Overordnet politik for informationssikkerhed Rødovre Kommune

Denne politik er godkendt af kommunalbestyrelsen den 31. maj 2022.

Vær opmærksom på at anvende senest godkendte version af politikken.

Indledning

Kommunalbestyrelsen fastlægger med denne overordnede politik principper for opretholdelse af informationssikkerhed i Rødovre Kommune. Den overordnede politik for informationssikkerhed beskriver, hvordan Rødovre Kommune vil beskytte systemer, data og informationer, hvor kommunen er ansvarlig for forvaltningen af data og informationer.

Rødovre Kommune anser det for centralt, at der er en god og effektiv sikkerhed i kommunen, som modsvarer den aktuelle risiko. Det vil sige, at kommunen lægger et sikkerhedsniveau som modsvarer, hvor stor betydningen data og information er for kommunen og for de personer, hvis informationer er registeret i kommunen.

Truslerne er mangeartede og ændrer sig hele tiden, derfor arbejder Rødovre Kommune med sikkerhed efter internationale standarder, som understøtter, at arbejdet sker effektivt og på et højt niveau. Rødovre Kommunes sikkerhedsarbejde kontrolleres og tilpasses løbende afhængig af truslerne for at beskytte borgernes oplysninger bedst muligt, og for at sikre både kommunens omdømme og borgernes tillid til kommunens forvaltning.

Rødovre Kommunes samlede informationssikkerhedspolitik er opdelt i:

- Denne politik, som er en overordnet politik for informationssikkerhed, der beskriver rammer, mål og overordnet organisering af indsatsen om informationssikkerhed. Den overordnede politik for informationssikkerhed vedtages af kommunalbestyrelsen efter indstilling fra direktionen.
- En operationel politik for informationssikkerhed, hvor organisering, ansvar og roller, samt sikkerhedsmål er præciseret. Den operationelle politik fastlægges af den administrative ledelse og godkendes af direktionen efter indstilling fra digitaliseringsstyregruppen.
- Retningslinjer, politikker og procedurer, som beskriver risikohåndtering på udvalgte områder med udgangspunkt i arbejdsprocesser, medarbejderpolitikker og tekniske og fysiske forhold. Retningslinjer, politikker og procedurer fastlægges i relevante ledelsesfora og med inddragelse af fagforvaltninger og interessenter.

Figuren illustrerer politikkens sammenhæng til øvrige relevante politikker og retningslinjer for styring af informationssikkerheden

Formål

Formålet med politikken for informationssikkerheden er at beskytte informationer og systemer uafhængigt af, hvor disse findes, oparbejdes og drives. Indsatsen skal tilgodese følgende behov:

- Informationer og it-services er **tilgængelige**, når de personer, som er autoriseret til at se og benytte dem, har behov for det
- Informationer er **korrekte**, og systemerne er driftssikre
- **Personoplysninger og andre fortrolige** informationer beskyttes, så de forbliver hemmelige for alle, der ikke har ret til at kende dem
- Der skal være **gennemsigtighed** i forhold til hvilke formål, data kan anvendes til, og der skal føres en fortegnelse over, hvor der behandles personoplysninger

Politik for Informationssikkerhed

Standarderne ISO 27001og ISO 27002 anvendes som reference og grundlag for styring af informationssikkerhedsindsatsen. Dernæst er Persondataforordningen (EU 27/4/2016/679) og Persondataloven (lov nr. 502 af 23/05/2018) grundlag for arbejdet specifikt med personoplysninger. Med grundlag i disse standarder og lovgivning opfylder Rødovre Kommune følgende mål:

- **Sikkerhedskultur og -bevidsthed.** Det er et ledelsesansvar overordnet at sikre en kvalificeret vurdering af den aktuelle risiko, og at medarbejderne kender reglerne. Kendskab til regler og bevidsthed om risici ved it-anvendelsen og behandling af personoplysninger skal vedligeholdes ved løbende målinger og awareness-aktiviteter, og ved at integrere sikkerhedsovervejelser i eksisterende arbejdsgange.
- **Sikker drift**. Der skal sikres et driftsmæssigt stabilt, sikkert, let tilgængeligt og funktionelt it-serviceniveau, hvor data er tilgængelige og beskyttet efter følsomhed, konsekvens for borgeren og betydning for kommunen. Kritiske it-driftsprocesser skal være formaliseret og systematisk overvåget.
- **Adgang og rettigheder til data og systemer.** Personoplysninger og følsomme og kritiske informationsaktiver skal beskyttes mod uautoriseret adgang og ændring. Adgang til og ændring af følsomme eller kritiske systemer eller data skal kunne spores til brugeren. De ansvarlige ledere skal have let adgang til oplysninger, der er nødvendige for at kunne udføre ledelsestilsyn.
- **Projekter.** Anskaffelse, udvikling og vedligeholdelse af it-systemer skal foretages i henhold til en formaliseret projekt- og/eller ændringsstyringsproces, så der ikke sker brud på sikkerheden eller utilsigtede ændringer i sikkerhedsniveauet. Højrisikoprojekter, herunder væsentlige organisatoriske, tekniske eller fysiske ændringer kræver en ledelsesgodkendt risikohåndteringsplan inden

igangsætning og involvering af Databeskyttelsesrådgiveren, hvis der er tale om behandling af større mængder følsomme personoplysninger.

- **Fysisk sikkerhed**. På steder, hvor der opbevares og anvendes informationer, systemer, infrastruktur og data, skal der være etableret et risikotilpasset niveau af fysisk sikkerhed mod eksempelvis brand, vandskade, tyveri, hærværk, skader forårsaget af menneskelige fejl mv. De fysiske sikringsforanstaltninger må ikke blokere flugtveje eller på anden vis svække personsikkerhed.

- **Håndtering af sikkerhedshændelser.** Der skal sikres en styret proces for håndtering af sikkerhedshændelser, så skaden ved kritiske hændelser holdes på et minimum, og kommunens kritiske opgaver kan videreføres i en nødsituation. Driftsmiljøet og vigtige arbejdsgange skal kunne videreføres inden for en af ledelsen besluttet tidshorisont. Sikkerhedshændelser registreres og omfanget skal mindst en gang årligt evalueres. Ved alvorlige sikkerhedshændelser skal der foretages en efterfølgende evaluering. Tidsfristen for registrering af sikkerhedsbrud skal rapporteres som angivet i Databeskyttelsesforordningen.

Informationssikkerhedspolitikken, retningslinjer og instrukser skal være tilgængelige for alle medarbejdere og skal være indarbejdet i relevante publikationer, herunder medarbejderpolitikker, håndbøger, mv.

Sikkerhedsniveauet fastlægges på baggrund af en risikovurdering og under hensyn til lovbestemte og kontraktlige krav. Ved etablering af sikringsforanstaltninger skal effektivitets- og fleksibilitetspåvirkninger medtænkes. Der skal udarbejdes en årsplan for informationssikkerhed, som beskriver hvilke tiltag informationssikkerhedsorganisationen vil gennemføre for at sikre opfyldelsen af ovenstående målsætninger.

Gyldighedsområde

Informationssikkerhedspolitikken gælder for alle forvaltninger, institutioner og selvejende institutioner ved Rødovre Kommune, samt for eksterne brugere, politikere, samarbejdspartnere og leverandører.

Organisation og ansvar

Alle kommunens ansatte har et medansvar for at retningslinjer for informationssikkerhed overholdes. Ansvaret for den enkelte medarbejder i Rødovre Kommune skal være præcist og entydigt beskrevet med udgangspunkt i nedenstående overordnede organisering:

- **Kommunalbestyrelsen** fastlægger den overordnede informationssikkerhedspolitik efter indstilling fra direktionen.

- **Kommunaldirektøren** er øverste it-sikkerhedsansvarlige og godkender i samråd med direktionen den operationelle informationssikkerhedspolitik efter indstilling fra digitaliseringsstyregruppen.

- **Direktører** har inden for eget område ansvar for implementering og opfølgning på efterlevelse af informationssikkerhedspolitikken.

- **Digitaliseringschefen** varetager, med reference til digitaliseringsstyregruppen, it-sikkerheds-koordineringen og øvrige aktiviteter i henhold til sikkerhedsårsplanen, som aftales med styre-gruppen og godkendes af kommunaldirektøren. Digitaliseringschefen skal sikre, at informations-sikkerhedsmæssige problemstillinger er tilstrækkelig klart belyst, inden der træffes beslutninger om nye projekter eller ændringer. Det er digitaliseringschefens ansvar, at information til styre-gruppen og at information og værktøjer til systemejere effektivt understøtter varetagelsen af de-res respektive opgaver. Digitaliseringschefen er ansvarlig for at driften til ethvert tidspunkt lever op til forvaltningernes sikkerhedsbehov.

- **Digitaliseringsstyregruppen** har det overordnede ansvar for den tværgående indsats, herun-der at politikken og beslutninger er kendt på alle ledelsesniveauer og efterleves effektivt, samt at det generelle niveau svarer til det aktuelle behov. Digitaliseringsstyregruppen godkender dispen-sationer og behandler sager. Er de væsentlige, skal kommunaldirektøren informeres.

- For alle systemer skal udpeges, så tæt på arbejdsgangen som muligt, en **systemejer** med ansvar for sikkerheden omkring aktivet. Digitaliseringsstyregruppen beslutter placering af ejerskab for fællessystemer.

- Alle **ledere** har ansvar for, at deres medarbejdere er bekendt med reglerne for anvendelse af udstyr, samt de systemer og data medarbejderen har adgang til i sin funktion, og at kravene til system- og datasikkerhed i lederens ansvarsområde er klart beskrevet.

- **Alle medarbejdere** har pligt til at sætte sig ind i udleverede regler og vejledninger om brug af kommunens it-faciliteter, at rapportere hændelser, trusler og sårbarheder, som medarbejderen bliver bekendt med, og at deltage aktivt i awareness-aktiviteter.

Inddragelse af topledelsen

Digitaliseringsstyregruppen skal rapportere status mindst en gang årligt til kommunaldirektøren. Kommunaldirektøren godkender på den baggrund, efter indstilling fra digitaliseringsstyregruppen og i samråd med direktionen, en ny årsplan for informationssikkerhed, herunder eventuel yderligere opfølgning eller kontrol.

Ved væsentlige brud på sikkerheden informerer digitaliseringschef kommunaldirektøren, som herefter behandler sagen.

Revidering af politikken

Den overordnede politik for informationssikkerhed revideres ved væsentlige ændringer og som minimum hvert fjerde år, når den nye kommunalbestyrelse er konstitueret efter et kommunalvalg.

Overtrædelser

Overtrædelser af den overordnede politik for informationssikkerhed eller andre bestemmelser, som er udmøntet heraf, betragtes som en sikkerhedshændelse. Alvorlige overtrædelser skal indgå i rapporteringen til øverste it-sikkerhedsansvarlig. Mindre alvorlige overtrædelser behandles af den medarbejderansvarlige leder.