Odder Kommune
Rådhusgade 3
8300 Odder
Tel. 8780 3333

Odder
Kommune

Overordnet Informationssikkerhedsstrategi

for Odder Kommune

Indhold

Indledning

Det er et krav, at Odder Kommune som dataansvarlig myndighed sikrer beskyttelse af personoplysninger.

Byrådet har det endelige politiske ansvar for, at kommunen håndterer borgeres, virksomheders og øvrige offentlige myndigheders informationer på betryggende vis.

I forhold til kommunens egen lokale digitaliseringsstrategi har vi længe selv valgt at digitalisere opgaveløsningen i form af selvbetjeningsløsninger til borgerne og til effektivisering af de interne arbejdsgange. Ydermere er kommunerne i de seneste år, fra centralt hold, blevet på pålagt at indføre *obligatorisk* digital selvbetjening og digital kommunikation med borgere, virksomheder og samarbejdsparter. Digitalisering er således et vilkår og ikke blot et muligt tilvalg.

Dette stiller store krav til vores informationssikkerhed og er dermed en afgørende faktor for kommunens digitaliseringsindsats.

Dette dokument beskriver Odder Kommunes overordnede informationssikkerhedsstrategi. Denne strategi sætter rammerne for operationel organisering og styring af informationssikkerhed, der udmøntes i etableringen af fastsatte regler og procedurer for Odder kommunes informationssikkerhedshåndtering. Hermed etableres grundlaget for det daglige arbejde med informationssikkerhed inden for kommunens virke.

Den samlede informationssikkerhedsbeskrivelse består af 3 dokumenter:

1.) Den overordnede informationssikkerhedsstrategi, som godkendes af Byrådet.

2.) Organisering og styring af informationssikkerhed, der fastlægger ansvar og styring. Denne godkendes af direktionen og tager udgangspunkt i ISO27001 standarden, som KL anbefaler at kommunerne anvender.

3.) De konkrete regler, som vi alle skal overholde i det daglige arbejde. Her har vi valgt at arbejde efter ISO27002 standarden for informationssikkerhed. Disse regler godkendes af kommunens øverste sikkerhedsansvarlige.

Både organisering og styring af informationssikkerhed og konkrete regler revideres ved behov inden for rammerne af den overordnede informationssikkerhedsstrategi.

Odder Kommune har tidligere anvendt standarden DS484 som ramme for informationssikkerhed. Den nye informationssikkerhedsbeskrivelse tager som angivet udgangspunkt i ISO27001/27002, som giver mulighed for løbende udvidelser til håndtering af nye sikkerhedsmæssige problemstillinger.

Mål for sikkerhedsniveau

Odder Kommune fastlægger på baggrund af konkrete risikovurderinger et sikkerhedsniveau, som svarer til betydningen af de pågældende informationer og systemer. Sikkerhedsniveauet og anvendelsen skal til en hver tid være i overensstemmelse med gældende lovgivning.

Ved fastlæggelse af sikkerhedsniveauet tages der udgangspunkt i 3 begreber: Fortrolighed, Integritet og Tilgængelighed. Disse begreber anvendes til afdækning af risici i samarbejde med afdelingernes system- og dataansvarlige.

Fortrolighed
Borgerne skal til enhver tid kunne stole på, at de trygt kan overlade deres fortrolige data til Odder Kommune. Informationssikkerhed skal sikre fortrolig behandling, transmission og opbevaring af data, hvor kun autoriserede brugere har adgang.

Integritet
Informationssikkerhed skal sikre pålidelig og korrekt brug af løsningerne og minimere risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefra kommende hændelser.

Tilgængelighed
Informationssikkerhed skal være medvirkende til, at vi opnår høj tilgængelighed og minimere risiko for nedbrud på vore systemer.

Odder Kommune skal dermed træffe fornødne foranstaltninger til, at beskytte oplysninger mod uautoriseret anvendelse, fejl i de registrerede eller behandlede oplysninger og til at sikre den højst mulige "oppetid" for vores løsninger.

Holdninger og principper

Troværdigheden på informationssikkerhedsområdet over for omverdenen herunder borgere, virksomheder og samarbejdspartnere må ikke berettiget kunne drages i tvivl. Herigennem kan kommunen opnå og bibeholde et godt omdømme over for borgere og virksomheder.

Odder Kommune vil fastlægge informationssikkerhedsforanstaltninger som en afvejning mellem de ofte modstridende hensyn, ønsket om høj sikkerhed, hensynet til brugervenlig it-anvendelse og omkostningerne ved investering i sikkerhed.

Sikkerhedsforanstaltninger kan til tider opleves som en barriere for medarbejdernes daglige anvendelse af IT og *kan* give anledning til besværlige arbejdsgange. Her vil Odder Kommune sikre medarbejdernes forståelse for nødvendigheden af disse foranstaltninger, således at sikkerhed bliver en *naturlig* del af arbejdet i kommunen. Odder Kommune vil løbende arbejde med at informere medarbejderne, så de får de nødvendige kompetencer, til at sikre at informations-sikkerheden kan overholdes samtidig med, at arbejdet kan udføres så effektivt som muligt.

Følgende 3 målsætninger konkretiserer ovennævnte principper:

1. Fortrolighed i forvaltningen

Vi vil i vores IT-anvendelse sikre, at behandling af data og informationer sker med fortrolighed og i overensstemmelse med god forvaltningsskik. Informationssikkerhed skal derfor sikre, at informationer om borgerne holdes fortroligt for uvedkommende.

2. Sikre kommunens medarbejdere, borgere og virksomheder adgang til en stabil og korrekt kommunal service.

Odder Kommune understøtter alle forretningsområder, borgere og virksomheder med digitale løsninger for at sikre en effektiv administration, der medfører hurtig og korrekt service.

Informationssikkerhedsforanstaltninger skal sikre borgere og virksomheder tilgængelighed og pålidelighed i adgang til de eksterne systemer på www.odder.dk og selvbetjeningsløsninger.

For de interne systemer skal der sikres stabil drift, således at It-anvendelsen understøtter korrekt service til tiden.

3. Forebyggende sikkerhed

Informationssikkerheden skal implementeres gennem forebyggende tekniske tiltag og informationsaktiviteter, der øger medarbejdernes kompetencer og viden omkring informationssikkerhed.

Tekniske kontroller er væsentlige, men den menneskelige faktor i form af brugeradfærd ses som den største risiko-faktor. Den menneskelige faktor kan ikke kontrolleres og er derfor afhængig af medarbejdernes kompetencer og forståelse for deres rolle i forbindelse med informations-sikkerhed.

Gyldighed og omfang

Overholdelse af kommunens informationssikkerhed er gældende for alle ansatte, byrådspolitikere og eksterne samarbejdspartnere.

Kommunens informationssikkerhed gælder for alle lokaliteter hvor der sker en anvendelse og bearbejdning af kommunens informationer – Rådhus, institutioner, hjemmearbejdspladser, eksterne adgange, adgang via mobil mv.

For leverandører, som har adgang til kommunens systemer, gælder det, at de skal have implementeret et sikkerhedsniveau, der mindst svarer til kommunens niveau. Dette sikres ved indgåelse af databehandleraftaler og Odder Kommune skal have mulighed for at sikre sig, at leverandører reelt lever op til det påkrævede sikkerhedsniveau.

Ansatte, byrådsmedlemmer og samarbejdspartnere med fysisk eller logisk adgang til kommunens systemer skal være bekendt med sikkerhedsreglerne og skal forpligte sig til at overholde reglerne.

Organisering, ansvar og godkendelse

Informationssikkerhedsstrategien godkendes af Byrådet og varetages af kommunaldirektøren, der er den øverste sikkerhedsansvarlige. Det daglige arbejde udføres i samarbejde med kommunens Informationssikkerhedsorganisation.

Informationssikkerhedsorganisationen består af den øverste sikkerhedsansvarlige, en informationssikkerhedsgruppe og herunder direktører og stabs- og virksomhedsledere

Chefen for It- og Indkøb er formand for Informationssikkerhedsgruppen, der mødes ad hoc og straks i forbindelse med alvorlige informationssikkerhedshændelser.

Informationssikkerhedsgruppen sikrer i samarbejde med den øverste sikkerhedsansvarlige vedligeholdelse af den samlede informationssikkerhedsbeskrivelse: strategi, organisering og styring, samt de konkrete regler. Ligeledes sikrer de den løbende risikovurdering, samt information til ledelsen omkring informationssikkerhed.

Direktører og de enkelte stabs- og virksomhedsledere er ansvarlige for udbredelse af informationssikkerhedsregler til egne medarbejdere og for overholdelse af informationssikkerheden i de fagspecifikke områder og systemer inden for deres ansvarsområde.

Sikkerhedsbevidsthed

Medarbejdere med adgang til kommunens systemer skal som nævnt i holdninger og principper overholde informationssikkerhedsregler, der er relevante for deres arbejde. Her er det ledelsens ansvar, at sikre at medarbejderne får de fornødne kompetencer, at informationssikkerhed bliver en del af kulturen og indarbejdes i arbejdets tilrettelæggelse.

Informationssikkerhedsgruppen arbejder kontinuerligt med information i form af video, tests mv. der kan understøtte ledelsen arbejde med udvikling af medarbejdernes kompetencer omkring informationssikkerhed.

Det skal til en hver tid være muligt for medarbejderne at få adgang til den overordnede informationssikkerhedsstrategi, informationssikkerhedsregler og de underliggende procedurer via kommunens intranet.

Overtrædelse

Bevidst eller ubevidst overtrædelse af kommunens informationssikkerhed kan medføre, at borgernes oplysninger kompromitteres, at kommunens brugere, samarbejdspartnere, borgere mv. oplever ustabilitet, uregelmæssigheder og uhensigtsmæssigheder i anvendelse og bearbejdning af kommunens informationer. Dette kan medføre økonomisk tab og forringelse af den kommunale service og kommunens omdømme.

Overtrædelse af informationssikkerheden skal rapporteres til Informationssikkerhedsgruppen og er den daglige leders ansvar. I alvorlige tilfælde behandles overtrædelsen af kommunaldirektøren og kan få ansættelsesmæssige konsekvenser.

Godkendelse

Den overordnede informationssikkerhedsstrategi er godkendt af Byrådet den 22. maj 2017.