Notat

Albertslund Kommune

Albertslund Kommunes Informationssikkerhedspolitik
Informationssikkerhedspolitikken er først og fremmest et strategisk styringsredskab, der fastsætter rammerne for arbejdet med informationssikkerhed.

Dato: 1. juli 2014
Sags nr.: 14/3911

Sikkerhedspolitikken beskriver kommunens overordnede holdning til informationssikkerhed og skaber, sammen med en løbende risikovurdering, grundlaget for sikker anvendelse af informationsteknologi i Albertslund Kommune.

Sikkerhedspolitikken understøttes af et regulativ, der beskriver målsætning, afgrænsning og ansvar for sikkerhed.

Borgerne i Albertslund Kommune skal kunne følge sig trygge ved, at deres data bliver behandlet fortroligt. Sikkerhedspolitikken skal tage hensyn til kommunens visioner og politik på miljøområdet, leve op til lovgivningen, herunder kravene i persondataloven, og stemme overens med gængs praksis for offentlige myndigheder i Danmark.

Sikkerhedsniveauet skal løbende justeres ift. den teknologiske udvikling og behovet for effektiv borgerbetjening.

Informationssikkerhedspolitikken har til formål at sikre:

Tilgængelighed
At opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud.

Integritet
At opnå en pålidelig og korrekt funktion af informationssystemerne med minimeret risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.

Fortrolighed
At etablere mulighed for fortrolig behandling, transmission og opbevaring af data, hvor kun autoriserede og autentificerede brugere har adgang.

Risikovurderingerne gennemføres periodisk, samt ved anskaffelser og ændringer af systemer eller det it-miljø, systemerne opererer i.

Anvendelse og gyldighed
Informationssikkerhedspolitikken gælder for personoplysninger og værdioplysninger i kommunen, det vil sige oplysninger, der har en væsentlig økonomisk eller forvaltningsmæssig betydning for kommunen.

Informationssikkerhedspolitikken gælder for alle ansatte samt for al anvendelse af informationssystemer i Albertslund Kommune.

ØKONOMI & STAB

Økonomi & Stab
Digitalisering

Albertslund Kommune
Nordmarks Allé 1
2620 Albertslund

okonomiogstab@albertslund.dk
T 43 68 68 68

Albertslund Kommune

Informationssikkerhedshåndbog
Informationssikkerhedsreglerne i Albertslund Kommune er samlet i en informationssikkerhedshåndbog, som indeholder:

- Informationssikkerhedspolitikken
- Informationssikkerhedsregulativ for Albertslund Kommune.
- En række uddybende informationssikkerhedsregler for Albertslund Kommune.

Informationssikkerhedshåndbogen gælder for hele kommunen og publiceres elektronisk på kommunens intranet.

Informationssikkerhedsregulativet og de uddybende sikkerhedsregler skal tage udgangspunkt i ISO 27001, som beskriver risikoanalyse, planlægning, udførelse, og efterlevelse af sikkerhedsreglerne på følgende områder:

1. Sikkerhedspolitik
2. Organisering
3. Styring af aktiver
4. Medarbejdersikkerhed
5. Fysisk sikkerhed
6. Kommunikation og drift
7. Adgangsstyring
8. Anskaffelse, udvikling og vedligeholdelse af systemer
9. Styring af sikkerhedshændelser
10. Beredskab
11. Krav og politikker

Ansvar og organisering skal være beskrevet i kommunens regulativ for Informationssikkerhed og afspejle den gældende organisering.

Bevidsthed om informationssikkerhed
En høj sikkerhedsbevidsthed og hensigtsmæssig adfærd hos medarbejderne er blandt de vigtigste sikkerhedsforanstaltninger. Det er således kommunens mål, at der overalt er en høj bevidsthed om informationssikkerhed.

Derfor skal informationssikkerhedspolitikken, Informationssikkerhedsregulativet og de sikkerhedsregler der uddyber dette kommunikeres til alle relevante interessenter - herunder samtlige af kommunens medarbejdere.

Medarbejderne skal ved ansættelse og løbende uddannes og bevidstgøres om kommunens informationssikkerhedspolitik.

Informationsberedskab
Informationssystemer, der er vitale for kommunens betjening af borgerne og virksomhederne, og som således er kritiske for kommunens drift, skal identificeres, og der skal fastsættes maksimalt acceptable tider for utilgængelighed for så vidt angår disse informationssystemer.

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 informationssystemer.

Opfølgning på informationssikkerhed
Kommunen vil måle, vurdere og følge op på informationssikkerheden ved at.

- Løbende registrering og opfølgning på sikkerhedshændelser
- Behandle sikkerhedshændelser og -tiltag i relevante fora med henblik på løbende forbedring af informationssikkerhed og vidensdeling
- Løbende opfølgning på kommunens vidensniveau vedr. informationssikkerhed
- Løbende revisioner og evalueringer af informationssikkerheden
- Revurdere informationssikkerhedspolitikken mindst en gang hvert 2. år
- Revurdere informationssikkerhedsregulativet mindst en gang om året.