Policy for informasjonssikkerhet i leverandørforhold

Innledning

Denne policyen omfatter rammer og føringer for hvordan informasjonssikkerheten skal ivaretas av kommunens leverandører. Det kan være personopplysninger som behandles av en leverandør (databehandler), eller et kan være informasjon som av annen grunn er tilgjengeliggjort for leverandør eller av leverandør.

Omfang

Denne policyen gjelder for alle systemer og prosesser som omfattes av styringssystemet for informasjonssikkerhet, og skal legges til grunn i alle anskaffelsesprosesser hvor personvern og informasjonssikkerhet må tas hensyn til.

Målsettinger

- Sikre at leverandørene ivaretar informasjonssikkerheten i henhold til kommunens informasjonssikkerhetspolicy og øvrige policyer.

Avtalereguleringer

Disse prinsippene handler om å sikre formell styring av leverandørene.

- Alle leverandører skal reguleres med formelle avtaler. De samme kravene skal gjelde for leverandørenes underleverandører.
- Avtaleforholdet skal inkludere kommunens krav til informasjonssikkerhet. De samme kravene gjelder for leverandørens underleverandører.
- Dersom det er hensiktsmessig, så skal mer detaljerte krav for håndtering av informasjon, systemer, tilganger og IT-utstyr spesifiseres i egen avtale.
- Når leverandøren planlegger større endringer til virksomhetskritiske systemer eller operative systemer som kommunen bruker, så skal leverandøren informere kommunen om risikoer knyttet til endringen. Leverandøren skal foreslå tiltak for å redusere risikoene. Leverandøren skal også avvente godkjenning fra kommunen før endringen gjennomføres.

Behandling av personopplysninger

Disse prinsippene handler om å sikre at leverandørene behandler personopplysninger i tråd med personopplysningsloven.

- Når leverandører behandler personopplysninger på vegne av kommunen, så er de etter personopplysningsloven databehandler. Leverandørene skal stille tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven, jf GDPR artikkel 28, punkt 1. Eksempler på

garantier kan være at leverandøren har et sertifisert styringssystem for informasjonssikkerhet, eller at de gjennom annen dokumentasjon kan demonstrere etterlevelse av lovverket.
- Alle databehandlere skal reguleres med databehandleravtale. Kommunen skal bruke standardiserte maler for slike avtaler, for eksempel malen til Datatilsynet.
- Gran kommune godtar Statens standardavtaler med dette dokumentet og Krav fra Kins, som tillegg i anskaffelsesprosesser

Ansvar

- Informasjonssikkerhetsleder (CISO) er ansvarlig for innholdet i denne policyen.
- Systemeiere er ansvarlige for at systemer som driftes av leverandører er avtaleregulert, og at relevante sikkerhetskrav er inkludert i avtalene.
- Se også dokumentet Roller og ansvar.

Resultat

Lavere risiko for sikkerhetsbrudd som følge av at leverandørene ivaretar informasjonssikkerheten innenfor de rammene kommunen har satt.

Referanser

- ISO 27002:2022 5.1 «Policyer for informasjonssikkerhet»
- ISO 27002:2022 5.19 «Informasjonssikkerhet i leverandørforhold»
- ISO 27002:2022 5.20 «Håndtering av informasjonssikkerhet i leverandøravtaler»
- ISO 27002:2022 5.21 «Håndtering av informasjonssikkerhet i IKT-leveransekjeden»
- ISO 27002:2022 5.22 «Overvåking, gjennomgang og endringshåndtering av leverandørtjenester»

Endringslogg

Dokumentversjon	Endringer	Endret dato	Endret av
1		23.03.2024	Tore Løvhaug