FREDENSBORG
KOMMUNE

Informationssikkerhedspolitik for Fredensborg Kommune

Godkendt af Byrådet den 30.05.2023

Indhold

1. Indledning

1.1 Formål med informationssikkerhedspolitikken

Fredensborg Kommunes informationssikkerhedspolitik er vores sikkerhedsgrundlag og vores fælles forståelse af, hvad informationssikkerhed er. Informationssikkerhedspolitikken fastlægger vores ambitionsniveau og opstiller rammerne for de sikkerhedstiltag, som er nødvendige at følge, når vi som en organisation skal leve op til forskellige krav.

Med informationssikkerhed forstår vi den nødvendige beskyttelse af samtlige ressourcer, der indgår i eller bidrager til kommunens behandling og kommunikation af data elektronisk, i papirform mm., herunder også teknologi og organisatoriske processer.

1.2 Hovedmålsætninger i informationssikkerhedspolitikken

Informationssikkerheden skal understøtte Fredensborg Kommunes opgaveløsning i forhold til at sikre stabilitet i tilgangen til data, fortrolighed i forhold til fortrolige og følsomme data samt pålidelighed i datas indhold. Det sikres ved, at kommunen i vores daglige aktiviteter lever op til almindeligt anerkendte principper for informationssikkerhed.

Målet for informationssikkerheden er at:

- Understøtte bevidstheden om informationssikkerhed i organisationen
- Opnå høj driftssikkerhed og minimeret risiko for store nedbrud og tab af data
- Opnå korrekt funktion af it-systemerne med minimeret risiko for manipulation af data og systemer og fejl i disse
- Opnå mulighed for fortrolig behandling, transmission og opbevaring af data. Dvs. at faciliteter hertil skal være til stede og benyttes efter konkret behov
- Sikre mod forsøg på tilsidesættelse af sikkerhedsforanstaltninger

1.3 Omfang

Informationssikkerhedspolitikken er det dokument, der angiver de beslutninger, som Fredensborg Kommune har truffet med henblik på nærmere at fastlægge det tilstrækkelige sikkerhedsniveau samt definere de krav, der skal stilles, for at sikkerhedsniveauet opretholdes. Derfor fastlægges omfanget af informationssikkerhedspolitikken således:

- Informationssikkerhedspolitikken gælder for alle ansatte i Fredensborg Kommune uanset ansættelsesform, herunder også eksterne konsulenter.
- Informationssikkerhedspolitikken gælder for alle systemer og alle data i kommunens besiddelse.
- Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til organisationens systemer og data, skal ligeledes have kendskab til og følge informationssikkerhedspolitikken.
- Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af Fredensborg Kommunes it-systemer og papirarkiver.
- Informationssikkerhedspolitikken godkendes af Byrådet og gennemgås en gang årligt for at sikre, at den er i overensstemmelse med de sikkerhedsmålsætninger, som Fredensborg Kommune arbejder efter.

2. Sikkerhedsniveau

Fredensborg Kommunes sikkerhedsniveau skal først og fremmest indfri de forventninger til troværdighed og stabilitet, der er til behandling af forretningskritiske data i en organisation med samfundsmæssig betydning. Fredensborg Kommune ønsker at fremstå med et højt sikkerhedsniveau, der tilgodeser:

- Lovgivningsmæssige krav
- De anerkendte standarder for informationssikkerhed i form af ISO 27001

3. Organisering og ansvar

3.1 Interne organisatoriske forhold

Direktionen beslutter overordnede strategiske projekter af informationssikkerhedsmæssig karakter, men har i praksis delegeret det daglige ansvar for informationssikkerheden til centercheferne.

Centercheferne vil uddelegere ansvar og opgaver vedrørende de enkelte funktionsområder, herunder også for vejledning og instruktion af medarbejdere.

GDPR-teamet (Jura) og IT-sikkerhedsteamet (IT) vejleder ledelse og medarbejdere i informationssikkerhedsspørgsmål, koordinerer og følger op på informationssikkerhedsrelaterede aktiviteter.

3.2 Eksterne samarbejdspartnere

Der skal indgås skriftlige aftaler med eksterne samarbejdspartnere og de sikkerhedskrav, der stilles skal defineres ud fra databeskyttelsesforordningen, den danske persondatalov samt ISO 27001. Kravene skal fremgå af de skriftlige aftaler.

For at sikre klarhed over de sikkerhedskrav, der skal stilles, skal der ske en konkret identifikation af risici i forbindelse med brug af eksterne leverandører.

Eksterne samarbejdspartnere, der har adgang til data, skal efterleve samme retningslinjer som gælder internt i organisationen.

4. Klassifikation af systemer og data

For at sikre at vores systemer og data har det rigtige sikkerhedsniveau, skal disse identificeres og klassificeres.

Data og systemer skal klassificeres i forhold til tilgængelighed og til sikkerhed (fortrolighed og datas pålidelighed).

Tilgængelighed af data og systemer prioriteres indbyrdes i følgende kategorier:

- A – tilgængelighed er forretningskritisk, og kan ikke erstattes af manuelle procedurer
- B – tilgængelighed er vigtigt, men funktionerne kan udføres manuelt i en begrænset tidsperiode
- C – tilgængelighed er ikke kritisk, og funktionerne kan afbrydes i en længere tidsperiode

Informationssikkerhed af data klassificeres efter følgende kategorier:

- 1 – forretningskritiske beslutninger bliver taget på grundlag af data – data med høj grad af fortrolighed
- 2– data danner grundlag for beslutninger, men de er ikke kritiske – data er interne og eksponeres ikke udadtil
- 3 – data danner aldrig eller kun sjældent grundlag for beslutninger – data er offentlige

5. Brugeradfærd

Opretholdelse af det ønskede sikkerhedsniveau er afhængig af, at vi alle tager ansvar for informationssikkerheden.

Alle ansatte skal være bekendt med informationssikkerhedspolitikken og gældende retningslinjer for ønsket adfærd. Find listen med links til gældende retningslinjer nedenfor under afsnit 10. Henvisninger.

Anvendelse af it og behandling af data er selvfølgelige redskaber i varetagelsen af de daglige arbejdsopgaver. Håndteringen af vore redskaber kræver ikke specielle forudsætninger, men bør ske med omtanke og almindelig sund fornuft:

- Persondata behandles fortroligt.
- Der anvendes personligt login og password, og password skiftes i overensstemmelse med passwordpolitikken, som kan findes under afsnit 10.
- Datamedier, herunder f.eks. USB-stik, harddisk og CD-rom, med persondata og vigtige informationer behandles og beskyttes med omhu mod at uvedkommende får adgang til dem.
- Mobilt udstyr beskyttes og opbevares, så andre ikke kan få adgang til det.
- Det er vigtigt at kunne anvende internettet i mange sammenhænge. Besøg på sider med racistisk, uetisk eller pornografisk indhold er ikke acceptabelt på kommunens udstyr og internet.
- Der må kun anvendes it-programmer, som er godkendt af It-afdelingen.
- Hvis man oplever, at der sker brud på informationssikkerheden, er det vigtigt at informere sin nærmeste leder og GDPR-teamet (Jura). Find link til retningslinjer under afsnit 10.

Der udarbejdes detaljerede retningslinjer for ønsket brugeradfærd på udvalgte områder som f.eks. e-mail og internet, password, og rapportering af sikkerhedshændelser. Som afhjælpningsforanstaltninger til at minimere vurderede risici, skal retningslinjerne jævnligt revurderes og opdateres.

6. Fysisk sikkerhed

Adgangen til fysiske lokaliteter er sikret mod uvedkommendes adgang.

6.1 Sikre områder

Lokaler, hvor der opbevares fortrolige dokumenter eller medarbejderdata, skal være aflåst, når ingen er til stede.

6.2 Beskyttelse af udstyr

It-udstyr beskyttes mod ødelæggelse og skade, der følger af brand, vandskade, strømsvigt og andre skader, som udspringer af hændelser i det omkringliggende miljø.

Kritisk it-udstyr skal overvåges og vedligeholdes efter leverandørens anvisninger. Ved bortskaffelse, reparation eller genbrug af it-udstyr sikres det, at udstyret er forsvarligt renset for alle data.

Når it-udstyr bortskaffes eller på anden måde udskiftes, slettes alle data på en sådan måde, så de ikke kan gendannes.

7. Styring af netværk og drift

7.1 Skadevoldende programmer (vira, orme, spy- og malware)

Skadevoldende programmer kan sætte hele organisationen ud af drift, og det kan være meget dyrt at rense it-systemerne, hvis de er blevet ramt af et hackerangreb eller en virus. Alt godkendt it-udstyr, der er tilsluttet Fredensborg Kommunes netværk har, hvor det er muligt, installeret et aktivt og opdateret antivirusprogrammel, der kan opdage, rense og beskytte mod forskellige former for skadevoldende programmer. Eksterne brugere skal have udleveret godkendt udstyr fra IT-afdelingen for at kunne arbejde i Fredensborg Kommunes systemer. Alternativ skal aftales med IT.

Det er ikke tilladt at installere egne programmer på Fredensborg Kommunes IT-udstyr.

7.2 Netværkssikkerhed

For at undgå uautoriseret adgang, skal vores netværk sikres. Sikring af vores netværk imod uautoriseret adgang styres af it-afdelingen. Det sker f.eks. via adgangskontrol og adskillelse af netværkstjenester, hvor dette er hensigtsmæssigt.
Der må ikke installeres netværksudstyr som f.eks. trådløse modems uden it-afdelingens godkendelse.

Der er etableret firewall-løsninger, der beskytter mod forbindelse til upålidelige netværk.

Der etableres udelukkende forbindelser fra internettet til sikkerhedsgodkendte servere som f.eks. e-mail- og webservere.

7.2.1 Trådløse netværk

Der er etableret trådløst netværk på alle Fredensborg Kommunes lokationer. Der må kun etableres trådløst lokalnet efter it-afdelingens godkendelse. Nettet skal konfigureres således, at uautoriseret adgang og aflytning ikke er mulig. Trådløse netværk betragtes som usikre, ubeskyttede netværk, og adgang til trådløst netværk kræver gyldigt brugernavn og kodeord samt anvendelse af godkendt udstyr.

Gæster kan få adgang til gæstenetværket og tilslutte eget udstyr til netværket ved at validere sig med telefonnummer. Netværket kan og må kun anvendes til internetadgang – direkte adgang til interne systemer er ikke tilladt fra gæstenetværket. Der foretages overvågning og logning af gæsters anvendelse af internettet.

8. Adgang og rettigheder til data og systemer

Følsomme og kritiske systemer og data skal beskyttes mod uautoriseret adgang og ændring, uanset hvor de er, og uanset hvorfra de tilgås. Adgang til og ændring af følsomme eller kritiske systemer eller data skal let kunne spores til personen (logning).

8.1 Brugerens ansvar

Alle medarbejdere er ansvarlige for deres personlige adgangskoder, og for at følge vedtagne retningslinjer for password.

8.2 Styring af netværksadgang, systemadgang og adgang til brugersystemer og informationer

Styringen af brugeradgange til netværk, systemer mm. sikrer, at alle brugere og alt netværksudstyr er identificeret, og at der er opdaterede fortegnelser herover. Der er sikringsforanstaltninger, så adgangskontroller til systemer og data ikke kan omgås.

8.3 Mobilt udstyr og fjernarbejdspladser

Informationssikkerhedspolitikken gælder for alt it-udstyr tilhørende Fredensborg Kommune. I retningslinjer fastlægges de regler, som skal overholdes ved brug af mobilt udstyr og hjemmearbejdspladser.

9. Sikkerhedsbrud

9.1 Rapportering af sikkerhedsbrud og svagheder

En væsentlig faktor i informationssikkerhedsarbejdet består i at reagere på hændelser af sikkerhedsmæssig karakter. Derfor skal sikkerhedsbrud rapporteres, herunder også mistanke om brud, og der skal ske opfølgning herpå. Alle medarbejdere har pligt til at rapportere sikkerhedsbrud til GDPR-teamet (Jura), så de kan imødegås, inden de udvikler sig. Procedure for rapportering af sikkerhedsbrud er beskrevet på HosFrede.dk. Find procedure under afsnit 10.

10. Henvisninger

Informationssikkerhedspolitikken angiver de overordnede mål for sikkerhedsniveauet i Fredensborg Kommune. Informationssikkerhedspolitikken bliver derfor suppleret af retningslinjer og procedure for specifikke områder. De kan findes via link her[1]:

1. Passwordpolitik
2. Procedure ved sikkerhedsbrud

[1] Log ind på HosFrede.dk med dit fulde navn og medarbejdernummer.