Ikast-Brande Kommune

Informationssikkerhedspolitik

Behandlet i Byrådet den 20. marts 2023

Indholdsfortegnelse

1. Indledning

Denne informationssikkerhedspolitik er den overordnede ramme for informationssikkerheden hos Ikast-Brande Kommune.

Politikken understøtter Ikast-Brande Kommunes værdigrundlag:

Dialog, Tillid og Ansvarlighed

Som et led i den overordnede sikkerhedsstyring tager Teknik- og Stabsdirektøren på grundlag af den løbende overvågning og rapportering informationssikkerhedspolitikken op til godkendelse ved hver ny byrådsperiode.

Derudover bliver informationssikkerhedspolitikken revideret én gang årligt af informationssikkerhedskoordinatoren.

Referencer

- Persondataloven (Lov nr 429 af 31/05/2000)
- Databeskyttelsesforordningen (Europa-Parlamentets og Rådets forordning (EU) 2016-679 af 27. april 2016)
- Databeskyttelsesloven (Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven))
- Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000
- Statsministeriets sikkerhedscirkulære (CIR nr. 204 af 07/12/2001)

- Informationsteknologi – Sikkerhedsteknikker – Ledelsessystemer for informationssikkerhed – Krav, ISO 27001 (4. udgave 2013-12-10).
- National Standard for Identiteters Sikringsniveauer (NSIS), Version 2.0.2

2. Formål

Informationer og informationssystemer er nødvendige og vigtige for Ikast-Brande Kommune. Informationssikkerheden har vital betydning for Ikast-Brande Kommunes troværdighed og funktionsdygtighed.

Formålet med informationssikkerheden er at definere en ramme for beskyttelse af Ikast-Brande Kommunes informationer og særligt at sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres *fortrolighed, integritet og tilgængelighed*.

Informationssikkerhedspolitikken uddybes i regler og procedurer. Disse samles i informationssikkerhedshåndbogen som ligeledes indeholder beredskabsplaner og risikovurderinger.

Ikast-Brande Kommunes beskyttelsesniveau er udarbejdet efter ISO 270001 standarden[1] og gældende lovgivning.

Den nærmeste personaleansvarlige leder skal oplyse medarbejderne om ansvarlighed i relation til Ikast-Brande Kommunes informationer og informationssystemer.

Hensigten med informationssikkerhedspolitikken er at tilkendegive over for alle, som har en relation til Ikast-Brande Kommune, at anvendelse af informationer og informationssystemer er underkastet standarder og regler.

På den måde kan sikkerhedsproblemer forebygges, eventuelle skader kan begrænses, og reetablering af informationer kan sikres.

3. Målsætninger

Ikast-Brande Kommune bestræber sig på, at følge disse målsætninger i arbejdet med informationssikkerhed og beskyttelse af de registreredes privatliv ved behandling af personoplysninger.

- Kritiske informationssystemer skal være identificeret og forsvarligt beskyttet mod brud på *fortrolighed, integritet* og *tilgængelighed.*
    - Med *fortrolighed* menes, at person- og værdioplysninger i alle tilfælde kun er tilgængelige for de medarbejdere, systemer eller eksterne parter, der har et lovligt arbejdsbetinget behov for at have adgang til disse.
    - Med *integritet* menes, at person- og værdioplysninger i alle tilfælde er valide og med garanti for, at data ikke er manipulerede.
    - Med *tilgængelighed* menes, at det skal være muligt at tilgå systemer og data for autoriserede personer, når det er nødvendigt.

[1] https://www.digst.dk/sikkerhed/informationssikkerhed-i-myndigheder/nye-styrelsers-implementering-af-iso-27001/

- Risici skal nedbringes til et kendt og acceptabelt niveau, og det skal sikres, at gældende lovgivning til enhver tid overholdes.
- Kommunens niveau for sikkerhed fastlægges ved brug af periodisk gennemførte risikovurderinger, samt ved risikovurderinger, der gennemføres ved anskaffelser og ændringer af IT-systemer og ved ændringer af IT-miljøet, systemerne opererer i.
    - Risikovillighed
      Informationssikkerhedsniveauet skal være bestemt ud fra Ikast-Brande Kommunes aktuelle risikoniveau for henholdsvis databeskyttelse og informationssikkerhed. Dog går hensynet til overholdelse af gældende lovgivning, herunder den registreredes retsstilling og rettigheder, forud for hensynet til kommunens økonomiske og ressourcemæssige indsats for opnåelse af det besluttede risikoniveau.
- Der er udarbejdet et beredskab, der sikrer, at *vitale* informationssystemer kan retableres rettidigt i tilfælde af katastrofe, og der skal fastsættes maksimalt acceptable tider for utilgængelighed for så vidt angår disse IT-systemer. Der skal endvidere udarbejdes, vedligeholdes og afprøves beredskabsplaner, der sikrer nøddrift, eskalering, reetablering og genoptagelse af normal drift i tilfælde af større nedbrud, ulykker eller katastrofer i forhold til kritiske IT-systemer.

Ikast-Brande Kommune efterlever principperne i:

- ISO27001: 'Information technology – Security techniques – Information security management systems – Requirements', som er en international ledelsesstandard for informationssikkerhed, der sikrer styringen af den nødvendige beskyttelse af værdifulde data.

samt kravene til sikringsniveau i:

- National Standard for Identiteters Sikringsniveauer (NSIS) version 2.0.2, hvis formål er, at skabe rammer for tillid til digitale identiteter samt digitale ID-tjenester.

4. Omfang, organisation og ansvar

Informationssikkerhedspolitikken omfatter alle Ikast-Brande Kommunes informationer uanset hvilken form de opbevares og formidles på (papir, elektronisk og/eller mundtlige), herunder informationer, som ikke tilhører Ikast-Brande Kommune, men som Ikast-Brande Kommune kan gøres ansvarlig for[2].

Denne politik gælder for alle ansatte uden undtagelse, både fastansatte og personer, som midlertidigt arbejder for Ikast-Brande Kommune. Alle disse personer bliver her betegnet som "medarbejderne".

[2] Dette inkluderer f.eks. alle data om personale, data om finansielle forhold, data, som bidrager til administrationen af Ikast-Brande Kommune, produktionsdata og anlægsdata samt informationer, som er overladt Ikast-Brande Kommune af andre. Disse data kan være faktuelle oplysninger, optegnelser, registreringer, rapporter, forudsætninger for planlægning eller enhver anden information, som kun er til intern brug.

Alle leverandører, samarbejdspartnere og politikere, som har fysisk eller logisk adgang til Ikast-Brande Kommunes systemer, data og informationer skal gøres bekendt med informationssikkerhedspolitikken og følge den.

Byrådet i Ikast-Brande Kommune har det overordnede ansvar for informationssikkerhed og beskyttelse af de registreredes privatliv ved behandling af personoplysninger i Ikast-Brande Kommune.

Direktionen er ansvarlig for de styringsprincipper, der skal understøtte formålet med og målsætningerne i informationssikkerhedspolitikken. Direktionen delegerer beslutningskompetencen til informationssikkerhedsudvalget mht. specifikke ansvarsområder for beskyttelsesforanstaltninger, herunder ejerskab af informationssystemer, implementering af principper og relevante og tilstrækkelige kontroller i Ikast-Brande Kommune.

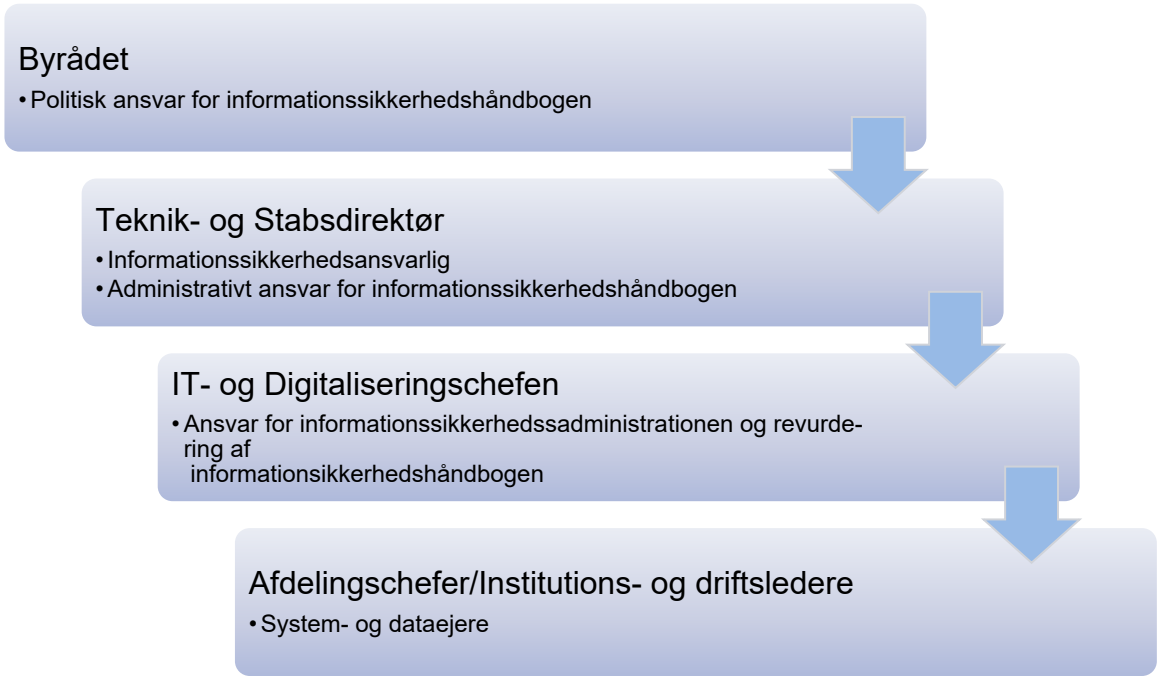
Ejerskab fastsættes for hvert vitalt og kritisk informationssystem. Ejerskabet vil være knyttet op på en system- og dataejer. System- og dataejer fastlægger hvorledes sikkerhedsforanstaltninger anvendes og administreres i overensstemmelse med informationssikkerhedspolitikken, herunder klassifikation af data i systemet.

Den informationssikkerhedsansvarlige koordinerer sikkerhedsarbejdet på tværs af organisationen og GDPR-organisationen samt har ansvaret for, at der gennemføres kontroller og rapporteringer om sikkerhedsarbejdet. Endvidere skal den informationssikkerhedsansvarlige sikre at der udarbejdes understøttende retningslinjer der gælder på tværs af direktørområderne iht. ovennævnte standarder.

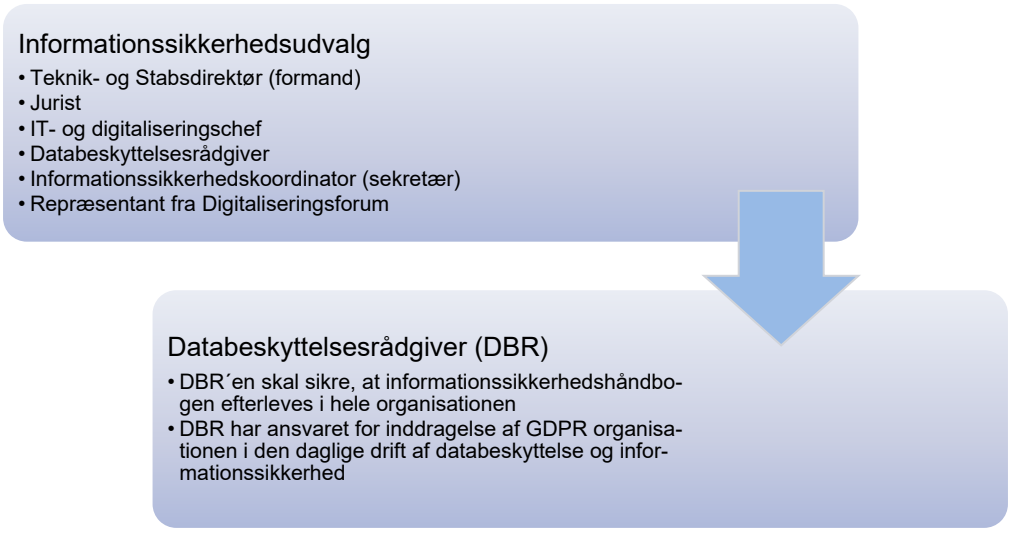
IT-afdelingen og databeskyttelsesrådgiveren rådgiver og understøtter den informationssikkerhedsansvarlige i koordinering, kontrol og afrapporteringer om sikkerhedsarbejdet.

Databeskyttelsesrådgiveren er i kommunen en uafhængig funktion, der fungerer som kommunens rådgiver og tilsynsfunktion på området. Databeskyttelsesrådgiveren skal inddrages og rådføres om overholdelse af de databeskyttelsesretlige regler. Databeskyttelsesrådgiveren rapporterer direkte til kommunens øverste politiske ledelsesniveau, som er byrådet i Ikast-Brande Kommune.

Ansvarsorganisation for I-sikkerheden ved Ikast-Brande Kommune



Driftsorganisation for informationssikkerheden ved Ikast-Brande Kommune



Ansvarsområder for driftsorganisationen fremgår af "Forretningsorden for Informationssikkerhedsudvalget".

5. Sikkerhedsbevidsthed

Informationssikkerhed vedrører Ikast-Brande Kommunes samlede informationsflow, og gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at bidrage til at beskytte Ikast-Brande Kommune informationer mod uautoriseret adgang, ændring og ødelæggelse samt tyveri. Alle medarbejdere skal derfor løbende uddannes i informationssikkerhed i relevant omfang.

Som brugere af Ikast-Brande Kommune informationer skal alle medarbejdere følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf. Medarbejderne må kun anvende Ikast-Brande Kommunes informationer i overensstemmelse med det arbejde de udfører, og skal beskytte informationerne på en måde, som er i overensstemmelse med gældende lovgivning samt Ikast-Brande Kommunes "Regler" i informationssikkerhedshåndbogen.

Alle medarbejdere har adgang til informationssikkerhedshåndbogen igennem Ikast-Brande Kommunes ISMS (Information Security Management System).