

Informationssikkerhedsstrategi

Indledning

Informationssikkerhedsstrategien er et strategisk styringsværktøj, der fastsætter rammer for arbejdet med informationssikkerhed.

Informationssikkerhed handler om, at Albertslund Kommune behandler en større mængde fortrolige og følsomme informationsaktiver, hvorfor borgere og samarbejdspartnere skal kunne have tillid til, at Albertslund Kommune behandler deres informationsaktiver sikkert.

Anvendelse

Albertslund Kommune arbejder efter en forståelse om informationsaktiver baseret på ISO2700x standarderne. Informationsaktiver er alle typer af informationer som kommunen opbevarer og behandler, både personhenførbare informationer, samt egne fortrolige informationer.

Strategien er gældende for hele Albertslund Kommune. Alle informationsaktiver, systemer, netværk og it-udstyr, som er i Albertslund Kommunes besiddelse, og som anvendes af Albertslund Kommune, er omfattet.

Formål

Strategien beskriver Albertslund Kommunes overordnede holdning til informationssikkerhed og skaber, sammen med risikostyring, grundlaget for sikker anvendelse af informationsteknologi i Albertslund Kommune.

Informationssikkerhedsstrategien har afsæt i ISO27001 standarden, som er en international standard for styring af informationssikkerhed. ISO27001 standarden danner grundlaget for arbejdet med informationssikkerhed og implementeringen af andre standarder og lovkrav indenfor området, eksempelvis databeskyttelsesforordningen, National Standard for Identiteters Sikringsniveauer (NSIS) og NIS2-direktivet.

Strategien skal udmøntes gennem implementering af sikkerhedsforanstaltninger på baggrund af risikovurderinger, med henblik på at sikre et passende sikkerhedsniveau for informationsaktiver, med udgangspunkt i tre centrale begreber:

- Fortrolighed, så informationer ikke kommer uvedkommende i hænder.
- Integritet, så informationer forbliver pålidelig, korrekt og intakt.
- Tilgængelighed, så informationer kan tilgås og anvendes, når der er behov for det.



Målsætninger

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

Princip 2: Formålsbegrænsning

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

Princip 3: Dataminimering

Albertslund Kommune indsamler, behandler og opbevarer informationsaktiver, 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 informationsaktiver 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

Informationsaktiver 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 multifaktor-identifikation af brugere af kommunens it-systemer med personhenførbare informationsaktiver i takt med de tekniske og økonomiske muligheder.

Informationssystemer er sat op og fungerer korrekt med minimeret risiko for ukorrekt informationsaktiver 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 eller fortrolige personoplysninger for at kortlægge behandlingsaktiviteter. Her indgår vurdering af afdelingernes it-systemer. Arbejdsgange og risikovurderinger opdateres ved ændringer og mindst 1 gang om året.

Arbejdsgange og processer for behandling af informationsaktiver 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 informationssikkerhedsstrategien, håndbogen og de uddybende regler til alle relevante interessenter.

I begyndelsen af ansættelsen gennemfører alle ansatte en test i behandling af personhenførbare oplysninger. Nærmeste leder er ansvarlig for, at de 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

