FAXE KOMMUNE

Informationssikkerheds-

og Datapolitik

Formål
Dette dokument beskriver Faxe Kommunes overordnede Informationssikkerheds- og Datapolitik.

Formålet med politikken er, at fastlægge det overordnede sikkerhedsniveau for behandling af informationer og beskyttelse af data om borgere, virksomheder, samarbejdspartnere, ansatte, brugere, politikere og andre med en relation til Faxe Kommune.

Kommunen er dataansvarlig for de oplysninger, som indhentes, anvendes og behandles samt for, at sikkerhedsniveauet for beskyttelse af informationsbehandling og data altid efterlever de til enhver tid gældende lovkrav. Politikken skal sikre, at informationsbehandlingen og databeskyttelse opfylder alle sikkerhedskriterier, som forventes opfyldt af en offentlig forvaltning,

Dette skal ske ved, at der foretages en løbende risikovurdering, som tager udgangspunkt i at alle tiltag skal være realistiske, operationelle, logiske og kontrollerbare. Kommunen skal satse på sikre løsninger med høj driftsstabilitet, brugervenlighed og informationsløsninger som er integrerede.

Politikken skal medvirke til at danne grundlag for, at digitaliseringsstrategien og de konkrete handleplaner kan effektueres.

Politikken fastsætter de nødvendige organisatoriske rammer, herunder placering af ansvar for varetagelse af informationssikkerhed og databeskyttelse.

På baggrund af den vedtagne politik, bliver der udarbejdet en Informationssikkerhedshåndbog. Informationssikkerhedshåndbogen tager udgangspunkt i principperne fra ISO 27001 standarden og skal sikre, at politikken og lovgivningen indarbejdes i administrationens arbejdsgange.

Politikken, Informationssikkerhedshåndbogen og en løbende risikovurdering skaber sammen rammerne for arbejdet med informationssikkerhed og databeskyttelse.

Godkendelse og kommunikation af politikken.
Informationssikkerheds- og datapolitikken skal godkendes politisk.

Center for HR, Økonomi & IT, udarbejder herefter Informationssikkerhedshåndbogen, der skal sikre, at alle brugere af Faxe Kommunes informationer og informationsaktiver ved hvordan de skal omsætte politikken i praksis i forhold til deres konkrete arbejdsopgaver og ved brug af informationsaktiverne.

Informationssikkerhedshåndbogen godkendes af direktionen.

Politikken og Informationssikkerhedshåndbogen skal være tilgængelige på kommunens intranet. Politikken skal kommunikeres til alle relevante interessenter, herunder alle medarbejdere ansat i Faxe Kommune, byrådsmedlemmer og samarbejdspartnere.

Informationssikkerhedshåndbogen skal kommunikeres til alle relevante interessenter herunder særligt medarbejdere, som benytter Faxe Kommunes informationsaktiver. Et informationsaktiv er ethvert aktiv, hvor der opbevares og/eller behandles informationer og data – f.eks. IT-systemer, servere, netværkskomponenter, software, samt fysiske aktiver som PC, printere og dokumenter.

En effektiv og konsekvent formidling af politikken og informationssikkerhedshåndbogen skal skærpe brugernes opmærksomhed på sikkerhed i forbindelse med anvendelse af de forskellige systemer ligesom politikken skal sikre, at alle brugere er beskyttet af et entydigt regelsæt.

Ansvaret for at formidle politikken og informationssikkerhedshåndbogen ligger hos de personaleansvarlige ledere.

Implementering og efterlevelse af politikken.
Det samlede informationssikkerhedsniveau er resultatet af, hvordan brugerne bidrager til en sikker behandling af data og brug af informationsaktiver.

Kommunens ansatte skal være bevidste om deres betydning for IT-sikkerheden i Faxe Kommune. Der skal være udfærdiget sikkerhedsmæssige regler for personalet, som dels skal beskytte kommunen og borgerne mod skader forvoldt af personalet og dels skal beskytte personalet mod ubegrundet mistanke om misbrug og sikkerhedsbrud.

Det er således vigtigt at politikken, informationssikkerhedshåndbogen og sikkerhedsniveauet er målrettet de konkrete opgaver, som kommunen udfører.

For IT-driftspersonale og andet personale med udvidede rettigheder til systemer, skal der være skærpede regler og sikkerhedsinstrukser.

Ansvaret for at efterleve sikkerheden omkring informationsbehandling og databeskyttelse er placeret hos den enkelte medarbejder.

Hvis en medarbejder opdager trusler imod kommunens informationsbehandling eller er bekendt med overtrædelser af politikken eller informationssikkerhedssikkerhedshåndbogen, skal dette altid meddeles til Databeskyttelsesrådgiveren.

Politikkens omfang.
Politikken gælder for alle medarbejdere i kommunen samt byrådsmedlemmer, samarbejdspartnere herunder virksomheder, private og selvejende institutioner, som udfører opgaver for kommunen.

Politikken omfatter alle kommunens forretningsgange, systemer og data i kommunens besiddelse, herunder oplysninger om borgere, virksomheder, kommunens finansielle og økonomiske forhold samt andre informationer, som kræver beskyttelse eller har væsentlig betydning for kommunen.

Politikken gælder for al anvendelse af Faxe Kommunes informationsaktiver og er således gældende for enhver information og alle data, som behandles af kommunen uanset på hvilket medie informationen er gemt.

Politikken vedrører den samlede administrative systemanvendelse, det samlede informationsflow og al databehandling. Systemer og data må udelukkende anvendes til udførelse af de relevante arbejdsopgaver og systemer og data skal beskyttes i overensstemmelse med deres indhold og følsomhed.

Som bruger af Kommunes systemer og data, er alle medarbejdere således forpligtet til at følge politikken og Informationssikkerhedssikkerhedshåndbogen.

Politikkens mål.
Det er politikkens mål, at sikre, at informationssikkerheden og databeskyttelse etableres på et effektivt og ensartet niveau, så risikoen for alvorlige fejl begrænses. Dette sikres bl.a. ved at informationssikkerheden indarbejdes i de eksisterende forretningsgange og at ansvaret er entydigt placeret.

Ved anskaffelse, implementering, opbevaring og brug af informationsaktiver foretages der i det enkelte tilfælde en risikobaseret vurdering, under hensyntagen til arbejdets gennemførelse, efterlevelse af lovgivningen samt økonomiske og personalemæssige ressourcer. Målsætningen om

et højt sikkerhedsniveau afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af IT, der bl.a. gennem digitalisering og integrationer, skal sikre effektive arbejdsgange.

Ved arbejdet med informationssikkerhed og databeskyttelse, skal der være særligt fokus på at sikre følgende:

- Fortrolighed
- Forretningssikkerhed og tilgængelighed
- Integritet
- Dataminimering
- Ansvar for data og sikkerhed
- Registreredes rettigheder.
- Risikobaseret betragtning

Fortrolighed:
Medarbejdere og samarbejdspartnere skal instrueres i lovens regler om fortrolighed.
Følsomme og fortrolige data skal sikres forsvarligt og lovligt uanset om de forefindes digitalt eller i papirform. Der skal indhentes fornødne fortrolighedserklæringer og informeres om straffelovens regler ved overtrædelse af de til enhver tid gældende lovregler om fortrolighed.
Vi skal sikre fortrolig behandling, transmission og opbevaring af data, hvor kun autoriserede brugere har adgang. Risici skal forbygges gennem klar funktionsadskillelse, herunder autorisation, udførelse og kontrol.

Forretningssikkerhed og tilgængelighed:
Data og værdier må ikke gå tabt. Data må ikke være tilgængelige for uvedkommende.
Vi skal sikre, at alle generelle grundlæggende forretningskritiske systemer fungerer og understøtter kommunens drift. Vi skal gennem bl.a. Serviceaftaler med leverandørerne opnå høj driftssikkerhed og tilgængelighed med høje oppetider på systemer og minimeret risiko for nedbrud. Vi skal afsætte ressourcer til, at medarbejderne uddannes på højt niveau i brug af alle systemer. Vi skal sikre, at data opbevares de rigtige steder og på denne måde bliver tilgængelige for alle relevante medarbejdere. Vi skal gennem integrationer mellem de enkelte systemer sikre, at dataflow automatiseres mest muligt.

Integritet:
Datagrundlaget for kommunens forretningsgange skal være retvisende:
Vi skal derfor opnå en pålidelig og korrekt funktion af informationssystemerne med minimeret risiko for ukorrekt datagrundlag, for eksempel som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.

Dataminimering:
Vi må ikke indhente eller opbevare flere data, end vi har brug for til løsning af en arbejdsopgave.
Vi skal gennem uddannelse af medarbejderne og procedurer for anskaffelse af nye systemer sikre, at vi ikke indhenter flere data end der er behov til løsning af den konkrete arbejdsopgave.
Vi skal gennem autorisationen til data på alle informationsaktiver sikre, at medarbejderne ikke har adgang til data, som de ikke har brug for til løsning af en arbejdsopgave.

Ansvar for data og sikkerhed:
Der skal være hjemmel til behandling af data.
Det skal besluttes, hvor/hvordan data opbevares sikkert vedr. løsning af konkrete arbejdsopgaver.
Ved indgåelse af ethvert samarbejde med en ekstern leverandør og med andre myndigheder, skal vi klarlægge hvem der har ansvaret for behandling af data og beskrive, hvordan data sikres bedst muligt. Der skal indgås de fornødne databehandleraftaler.

Kommunen er ansvarlig for, at der er hjemmel til at indhente og behandle data, der opbevares af

kommunens medarbejdere og i kommunens informationsaktiver. Det er lederens ansvar at instruere medarbejderne i hvor data må opbevares og behandles samt sikre, at medarbejderne ikke opbevarer private data i kommunens systemer.

Registreredes rettigheder:
Når kommunen registrerer personoplysninger i et informationsaktiv, har den registrerede en række rettigheder vedr. disse oplysninger.
Vi skal gennem uddannelse sikre, at alle medarbejdere kender de registreredes rettigheder.
Vi skal gennem tekniske og organisatoriske tiltag sikre, at vi implementerer de registreredes rettigheder i vores arbejdsgange så vi efterlever Databeskyttelsesforordningens princip om "Protection By Design".

Risikobaseret betragtning:
Informationssikkerheden og databeskyttelsen skal tilpasses de værdier og informationer, som skal beskyttes.
Al data behandles ud fra en risikobaseret betragtning. Det betyder, at der skal foretages risikoanalyse og risikovurdering dels inden anskaffelse af nye systemer og dels løbende af konkrete arbejdsgange.

Lokationer, der indeholder informationsaktiver, skal sikres forsvarligt mod vand, brand og indbrud.

Der skal foretages beredskabsstyring på særligt kritiske arbejdsprocesser og de systemer, der understøtter disse arbejdsprocesser. Formålet er at imødegå og begrænse konsekvenser af sikkerhedsbrud mest muligt samt sikre hurtig genetablering af kommunens sagsbehandling efter forekomst af kritiske hændelser som f.eks. oversvømmelse, brand, IT-nedbrud, hackerangreb eller virus.

Organisering og ansvar
Ansvaret for informationssikkerheden i kommunen ligger hos den sikkerhedsansvarlige direktør.
Arbejdet med sikkerhedspolitikkens vedligeholdelse og implementering/efterlevelse er forankret i Center for HR, Økonomi & IT og i Direktionssekretariatet.
Faxe Kommunes Databeskyttelsesrådgiver vejleder i lovgivningen, politikken og i Informationssikkerhedshåndbogen. Databeskyttelsesrådgiveren hjælper med at implementere lovgivningen, politikken og Informationssikkerhedshåndbogen i eksisterende arbejdsgange og påser om de er overholdt ved udarbejdelse af procedurer, anskaffelse af nye systemer samt om sikkerhedsbrud giver anledning til evaluering af de understøttende regler.

Datebeskyttelsesrådgiveren har ansvaret for sammen med fagdirektører at vurdere, om der ud fra en risikobaseret betragtning skal gives dispensation fra Informationssikkerhedshåndbogen i konkrete tilfælde.

Herudover har en række andre centrale aktører forskellige ansvar i forhold til de enkelte områder inden for politikken. Ansvaret beskrives i Informationssikkerhedshåndbogen og understøttende procedurer.

De væsentligste aktører og deres overordner ansvarsområder er beskrevet her:

Ansvarlig	Placering og forklaring	Ansvarsområder
Byrådet	Overordnet ansvarlig for en hensigtsmæssig og betryggende informationssikkerhed	Byrådet skal godkende den overordnede informationssikkerheds- og datapolitik. Løbende ændringer kan godkendes af Økonomiudvalget. Ved den fastlagte periodiske evaluering, skal politikken behandles af Byrådet.
Den sikkerhedsansvarlige direktør	Er den øverste sikkerhedsansvarlige for informationssikkerheden og databeskyttelse i Faxe Kommune.	Ansvarlig for den overordnede tilrettelæggelse af informationssikkerheden i kommunen og for opfølgning og kontrol. Opgaverne kan uddelegeres til en centerchef eller leder på IT-sikkerhedsområdet. Ansvaret kan ikke uddelegeres.
Direktionen	Direktionen skal godkende Informationssikkerhedshåndbogen.	Kommunens øverste ledelse skal støtte informationssikkerheds- og datapolitikken ved at udlægge klare retningslinjer, udvise synligt engagement samt sikre en præcis placering af ansvar.
Databeskyttelsesrådgiveren (DBR)	Er uafhængig af organisationen og skal understøtte Byrådet med at kontrollere om politikken overholdes.	Ansvarlig for at rådgive om brug af politikken og Informationssikkerhedshåndbogen. Skal behandle manglende overholdelse som en sikkerhedshændelse og informere ledelsen.
Center for HR, Økonomi & IT	Ansvarlig for at sikre den tekniske implementering og drift af informationssikkerheds- og datapolitikken	Ansvarlig for at sikre den tekniske implementering og drift af informationssikkerheds- og datapolitikken generelt og i de systemer, som centeret har ansvaret for. Skal bistå med rådgivning omkring IT-forhold i politikken. Skal bistå med opfølgning på efterlevelse af politikken.
Direktionssekretariatet	Ansvarlig for undervisning i regler om databeskyttelse og give sparring til DBR	Ansvarlig for at rådgive og undervise organisationen om databeskyttelse og i samarbejde med Center for HR, Økonomi & IT samt DBR koordinere undervisning og rådgivning i databeskyttelse og informationssikkerhed.
Centerchefer	Ansvarlig for at politikken implementeres i eget center.	Ansvarlig for, at implementere politikken og Informationssikkerhedshåndbogen i centerets arbejdsgange, herunder at alle medarbejdere uddannes tilstrækkeligt i forhold til løsning af deres arbejdsopgaver. Skal sikre, at der udarbejdes organisatoriske tiltag til beskyttelse af data.
Ledere	Ansvarlig for at den enkelte medarbejder bliver bekendt med relevante regler inden de får adgang til informationsrelaterede aktiver eller data.	Ansvarlig for at alle medarbejdere ved hvilke regler, der er relevante for dem og at alle medarbejdere ved hvor de kan læse politikken og sikkerhedshåndbogen. Ansvarlig for at evt. tvivlsspørgsmål afklares hurtigst muligt (evt. med DBR) og at der løbende følges op på reglerne ved evt. sikkerhedsbrud i afdelingen. Minimum to gange om året på personalemøde gennemgå relevante regler og evt. pjecer/vejledninger om de vigtigste emner for afdelingen.

Ledere (fortsat)		Ansvarlig for at instruere medarbejderne i, hvor data må opbevares og behandles samt sikre, at medarbejderne ikke opbevarer private data i kommunens systemer.
Medarbejdere	Ansvarlig for at læse de regler, som deres leder finder relevante for dem.	Skal sørge for altid at holde sig opdateret om reglerne. Er ansvarlig for at følge politikken og sikkerhedshåndbogen. Skal udvise sikker adfærd vedr. informationssikkerhed og databeskyttelse i forhold til de konkrete ansvarsområder og arbejdsopgaver og ved brug af informationsaktiver.
Dataejere	Udpeges af systemejer Skal være en fagchef/teamleder, der er ejer af delproces og har personaleansvar for medarbejdere i processen. Der kan være flere dataejere for hvert system.	Dataejeren har ansvaret for, at retningslinjer og instrukser for anvendelse af et system bliver overholdt af medarbejderne. Dataejer skal føre tilsyn og kontrol med, at retningslinjer og instrukser følges.
Systemejere	Alle systemer tilhører en systemejer. Systemejer er enten direktør eller centerchef. En systemejer har det faglige ansvar for de opgaveløsninger, som systemet understøtter. Opgaven som systemejer kan uddelegeres helt eller delvist. Ansvaret kan ikke uddelegeres. Et system kan kun have én systemejer.	Ansvarlig for sikkerheden omkring systemet og for at sikre, at der bliver udarbejdet, implementeret og vedligeholdt følgende for det enkelte system: procedurebeskrivelser for adgangsstyring, risikoanalyser og beredskabsplaner instrukser, uddybende systemdokumentation, interne kontroller herunder logning og evt. databehandleraftale. Ansvarlig for at der indgås tilstrækkelig supportaftale, udpeges budgetansvarlig, dataejer og systemadministrator. Ansvarlig for at interne procedurer vedr. godkendelse af systemer følges ved indkøb, tilkøb, test, udvikling og forlængelse af aftaler.
Systemadministratorer	Navngiven systemadministrator – typisk en medarbejder med særligt kendskab, som har ansvaret for at udføre opgaver uddelegeret af systemejer. Rollen kan underopdeles i flere roller.	Ansvarlig for supplerende opgaver i forbindelse med systemanvendelsen for det enkelte system. Det skal beskrives for hvert system, hvilke opgaver der ligger hos systemadministrator. Kan være ansvarlig for autorisation, logning, interne kontroller, udvikling, etablering af systemsupport, udarbejdelse af instrukser, uddybende systemdokumentation og administration af leverandøradgang.
Det enkelte Byrådsmedlem	Ansvarlig for at læse de regler, som er relevante for dem.	Ansvarlig for at følge politikken og sikkerhedshåndbogen og udvise sikker adfærd i forhold til informationssikkerhed og databeskyttelse i sammenhæng med de konkrete ansvarsområder og arbejdsopgaver og brug af informationsaktiver.
Samarbejdspartnere	Ansvarlig for at læse de regler, som ifølge samarbejdsaftalen er relevante for dem.	Hvis det er aftalt, at politikken og dele af sikkerhedsbogen er gældende for samarbejdet, skal samarbejdspartneren søger for at sætte sig ind i de relevante bestemmelser.

Sikkerhedsbrud
Der er etableret en procedure for håndtering af brud på informationssikkerheden og reglerne om databeskyttelse. Proceduren sikrer, at DBR og IT-Servicedesk informeres umiddelbart, så der iværksættes de nødvendige forholdsregler for at bringe problemet til ophør og forebygge lignende problemer.
DBR sikrer, at ledelsen involveres og informeres samt at der rapporteres til relevante myndigheder og evt. berørte borgere og virksomheder. DBR følger op på årsagerne til sikkerhedsbruddet og involverer ledelsen i nødvendigt omfang.

DBR samarbejder med ledelsen om at sikre nødvendig information i forhold til at håndtere evt. personaleretlige konsekvenser ved overtrædelse af politikken og sikkerhedshåndbogen. DBR rådgiver ikke i forhold til personaleretlige spørgsmål.

Økonomiudvalget informeres løbende om de registrerede sikkerhedsbrud.

Det skal derfor fremhæves, at overtrædelse af Informationssikkerhedspolitikken samt relaterede bilag, efter omstændighederne, kan medføre sanktioner.

Opfølgning og kontrol
Der føres løbende kontrol med informationssikkerheden og beskyttelse af data, herunder om lovgivning og interne regler og retningslinjer følges samt om iværksatte sikringstiltag virker.

Mindst hver andet år gennemføres en systematisk kontrol af informationssikkerheden.

Byrådet informeres årligt om udfordringer og nye tiltag vedr. informationssikkerhed og beskyttelse af data gennem DBRs årsrapport.
Byrådet forelægges årligt IT-revisionens rapport vedr. Faxe Kommunes informationssikkerhed.

Vedligeholdelse og godkendelse
Den sikkerhedsansvarlige direktør sikrer, at informationssikkerhedshåndbogen løbende opdateres og vedligeholdes.

Politikken skal revideres ved lovændringer og væsentlige organisatoriske ændringer, som kan have betydning for ansvarsfordelingen i forhold til politikken.

For at sikre en levende og ajourført informationssikkerhedshåndbog udarbejdes et årshjul vedr. informationssikkerhed og beskyttelse af data.
Følgende ting skal som minimum være en del af årshjulet:

- opfølgning på sikkerhedsbrud i systemer
- revisionserklæringer fra leverandører
- intern IT-revision
- oversigt over systemer – oversigt skal bl.a. indeholde oplysninger systemejer, systemadministrator, dataejer og budgetansvarlig.
- DBRs årsrapport, herunder opfølgning på efterlevelse af sikkerhedshåndbogen
- Evaluering af risikoanalyser

Årshjulet kan indeholde ting som kun skal foretages hvert andet år.

Øverste sikkerhedsansvarlige har ansvaret for, at denne opfølgning foretages mindst en gang om året eller ved større tekniske eller organisatoriske ændringer. Opfølgningen kan evt. foretages med ekstern bistand.

Denne politik er vedtaget af Faxe Kommunes Byråd.