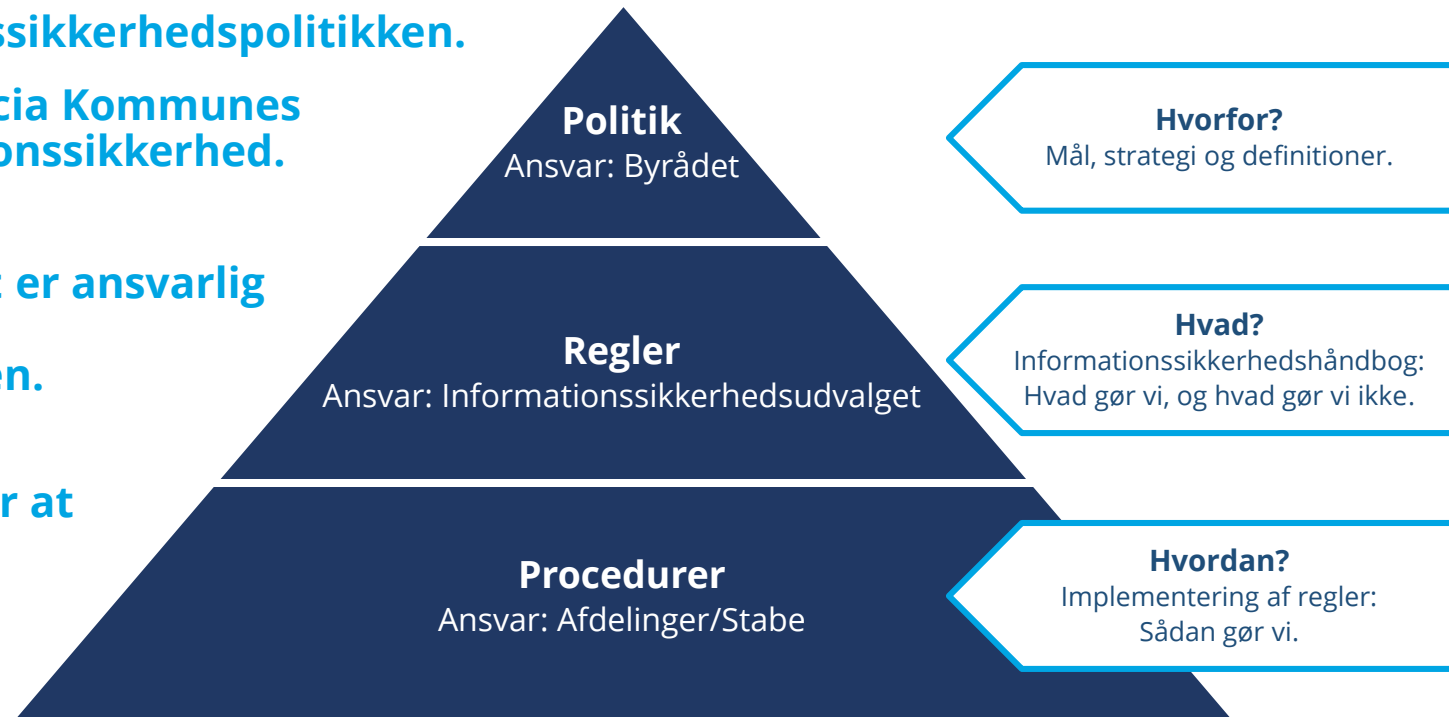
Byrådet godkender informationssikkerhedspolitikken.

Kommunaldirektøren er Fredericia Kommunes øverste ansvarlige for informationssikkerhed.

Informationssikkerhedsudvalget er ansvarlig for realisering og efterlevelse af informationssikkerhedspolitikken.

Chefer og ledere er ansvarlige for at implementere gældende regler i procedurer og arbejdsgange.

Alle er ansvarlige for at efterleve gældende regler.



# Sikkerhedsniveau

Fredericia Kommunes sikkerhedsniveau skal først og fremmest indfri de forventninger til troværdighed og stabilitet, der er til behandling af forretningskritiske data. Fredericia Kommune ønsker at fremstå med et sikkerhedsniveau, der tilgodeser:

- Gældende lovgivning
- De anerkendte principper for informationssikkerhed i form af ISO 27001

# Medarbejderens ansvar

Medarbejdere, politikere og samarbejdspartnere i Fredericia Kommune har et ansvar for at passe på borgernes og kommunens data. De er forpligtet til at efterleve Informationssikkerhedspolitikken med tilhørende regler, forretningsgange og procedurer.

Informationssikkerhed skal være en del af den måde de tænker, handler og arbejder på. Dermed er de med til at sikre, at borgere kan føle sig trygge, når de behandler deres data.

Hvis medarbejderen opdager trusler mod informationssikkerheden eller brud på denne, skal medarbejderen straks rapportere til nærmeste leder, som herefter vurderer, hvordan situationen skal håndteres.

Hvis der indtræffer en alvorlig informationssikkerhedshændelse, er det Informationssikkerhedsudvalgets ansvar, at der foretages en vurdering af hændelsens årsag, samt en vurdering af, om dette giver anledning til at iværksætte sikkerhedsmæssige tiltag.

# Afbalanceret informationssikkerhed

Sikkerhedsniveauet afbalanceres.

Data og systemer sikres ud fra en vurdering af, hvad der er en balanceret indsats, der vægter hensynet til brugervenlighed, sikkerhed, økonomi og fleksibilitet i det daglige arbejde.

Krav til informationssikkerhed skal vurderes i forhold til deres relevans for Fredericia Kommune - dermed holdes fokus på et informationssikkerhedsniveau, hvor sund fornuft er en afgørende faktor.

# Vision, mission og formål

---

# Vision og mission for informationssikkerhedspolitikken

## Vision

Fredericia Kommunes borgere, medarbejdere, samarbejdspartnere og virksomheder har tillid til og er trygge ved Fredericia Kommunes håndtering, brug og opbevaring af data og informationer.

## Mission

Fredericia Kommune beskytter individets rettigheder ved behandling af persondata.

# Formål for informationssikkerhedspolitikken

Informationssikkerhedspolitikken har to formål:

- **Teknisk og it-sikkerhedsmæssigt** – Fredericia Kommune efterstræber høj driftssikkerhed og minimeret risiko for nedbrud, tab og manipulation af data.
- **Adfærdsmæssigt** – Fredericia Kommune efterstræber bedst mulige understøtning af bevidstheden om informationssikkerhed i organisationen.



# Fortrolighed, tilgængelighed og integritet

---

# Parametre for informationssikkerhed

Informationssikkerhed er at beskytte informationers:

- Fortrolighed
- Tilgængelighed
- Integritet

For Fredericia Kommune er et højt sikkerhedsniveau både et krav for at kunne overholde lovgivning, og det er et kvalitetselement i forhold til at kunne tilbyde en sikker service over for borgere, samarbejdspartnere, myndigheder og professionelle.

# Fortrolighed

Fredericia Kommune skal sikre fortrolig behandling, opbevaring og overførsel af data, hvor kun brugere der har lov har adgang.

Brud på fortrolighed handler om, at data mister sin beskyttelse, og uvedkommende dermed får adgang til data, som de ikke burde have adgang til.

Teknisk betyder fortrolighed, at Fredericia Kommune bl.a. arbejder for:

- Adgangskontrol og rettighedsstyring, for at sikre autoriseret databehandling.
- Logning, for at dokumentere adgang til data.
- Kryptering, for at minimere risikoen for uautoriseret adgang til data.

Adfærdsmæssigt betyder fortrolighed, at medarbejderne følger retningslinjer, principper og procedure for informationssikkerhed og for eksempel ikke videregiver fortrolige oplysninger eller adgangskoder skriftligt eller mundtligt.

For Fredericia Kommune er fortrolighed den vigtigste parameter for informationssikkerhed.

# Tilgængelighed

Fredericia Kommunes informationer og informationssystemer skal være tilgængelige for brugerne, borgerne og virksomhederne, når de har behov for dem.

Teknisk betyder tilgængelighed, at Fredericia Kommune arbejder for:

- Driftssikre informationssystemer, som reagerer hurtigt.
- Brugervenlighed, så informationssystemer er let tilgængelige.
- Integrationer, så data flyder mellem relevante systemer.

Adfærdsmæssigt betyder tilgængelighed, at Fredericia Kommune arbejder for korrekt journalisering.

# Integritet

Fredericia Kommune skal opnå en pålidelig og korrekt behandling af information ved at minimere risiko for menneskelige eller systemmæssige fejl, forsøg på svindel eller bedrageri, samt udefrakommende hændelser

Teknisk betyder integritet, at Fredericia Kommune bl.a. arbejder for:

- Integrationer, for at dele og genbruge data.
- Brugervenlighed, for at undgå menneskelige fejl.
- Validitet, det vil sige tydelig versionering og klassifikation af data, så der sagsbehandles ud fra valide data

Adfærdsmæssigt betyder integritet, at Fredericia Kommune løbende kompetenceudvikler sine medarbejdere inden for informationssikkerhed og i korrekt sagsbehandling.

# Principper

---

# Principper

Fredericia Kommune implementerer informationssikkerhed efter følgende principper:

- **Procedurer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af driften og det daglige arbejde.**
- **Løbende uddannelse for at udvikle vidensniveauet hos alle medarbejdere og for at fastholde opmærksomheden på informationssikkerhed.**
- **En ærlig og troværdig kommunikation om sikkerhedshændelser over for berørte borgere og eksterne parter.**
- **Information til borgere og medarbejdere om deres muligheder og rettigheder.**
- **Praktisering af kontrakt- og leverandørstyring, så eksterne konsulenter, samarbejdspartnere og leverandører lever op til kommunens niveau for informationssikkerhed.**

# Opfølgning

---



# Opfølgning

Fredericia Kommune vurderer og følger op på informationssikkerhed på følgende måde:

- Løbende skriftlig registrering og opfølgning på informationssikkerhedshændelser
- Gennemføre interne audits om informationssikkerhed
- Opfølgning på vidensniveau inden for informationssikkerhed

# Organisering

---

# Fredericia Kommunes organisering af informationssikkerhed

## Øverste ansvarlige:

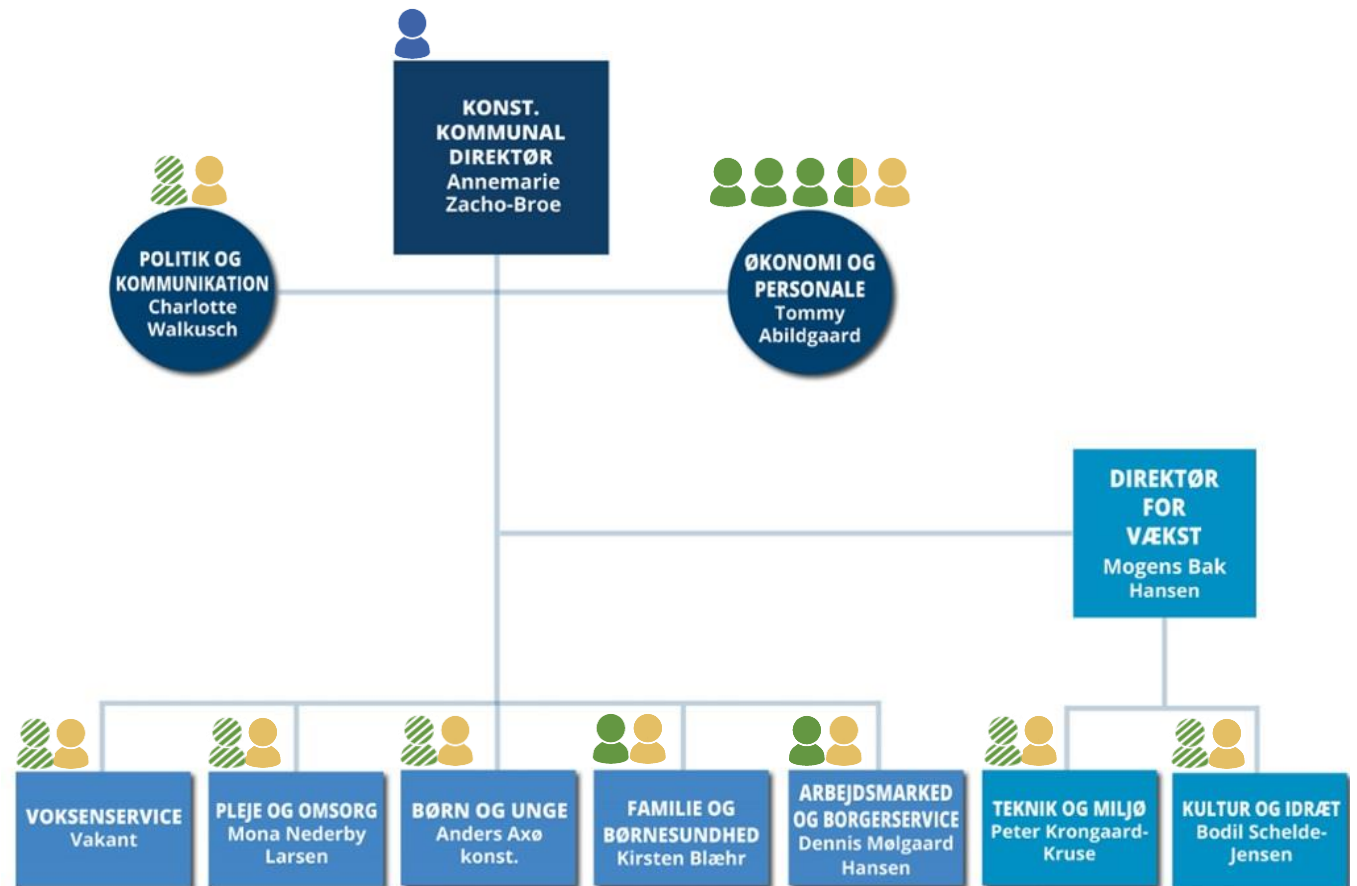
- **Kommunaldirektør**

## Informationssikkerhedsudvalg:

- **Økonomi og Personalechef**
- **Databeskyttelsesrådgiver (DBR)**
- **IT-chef**
- **Fællessekretariatschef (sekretær for udvalget)**
- **2 chefer fra fagområder og stabe (én skiftes hvert år)**

## Informationssikkerhedsnetværk:

- **Databeskyttelsesrådgiver (DBR)**
- **1 informationssikkerhedskoordinator pr. fagområde og stab**
- **Evt. suppleant pr. fagområde og stab**



# Interne organisatoriske forhold

Informationssikkerhedsudvalget har det overordnede ansvar for at sikre, at Fredericia Kommune har defineret en informationssikkerhedspolitik.

Informationssikkerhedsudvalget beslutter overordnede strategiske projekter af informationssikkerhedsmæssig karakter, men har i praksis delegeret det daglige ansvar for informationssikkerheden til niveau 2 chef.

Informationssikkerhedsudvalget uddelegerer ansvar og opgaver vedrørende de enkelte funktionsområder til stabs- og fagcheferne, herunder også for vejledning og instruktion af medarbejdere.

# Godkendelse

---

# Godkendelse

Informationssikkerhedspolitikken udarbejdes og vedligeholdes af Informationssikkerhedsudvalget, der indstiller politikken til godkendelse i byrådet.

Informationssikkerhedspolitikken er godkendt af Fredericia Byråd

Dato \_\_\_\_\_

Underskrift \_\_\_\_\_

# Versionsstyring

Versionsnummer	Dato for version	Ændring	Årsag	Ansvarlig
Version 1.00	Godkendt af Informationssikkerhedsudvalget den 14. maj 2018	Fredericia Kommunes første informationssikkerhedspolitik. FK har tidligere haft it-sikkerhedspolitik	EUs Databeskyttelsesforordning den 25. maj 2018	Kommunaldirektør Annemarie Zacho-Broe