Overordnet politik for informationssikkerhed for Rødovre Kommune

Denne politik er godkendt af kommunalbestyrelsen 24. april 2018
Ved udskrivning af politikken skal du være opmærksom på, at du anvender senest godkendte version.

Indledning

Kommunalbestyrelsen fastlægger med denne overordnede politik principper for opretholdelse af informationssikkerhed i Rødovre Kommune. I den overordnede politik er tidligere anvendt begrebet it-sikkerhedspolitik, mens der i denne overordnede politik anvendes begrebet 'informationssikkerhed', som anses for at være et bredere begreb, og dermed er bedre dækkende for det ansvar, som Rødovre Kommune har, og får skærpet når **persondataforordningen** træder i kraft den 25. maj 2018.

Den overordnede politik for informationssikkerhed beskriver, hvordan Rødovre Kommune vil beskytte systemer, data og informationer, som har stor betydning for kommunen eller andre, hvor kommunen er ansvarlig for forvaltningen af informationsaktiverne.

Rødovre Kommune anser det for centralt, at der er en god og effektiv sikkerhed i kommunen, som modsvarer den aktuelle risiko.

Det går ud over kommunens omdømme og påvirker borgernes tillid til kommunens forvaltning, hvis der ikke er styr på anvendelsen og driften af vores systemer.

Den overordnede informations-sikkerhedspolitik er opdelt i:

- 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 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, som beskriver risikohåndtering på udvalgte områder, med udgangspunkt i arbejdsprocesser, medarbejderpolitikker og tekniske og fysiske forhold. Retningslinjer fastlægges i relevante ledelsesfora og med inddragelse af fagforvaltninger og interessenter.
- Retningslinjer, som beskriver risikohåndtering på områder, der er fælles for alle medarbejdere i Rødovre Kommune, skal godkendes i direktionen.

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 fungerer korrekt.
- **Følsomme og 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.**

Politik for Informationssikkerhed

Standarderne ISO 27001og ISO 27002 (perondatabeskyttelsesforordningen pr. 25.5.2018) anvendes som reference og grundlag for informationssikkerhedsindsatsen, som i Rødovre Kommune skal opfylde 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 skal vedligeholdes ved løbende målinger og awarenessaktiviteter, og ved at integrere sikkerheds-overvejelser 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 og betydning for kommunen. Kritiske it-driftsprocesser skal være formaliseret og systematisk overvåget.

Adgang og rettigheder til data og systemer. Følsomme og kritiske informationsaktiver skal beskyttes mod uautoriseret adgang og ændring. Både kommunens egne og andres. Adgang til og ændring af følsomme eller kritiske systemer eller data skal kunne spores til personen. 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.

Fysisk sikkerhed. På steder, hvor der opbevares og anvendes informationer, systemer, infrastruktur og data, skal der etableres 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 etableres en parathed og et beredskab, så skaden ved kritiske hændelser holdes på et minimum og kommunens kritiske opgaver skal kunne videreføres i en nødsituation. Driftsmiljøet og vigtige arbejdsgange skal kunne videreføres inden for en af ledelsen besluttet tidshorisont. Sikkerhedshændelser skal 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, stillingsbeskrivelser mv.
I henhold til persondataforordningen skal nærmere definerede områder være tilgængelige for borgere og virksomheder.

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 it-sikkerhedsårsplan, som beskriver hvilke tiltag it-sikkerhedsorganisationen 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 informationssikkerhed. 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 informations-sikkerhed efter indstilling fra digitaliseringsstyregruppen.

- **Direktører** har inden for eget område ansvar for implementering og opfølgning på

efterlevelse af informations-sikkerhedspolitikken.

- **Digitaliseringschefen** varetager, med reference til digitaliseringsstyregruppen, it-sikkerhedskoordineringen og øvrige aktiviteter i henhold til sikkerhedsårsplanen, som aftales med styregruppen og godkendes af kommunaldirektøren. Digitaliseringschefen skal sikre, at informationssikkerhedsmæssige problemstillinger er tilstrækkelig klart belyst inden der træffes beslutninger om nye projekter eller ændringer. Det er digitaliseringschefens ansvar, at information til styregruppen og information og værktøjer til systemejere effektivt understøtter varetagelsen af deres 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, herunder at politikken og beslutninger er kendt på alle ledelsesniveauer og efterleves effektivt, samt at det generelle niveau svarer til det aktuelle behov. Digitaliseringsstyregruppen godkender dispensationer og behandler sager. Er de væsentlige, skal kommunaldirektøren informeres.

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

- **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 awarenessaktiviteter.

- 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.

Evaluering

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

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

Den overordnede politik for informationssikkerhed revideres hvert andet år, samt 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 og skal registreres. Alvorlige overtrædelser skal indgå i rapporteringen til øverste it-sikkerhedsansvarlig. Mindre alvorlige overtrædelser behandles af den medarbejderansvarlige leder. Digitaliseringsafdelingen skal orienteres om alle overtrædelser og digitaliseringsstyregruppen skal orienteres om principielle overtrædelser.