Kolding Kommune
en del af trekantområdet

Sammen designer vi livet

Kolding Kommunes politik for

Databeskyttelse og Informations-sikkerhed

Indhold

Forord

IT og Digitalisering er en integreret del af stort set alle Kolding Kommunes opgaver. Det skaber værdi i form af effektiv sagsbehandling og god borgerservice, men gør os også sårbar. Da vi samtidig befinder os i en verden præget af voksende usikkerhed, er det helt essentielt, at vi opprioriterer indsatsen for at beskytte vores informationer og vores it-systemer mod f.eks. hackerangreb og systemnedbrud.

Politik for Databeskyttelse og Informationssikkerhed udgør rammen for vores samlede arbejde med it- og informationssikkerhed. Her præciserer byrådet, hvordan rollerne og ansvaret er fordelt, hvilke overordnede principper og værdier organisationen skal arbejde ud fra, hvordan vi organiserer beredskabet i kritiske situationer, osv.

Politikken er det fundament, som vi har brug for til at manøvrere i en kompliceret verden, hvor vi konstant skal håndtere nogle svære balancer.

Hvis vi træder forkert, kan det få fatale følger. Det kan i yderste tilfælde koste liv og give alvorlige helbredsmæssige skader, hvis vi f.eks. ikke har styr på vores data i ældreplejen, det kan true forsyningssikkerheden, så vi ikke kan levere den service, som borgerne har krav på, det kan skade kommunens omdømme og gøre det svært at tiltrække dygtige medarbejdere og gode leverandører, osv.

Men samtidig må vi ikke falde i den modsatte grøft og blive så forsigtige og restriktive i vores brug af it-systemer, at vi ender med at være ineffektive og levere en dårlig service.

Med denne opdatering får Kolding Kommune en informationssikkerhedspolitik, som matcher tidens udfordringer. Politikken skal fremover gennemgås og ajourføres en gang årligt for at sikre, at organisationen kontinuerligt er klædt på til at varetage de sikkerhedshensyn, som er afgørende for en sikker, effektiv og brugervenlig forvaltning.

Politik for Databeskyttelse og Informations-sikkerhed

Politik for Databeskyttelse og Informationssikkerhed udgør den overordnede ramme for databeskyttelse, herunder men ikke begrænset til personoplysninger.

Formål

Adgang til velfungerende og sikker it er en fundamental forudsætning for, at Kolding Kommune kan levere en stabil og sikker serviceproduktion, som samtidig afspejler en god balance mellem fleksibilitet, effektivitet og sikkerhed.

Der skal etableres og vedligeholdes en afbalanceret Databeskyttelse og Informationssikkerhed, som omfatter alle nødvendige organisatoriske, fysiske og tekniske sikkerhedsforanstaltninger for at beskytte it-ressourcer og data mod alle former for trusler, interne eller eksterne, hændelige eller bevidste.

Formålet er at forhindre sikkerhedshændelser, der

- kan føre til tab af menneskeliv eller give alvorlige helbredsmæssige skader
- medfører risiko for personers rettigheder eller frihedsrettigheder
- medfører misligholdelse af væsentlige lovbestemte serviceforpligtelser
- truer forsyningssikkerheden
- påvirker kommunens omdømme negativt
- påvirker kommunens økonomiske forhold.

Gyldighed

Politik for Databeskyttelse og Informationssikkerhed og understøttende retningslinjer gælder for alle ansatte i Kolding Kommune, virksomheder med forretningsføreraftaler med Kolding Kommune, leverandører og øvrige private som offentlige samarbejdspartnere.

Politik for Databeskyttelse og Informationssikkerhed omfatter al anvendelse og adgang til Kolding Kommunes databærende informationssystemer.

Overordnede mål og principper

Arbejdet med Databeskyttelse og Informationssikkerhed i Kolding Kommune tager afsæt i god praksis for it-sikkerhed og følger principperne i ISO27000-standarden, som er en risikobaseret tilgang til styring af Databeskyttelse og Informationssikkerhed.

Databeskyttelse og Informationssikkerhed skal bevare fortrolighed, integritet og tilgængelighed af informationer og it-aktiver med en risikobaseret tilgang, hvor beskyttelsesniveauet og omkostningerne hertil skal være baseret på en forretningsmæssig risikovurdering og konsekvensanalyse.

Der er tre hovedmål for politikken:

- Fortrolighed: Beskyttelse af informationer og it-aktiver mod uautoriseret videregivelse eller adgang.
- Integritet: Beskyttelse af informationer og it-aktiver mod uautoriseret eller utilsigtet ændring eller ødelæggelse, samt sikring af informationernes nøjagtighed og pålidelighed.
- Tilgængelighed: Beskyttelse af relevante personers kontinuerlige adgang til informationer og it-aktiver.

Kolding Kommune ønsker et niveau for Databeskyttelse og Informationssikkerhed, der følger anerkendte branchestandarder og anbefalinger fra Center for Cybersikkerhed, Digitaliseringsstyrelsen og KL.

Lovgrundlaget for arbejdet med Databeskyttelse og Informationssikkerhed er Databeskyttelsesforordningen, Databeskyttelsesloven og på sigt den danske implementering af EU's NIS2-direktiv om at sikre et fælles højt sikkerhedsniveau på samfundskritisk kommunikationsinfrastruktur, it-systemer og digitale tjenester.

Der er tre hovedmål for politikken for Databeskyttelse og Informations-sikkerhed
- fortrolighed
- integritet
- tilgængelighed

Organisation og ansvar

Byrådet har det overordnede ansvar for Databeskyttelse og Informationssikkerhed i Kolding Kommune.

Direktionen er ansvarlig for styringsprincipperne og delegerer specifikke ansvarsområder for foranstaltninger, herunder ejerskab af datasikkerhed og informationssystemer.

Informationssikkerhedsudvalget godkender de understøttende retningslinjer for, hvordan politikken udmøntes i praksis.

Ejerskab fastsættes for hvert databærende informationssystem, herunder teknisk infrastruktur, fagsystemer og data. Ejeren fastlægger hvorledes passende tekniske og organisatoriske foranstaltninger implementeres og administreres i overensstemmelse med Politik for Databeskyttelse og Informationssikkerhed. Ejeren accepterer og tager ansvar for risici og konsekvenser.

IT og Digitalisering rådgiver, koordinerer, kontrollerer og rapporterer om status på databeskyttelsen og informationssikkerheden. Informationssikkerhedsorganisationen udarbejder hertil understøttende retningslinjer og procedurer.

Den enkelte medarbejder er ansvarlig for at overholde Politik for Databeskyttelse og Informationssikkerhed og er informeret herom på Intranettet og i bilag til ansættelsesbrevet.

Risikostyring

Kolding Kommunes tilgang til risikostyring er baseret på relevante principper fra ISO27000 og har til formål at sikre, at de rette ledelseslag i kommunen systematisk og løbende forholder sig til og træffer beslutning om risici vedrørende Databeskyttelse og Informationssikkerhed og tager ejerskab af afledte konsekvenser.

Præsenteret for en konkret risiko er det ledelsens opgave at vurdere sandsynlighed og konsekvens ved risikoen og lægge de overordnede rammer for risikohåndteringen ud fra en af følgende strategier: accept, mitigering (formindskelse), overføring eller eliminering af risiko.

Når risikovilligheden skal fastlægges skal følgende hensyn tilgodeses og balanceres:

- Hensynet til den registrerede og dennes rettigheder.
- Kvalitet i borgerbetjening eller anden kerneydelse.
- Effektivitet i opgaveløsningen.
- Kommunens samlede informationssikkerhed.
- Økonomi og ressourcer.

Kolding kommune udarbejder som dataansvarlig en konsekvensanalyse, når en behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Konsekvensanalyser udarbejdes forud for, at databehandlingen igangsættes.

Sikkerheds-hændelser

Sikkerhedshændelser er hændelser, hvor kommunens informationssystemer i en periode har haft en lavere sikkerhed end normalt og/eller hændelser, der har medført et tab af fortrolighed, integritet eller tilgængelighed af kritiske forretningsdata, herunder også persondata.

Sikkerhedshændelser og brud på persondatasikkerheden rapporteres via intranettet.

Beredskab

Der forefindes beredskabsplaner for alle kritiske systemer og infrastruktur, herunder nødprocedurer og planer for genopretning.

Beredskabsplanerne revideres regelmæssigt og afprøves i praksis.

Informations-sikkerhedskultur

Medarbejdernes viden og adfærd i dagligdagen har stor betydning for kommunens samlede Databeskyttelse og Informationssikkerhed. Derfor skal alle medarbejdere i kommunen efterleve de retningslinjer, vejledninger, instrukser m.m., som er relevante i forhold til den enkeltes funktion, rolle og arbejdsopgaver.

Det er personaleledernes ansvar i samarbejde med informationssikkerhedsorganisationen, at medarbejderne gennemfører uddannelses- og træningsaktiviteterne og i deres daglige arbejde bidrager til en god sikkerhedskultur i kommunen.

Medarbejdernes viden og adfærd i dagligdagen har stor betydning for kommunens samlede databeskyttelse og informations-sikkerhed

Dispensation

Dispensationer til Kolding Kommunes Politik for Databeskyttelse og Informationssikkerhed og retningslinjer godkendes af Informationssikkerhedsudvalget.

Rapportering

Formanden for Informationssikkerhedsudvalget informerer Direktionen om alle væsentlige sikkerhedshændelser.

IT og Digitalisering udarbejder årligt en informationssikkerhedsstatus inkl. godkendte dispensationer, som behandles af Direktionen og rapporteres til Byrådet.

Overtrædelse og sanktioner

Alle medarbejdere er forpligtet til at følge den gældende politik for Databeskyttelse og Informationssikkerhed, herunder retningslinjer, forretningsgange og relaterede bilag. Den nærmeste leder har ansvaret for at håndtere overtrædelse af informationssikkerhedsreglerne.

Forsætlig overtrædelse, groft uansvarlig adfærd og misbrug rapporteres til HR-afdelingen og nærmeste leder. Overtrædelse af Politik for Databeskyttelse og Informationssikkerhed eller understøttende retningslinjer kan få ansættelsesretlige konsekvenser.

Godkendelse og revision

Kolding Kommunes Politik for Databeskyttelse og Informationssikkerhed forvaltes af IT og Digitalisering, som har ansvar for opfølgning og revision. Politikken er et levende dokument, der revurderes og godkendes årligt i henhold til det aktuelle trusselsniveau og kommunens modenhed.

Kolding Kommunes Politik for Databeskyttelse og Informationssikkerhed godkendes af Byrådet og træder i kraft samme dato. Redaktionelle ændringer, som ikke ændrer grundlæggende ved Politik for Databeskyttelse og Informationssikkerhed kan dog godkendes af Informationssikkerhedsudvalget. Tilsvarende gælder ændringer affødt af Byrådets beslutninger, der medfører, at der skal laves konsekvensrettelser i Politik for Databeskyttelse og Informationssikkerhed.

Politikken er senest godkendt 20. dec. 2022.

K

Politik for **Databeskyttelse og Informationssikkerhed**

Grafisk design: Kommunikationsafdelingen, Kolding Kommune

Centralforvaltningen
IT og Digitalisering
Telefon 7979 2211
infosik@kolding.dk

Kolding Kommune
en del af trekantområdet

Sammen designer vi livet