

 Troms fylkeskommune Romssa fylkkasuohkan Tromssan fylkinkomuuni				Dok.id.: 1.4.1.1.14
Retningslinje for leverandørstyring				Dok.type: Styringsdokument er
Versjon: 1.00	Skrevet av: Stian Strømmesen	Gjelder fra: 31.10.2025	Godkjent av: Tor Arne Morskogen	Sidenr: 1 av 4

1. Innledning

Leverandørstyring handler om å evaluere, administrere og overvåke organisasjonens forhold til eksterne leverandører for å sikre at deres tjenester og produkter oppfyller etablerte standarder for kvalitet og sikkerhet. Retningslinjen skal sikre ivaretagelse av informasjon og personopplysninger som behandles av leverandører.

2. Omfang

Denne retningslinjen omfatter rammer og føringer for hvordan Troms fylkeskommune skal stille krav til fylkeskommunens leverandører om ivaretagelse av informasjonssikkerhet og personvern, og skal gi anbefalte sikkerhetskrav for anskaffelse og forvaltning.

Med leverandører mener vi også andre som er i leveransekjeden, herunder underleverandører eller andre tredjeparter.

3. Målsettinger

Sikre at leverandørene ivaretar informasjonssikkerheten og personvernet i henhold til inngåtte avtaler og gjeldende regelverk.

4. Krav til leverandører som behandler informasjon på vegne av Troms Fylkeskommune

Leverandøren har taushetsplikt om informasjonen leverandøren får tilgang til i kontraktsforholdet.

Dersom leverandøren skal behandle personopplysninger skal det inngås databehandleravtale.

Hvis leverandøren skal benytte Troms Fylkeskommune sine IKT-systemer skal IKT-reglementet for bruk av IKT-ressurser følges.

5. Avtaleregulering av leverandørene

Disse informasjonssikkerhetskravene handler om å sikre at relevante krav til informasjonssikkerhet og personvern er definert og avtalefestet. Dersom det er hensiktsmessig, så skal mer detaljerte krav for håndtering av informasjon, systemer, tilganger og IT-utstyr spesifiseres i egen avtale.

- *Standardavtaler.* Alle leverandører skal der det er mulig, reguleres med relevante standardavtaler. Kravene i standardavtalene skal også gjelde for leverandørenes underleverandører.

Retningslinje for leverandørstyring	Versjon.: 1.00	Dok.id.: 1.4.1.1.14
	Side : 2 av 4	

- *Sikkerhets- og personvernkrav.* Avtaleforholdet skal inkludere krav til informasjonssikkerhet og personvern. De samme kravene skal gjelde for leverandørens underleverandører.

Når en leverandør behandler personopplysninger på vegne av fylkeskommunen, skal det i tillegg etableres en databehandleravtale for å sikre at behandlingen skjer i tråd med personvernregelverket. Fylkeskommunen skal bruke standardiserte maler for slike avtaler, enten malen til [DFØ](#) eller [Datatilsynet](#).

- *Vurdering av tilstrekkelige garantier.* Når en leverandør behandler personopplysninger på vegne av fylkeskommunen, så er leverandøren etter personopplysningsloven en databehandler. Databehandlere skal stille tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven. Eksempler på garantier kan være at databehandleren har et sertifisert styringssystem for informasjonssikkerhet (ISO 27001), at de har et styringssystem for informasjonssikkerhet og personvern (ISO 27701), eller at de gjennom annen dokumentasjon kan demonstrere etterlevelse av lovverket.

6. Informasjonssikkerhetskrav til leverandører

6.1 Sikkerhetsrevisjon

Troms Fylkeskommune skal ha tilgang til å gjennomføre sikkerhetsrevisjon av løsning/leverandør. Dette inkluderer penetrasjonstesting og sårbarhetsskanning.

6.2 Risikostyring

Leverandøren skal ha en løpende prosess for fortløpende identifisere, vurdere og håndtere sårbarheter i tjenesten.

Leverandør bør være åpen om sine sikkerhetspraksiser og regelmessig rapportere sikkerhetsstatus og eventuelle hendelser.

6.3 Avslutning av avtale

Leverandøren skal yte bistand til Troms Fylkeskommune dersom fylkeskommunen ønsker å avslutte avtalen. Leverandøren skal legge til rette for at fylkeskommunens data blir overført til fylkeskommunen eller til tredjepart utpekt av fylkeskommunen.

Troms Fylkeskommune skal beholde eierskapet til fylkeskommunens data etter at kontrakten er avsluttet og til data er flyttet og/eller slettet fra tjenesten.

6.4 Beskyttelse av data under overføring

Data som overføres via nettverk skal sikres. Dette gjelder både data som overføres til og fra tjenesten, internt i tjenesten og data som utveksles med andre tjenester.

6.5 Beskyttelse av datasenter

Leverandør skal forhindre uautorisert tilgang til sine datasenter samt beskytte mot tyveri, skade, tap og at utstyr svikter for å sikre kontinuerlig drift.

Retningslinje for leverandørstyring	Versjon.: 1.00	Dok.id.: 1.4.1.1.14
	Side : 3 av 4	

6.6 Beskytte lagret informasjon

Leverandøren skal definere, velge, dimensjonere og implementere passende kryptografiske mekanismer støttet av en tilstrekkelig nøkkeladministrasjonsinfrastruktur for å sikre sikker drift av tjenestene. Det gjelder data i ro så vel som data i bevegelse (data in transit).

Leverandør skal sikre at det finnes pålitelige sikkerhetskopiering og evne til gjenoppretting for å beskytte data mot tap eller skade.

6.7 Separasjon mellom kunder

Leverandøren må skille Troms Fylkeskommune sine tjenester og data fra andre kunder hos leverandøren.

6.8 Backup

Leverandør skal sørge for tilfredsstillende backup av data slik at data kan gjenskapes (restores) raskt og effektivt ved behov.

6.9 Sletting av data

Leverandøren må kunne dokumentere hvordan man sletter data og hvordan man sikrer at slettede data ikke kommer på avveie eller kan gjenskapes.

6.10 Tilgjengelighet

Tjenesten skal være tilgjengelig for Troms Fylkeskommune når fylkeskommunen har behov for tjenesten. Leverandøren skal kunne garantere oppetid og dokumentere historisk oppetid/tilgjengelighet.

6.11 Endringshåndtering

Leverandøren skal ha prosess for å håndtere endringer for å sikre at endringer som kan påvirke sikkerheten identifiseres og håndteres, og at uautoriserte endringer kan oppdages.

6.12 Sporbarhet

Alle relevante handlinger som utføres av leverandøren skal logges. Loggen skal ikke kunne manipuleres. Troms Fylkeskommune skal få tilgang til loggene på forespørsel.

6.13 Tilgangskontroll/autentisering

Løsningen skal ha en robust tilgangskontroll som sikrer at rett person får tilgang til rett informasjon og rette funksjoner i løsningen. Autentisering utelukkende basert på brukernavn og passord anses ikke som forsvarlig.

Dersom det er relevant for tjenesten skal leverandør skal tilby verktøy for administrasjon av Troms Fylkeskommune sine brukere og deres tilganger og ha tilstrekkelig støtte for bruk av eksterne identitetstilbydere slik som bla Microsoft Entra ID.

6.14 Sikkerhetsovervåking

Leverandøren skal ha tilstrekkelig sikkerhetsovervåking av tjenesten, rutiner for varslings ved hendelser, samt evne til å håndtere sikkerhetshendelser raskt og effektivt.

Retningslinje for leverandørstyring	Versjon.: 1.00	Dok.id.: 1.4.1.1.14
	Side : 4 av 4	

Leverandør skal på forespørsel gi Troms Fylkeskommune tilgang til revisjonsrapporter for vurdering av sikkerhetsovervåkingen, vurdering av tilgangsstyringen til systemer og komponenter for leverandørens egne administratorer og hvilke prosedyrer og rutiner de har for varsling.

Sikkerhetslogger skal gjøres tilgjengelig for Troms Fylkeskommunes på forespørsel.

7. Ansvar

- Ansvarlig for styringssystem for informasjonssikkerhet og personvern (INFODOK) eier denne retningslinjen.
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 - Informasjonssikkerhet og personvern](#)

8. Resultat

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

1. Referanser

- 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»
- NIS2 artikkel 21 nr 2 bokstav d «Supply chain security»