Albertslund 16. maj 2019

Informationssikkerhedspolitik for Albertslund Kommune 2019 - 2023

Informationssikkerhedspolitikken er et strategisk styringsredskab, der fastsætter rammerne for arbejdet med informationssikkerhed.

Informationssikkerhed handler om, at Albertslund Kommune behandler mange informationer, som er er fortrolige, og at borgerne skal kunne føle sig trygge ved, at deres data bliver behandlet sikkert.

Informationssikkerhedspolitikken har til formål at sikre fortrolighed, integritet og tilgængelighed til information.

Politikken beskriver Albertslund Kommunes overordnede holdning til informationssikkerhed og skaber, sammen med den løbende risikovurdering, grundlaget for sikker anvendelse af informationsteknologi i Albertslund Kommune.

Informationssikkerhedspolitikken skal leve op til persondataforordningen, databeskyttelsesloven og ISO27001, der er en international standard for informationssikkerhed. Desuden skal politikken være i overensstemmelse med god forvaltningsskik.

Anvendelse og gyldighed

Informationssikkerhedspolitikken gælder for personoplysninger og værdioplysninger, der håndteres af Albertslund Kommune eller af samarbejdspartnere på vegne af kommunen. Det vil sige oplysninger, der har en væsentlig forvaltningsmæssig eller økonomisk betydning for kommunen, uanset om det for eksempel er oplysninger om en borgers helbredsmæssige forhold eller oplysninger i forbindelse med salg af kommunale grunde.

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

Målsætninger

Informationssikkerhedspolitikkens målsætninger bygger på persondataforordningens seks principper og at borgere skal kunne være trygge ved, at Albertslund Kommune opbevarer og behandler oplysninger sikkert.

Princip 1: Lovlighed, rimelighed og gennemsigtighed

Ledere og medarbejdere kender og følger de lovgivningsmæssige rammer for opbevaring og behandling af data.

Det er gennemsigtigt for borgeren, hvilke oplysninger og vurderinger, der er grundlaget for afgørelser.

Princip 2: Formålsbegrænsning

Albertslund Kommune indsamler og viderebehandler data ud fra det oprindelige formål med indsamlingen.

Princip 3: Dataminimering

Albertslund Kommune indsamler, behandler og opbevarer data, der er tilstrækkelig, relevant og begrænset til, hvad der er nødvendigt i forhold til formålet.

Princip 4: Rigtighed

Oplysninger, der behandles skal være korrekte og i nødvendigt omfang ajourførte.

Princip 5: Opbevaringsbegrænsning

IT-systemer er sat op, så personoplysninger og anden data opbevares i det tidsrum, der er nødvendigt i forhold til formålet og til andre legitime formål, for eksempel lovbestemt statistik.

Princip 6: Integritet og fortrolighed

Data behandles, transmitteres og opbevares kun hvor autoriserede og autentificerede brugere har adgang. Autentificering betyder, at de enkelte brugeres identitet og ret til adgang til systemet kan bekræftes.

Der arbejdes i retningen af at indføre flerfaktor-identifikation af brugere af kommunens it-systemer med personhenførbare data i takt med de tekniske og økonomiske muligheder.

Informationssystemer er sat op og fungerer korrekt med minimeret risiko for ukorrekt data, for eksempel som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.

Sikkerhedsniveauet justeres løbende i forhold til den teknologiske udvikling og behovet for effektiv borgerbetjening.

Ansvarlighed

Alle afdelinger udarbejder arbejdsgange og risikovurderinger for processer, hvor der indgår følsomme personoplysninger for at kortlægge behandlingsaktiviteter. Her indgår vurdering af it-miljøet og systemerne. Arbejdsgange og risikovurderinger opdateres ved ændringer og mindst 1 gang om året.

Arbejdsgange og processer for behandling af persondata følges.

Der er klart formulerede og opdaterede beskrivelser af ansvarsfordeling for informationssikkerhed. De er tilgængelige for ansatte på medarbejdersiden.

Der er klart formulerede beskrivelser af ansvar for it-systemer. De er tilgængelige for ansatte på medarbejdersiden.

Informationsberedskab

Informationssystemer, der er vitale for kommunens betjening af borgere og virksomheder, og som er kritiske for kommunens drift, skal identificeres, og der skal fastsættes maksimalt acceptable tider for systemernes utilgængelighed.

Der skal desuden 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.

Implementering

En høj sikkerhedsbevidsthed og hensigtsmæssig adfærd hos ledere og medarbejdere er blandt de vigtigste sikkerhedsforanstaltninger. Derfor kommunikeres informationssikkerhedspolitikken, håndbogen og de uddybende regler til alle relevante interessenter.

I begyndelsen af ansættelsen gennemfører alle ansatte en test i behandling af personfølsomme oplysninger. Nærmeste leder er ansvarlig for, at den enkelte medarbejdere som en del af introduktionsprogrammet i starten af ansættelsen gøres bekendt med de rammer for behandling af følsomme oplysninger, der gælder for fagområdet.

Der er løbende generelle, fagspecifikke og temabaserede informationsaktiviteter om informationssikkerhed i Albertslund Kommune.

Informationssikkerhed i Albertslund Kommune

Informationssikkerhedspolitik

Informationssikkerhedshåndbog

Informationssikkerhedsregler i Albertslund Kommune

- Automatisk sletning af mails i Outlooks Slettet-boks
- Destruktion af personoplysninger på papir
- Fagansvarliges ansvar om GDPR
- GDPR-kontaktpersonens rolle
- GDPR-årshjul (4. kv. 2019)
- IT-retningslinjer på sikkerhedsområdet (2. kv. 2019)
- Procedure for sikkerhedsbrud
- Procedure og regler for brug af video og billeder (3. kv. 2019)
- Retningslinjer i forhold til adgangskoder
- Retningslinjer til brug for tilrettelæggelse af informationssikkerhedskoordinators indsats og præcisering af ledernes rolle
- Social mediepolitik (3. kv. 2019)
- Systemejers forpligtelser (3. kv. 2019)
- Vejledning om pligt til at inddrage databeskyttelsesrådgiveren (DPO)