Ikast-Brande Kommune

Informationssikkerhedspolitik

(efterfølgende benævnt I-sikkerhedspolitik)

Maj 2016
Sag nr. 2015/06550

Godkendt i Byrådet den 20.06.2016

Indhold

1. Indledning

Denne I-sikkerhedspolitik 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, I-Sikkerhedspolitikken op til revurdering efter behov. Dog mindst én gang om året.

Referencer:

- Databeskyttelsesforordningen
- Databeskyttelsesloven LOV nr 502 af 23/05/2018
- Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000
- Statsministeriets sikkerhedscirkulære (CIR nr. 204 af 07/12/2001)
- International Organization for Standardization, ISO 27001

2. Formål

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

Formålet med I-sikkerhedspolitikken 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*.

I-sikkerhedspolitikken uddybes i regler og procedurer. Disse samles i I-sikkerhedshåndbogen som ligeledes indeholder beredskabsplaner og risikovurderinger.

Ikast-Brande Kommunes beskyttelsesniveau er udarbejdet efter ISO 27001 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 I-sikkerhedspolitikken 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. Omfang, organisation og ansvar

I-sikkerhedspolitikken 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".

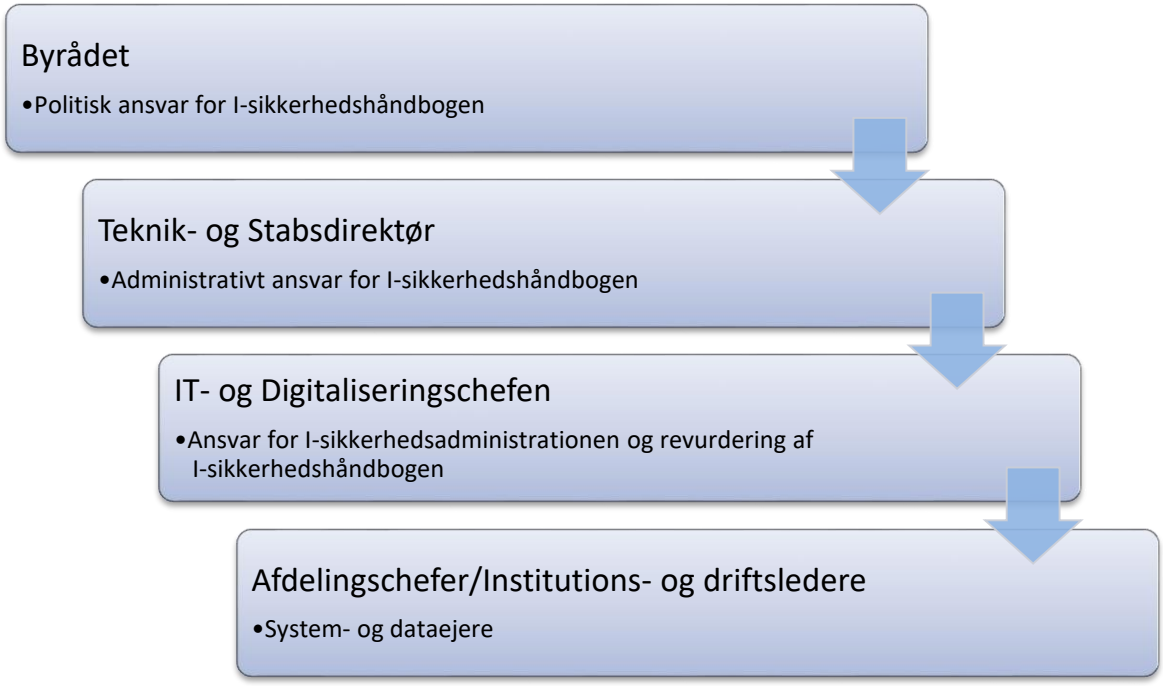
[1] http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Implementering-af-ISO27001

[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 politikkere, som har fysisk eller logisk adgang til Ikast-Brande Kommunes systemer, data og informationer skal gøres bekendt med I-sikkerhedspolitikken og følge den.

I-sikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte og indirekte indflydelse på drift og brug af Ikast-Brande Kommunes informationssystemer.

Ansvarsorganisation for I-sikkerheden ved Ikast-Brande Kommune:



Driftsorganisation for I-sikkerheden ved Ikast-Brande Kommune

Ansvarsområder for driftsorganisationen fremgår af "Forretningsorden for Informationssikkerheds-udvalget".

4. Sikkerhedsniveau

Det er Ikast-Brande Kommunes politik at beskytte sine informationer og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med Ikast-Brande Kommunes retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

Ikast-Brande Kommune har besluttet sig for et informationssikkerhedsniveau, der mindst svarer til de basale beskyttelsesforanstaltninger i ISO 27001 standarden, hvilket er beskrevet i Ikast-Brande Kommunes I-sikkerhedshåndbog.

Ansvaret for den daglige styring af informationssikkerhedsindsatsen er placeret hos den enkelte system- og dataejer. Denne sikrer, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er nødvendige og beskrevet i I-sikkerhedshåndbogen, gennemføres og efterleves. Informationssikkerheden integreres i alle forretningsgange, driftsopgaver og projekter samt i forhold til samarbejdet med aktuelle serviceleverandører.

De enkelte system- og dataejere skal gennemføre en afbalanceret risiko- og konsekvensvurdering under hensyntagen til de økonomiske forhold. Risiko- og konsekvensvurderingerne skal gennemgås mindst én gang om året eller ved større organisatoriske ændringer. Risiko- og konsekvensvurderingerne afgør, om der skal udarbejdes beredskabsplaner i forhold til aktuelle fagsystemer, forretningsservices samt medarbejdere og bygningsrelaterede forhold m.v., uagtet valg af serviceleverandør og dennes ydelser. Ikast-Brande Kommune beredskabsplan(er) skal ajourføres løbende – minimum én gang om året som skrivebordsøvelse.

5. Sikkerhedsbevidsthed

Informationssikkerhed vedrører Ikast-Brande Kommunes samlede informationsflow, og gennemførelse af en I-sikkerhedspolitik kan ikke foretages af ledelsen alene. Alle medarbejdere har et ansvar for at bidrage til at beskytte Ikast-Brande Kommunes 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 I-sikkerhedspolitikken 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 I-sikkerhedshåndbogen.

6. Brud på persondatasikkerheden

Såfremt en medarbejder opdager trusler mod informationssikkerheden eller overtrædelse på denne, skal dette straks meddeles til den nærmeste daglige leder.

Alle medarbejdere i Ikast-Brande Kommune er forpligtet til at efterleve den til enhver tid gældende I-sikkerhedspolitik med tilhørende retningslinjer, forretningsgang og relaterede bilag. En overtrædelse kan, efter omstændighederne, medføre sanktioner.

7. Kommunikationsplan/medieplan

For at støtte op om system- og dataejernes opgave i at sikre, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er nødvendige og beskrevet i I-sikkerhedshåndbogen, gennemføres og efterleves, er der fokus på forskellige kommunikationstiltag. Det er f.eks.:

- at samtlige system- og dataejere gennemgår en workshop, hvor de bliver gjort bekendt med deres rolle og ansvar.
- at samtlige nyansatte medarbejdere er forpligtet til at læse "Velkomsthilsen fra IT-afdelingen". Såfremt en medarbejder oprettes med en mailadr: xxxxx@ikast-brande.dk vil vedkommende automatisk få tilsendt velkomstmailen. For øvrige medarbejdere henvises til intranettet.
- at der løbende gennemføres awareness kampagner med særligt fokus på relevante I-sikkerhedsemner
- at der informeres om aktuelle sikkerhedshændelser eller lign. på intranettet og på infoskærmene
- at der gives informationer om I-sikkerhed via digitaliseringsforum og I-sikkerhedsudvalget
- at DBR´en kan deltage i møder på de enkelte forretningsområder, hvor der skønnes et behov for ekstra fokus på ét eller flere I-sikkerhedsemner

Alle medarbejdere har endvidere adgang til I-sikkerhedshåndbogen igennem Ikast-Brande Kommunes ISMS (InformationSecurityManagementSystem).

Denne informationssikkerhedspolitik er godkendt af Byrådet den 20. juni 2016

Revideret den 17. juni 2019.

------- --------------------------------