Sikkerhetskrav i forbindelse med anskaffelser

Informasjonssikkerhetskrav

Styringssystem for informasjonssikkerhet Formål med kravene: sikre at leverandøren har et eget styringssystem.		Veiledning til krav	Referanse
1.1	Leverandør skal ha et egnet styringssystem for informasjonssikkerhet. Styringssystemet skal dekke alle enheter og prosesser som inngår i leveransen.	Kravet skal sikre at leverandør har et helhetlig og aktivt forhold til informasjonssikkerhet. Styringssystemet vil diktere at leverandør involverer ledelsen, gjennomfører risikovurderinger og implementerer sikringstiltak.	ISO 27001 DBA bilag C.2.2
1.2	Leverandør skal etablere og forvalte tilstrekkelige sikkerhetstiltak for å ivareta informasjonssikkerheten for behandlingen av informasjonen i tjenesten.	Sikkerhetstiltak er	ISO 27001 DBA 7.1
1.3	Leverandør skal løpende gjennomføre risikovurderinger. Risikovurderingene skal fremvises på forespørsel.	Risikovurderinger er nødvendig for å kunne vurdere risikobildet og iverksette nødvendige sikkerhetstiltak.	ISO 27001 DBA 7.2
Organisering av informasjonssikkerhet Formål med kravene: sikre at leverandøren har en sikkerhetsorganisasjon med tydelige roller og ansvar.		Veiledning til krav	Referanse
2.1	Leverandør skal dokumentere sin sikkerhetsorganisasjon. Dokumentasjonen skal inkludere oversikt over personell med tilhørende rollebeskrivelser og ansvar.	Kravet skal sikre at leverandør har tildelt ansvar for informasjonssikkerhet til spesifikke ansatte. Disse ansatte vil typisk utgjøre kontaktpunktene mot kommunen.	ISO 27002 6.1

Personellsikkerhet Formål med kravene: sikre at leverandørens ansatte har tilstrekkelig informasjonssikkerhetskompetanse til å forvalte kommunens informasjon.		Veiledning til krav	Referanse
3.1	Leverandør skal ha en dokumentert prosess for opplæring/kompetanseheving i informasjonssikkerhet og personvern for sine ansatte.	Kravet skal sikre at leverandøren har et regime for å styrke kompetansen for egne ansatte.	ISO 27002 7.2
3.2	Leverandør skal dokumentere at de ansatte som er involvert i leveranse av tjenesten har tilstrekkelig kompetanse i informasjonssikkerhet og personvern.	Kravet skal sikre at ansatte som er involvert i leveransen har tilstrekkelig kompetanse.	ISO 27002 7.2
Informasjonsforvaltning Formål med kravene: sikre at leverandøren tar eierskap til informasjon og informasjonssystemene, herunder kommunens informasjon.		Veiledning til krav	Referanse
4.1	Leverandøren skal ha oversikt over utstyr og systemer som er involvert i leveransen til kommunen.	Kravet skal sikre at leverandør har oversikt og kontroll på sitt utstyr, så for eksempel en bærbar maskin med kommunens opplysninger ikke kommer på avveie.	ISO 27002 8.1
4.2	Leverandøren skal ha en dokumentert policy for akseptabel bruk av utstyr og informasjonssystemer.	Kravet skal bidra til å regulere hva de ansatte kan bruke sitt utstyr til.	ISO 27002 8.1
4.3	Avhending/sletting av medier, herunder backupmedier, skal skje på en tilstrekkelig sikker måte.	Kravet skal sikre at flyttbare medier og backupmedier slettes før de avhendiges.	ISO 27002 8.3

Tilgangskontroll Formål med kravene: begrense tilgang til informasjon og informasjonssystemer.		Veiledning til krav	Referanse
5.1	Leverandør skal ha en dokumentert prosess for tilgangsstyring, herunder oppretting, endring og sletting av brukere. Bruk av privilegerte kontoer skal begrenses.	Kravet skal sikre at leverandør har god kontroll på tilgangsstyringen sin.	ISO 27002 9.1
5.2	Løsningen skal ha rollebasert tilgangsstyring.	Kravet går ut på at tjenesten skal skille mellom forskjellige roller. Noen kan for eksempel være	ISO 27002 9.2

		administratorer, mens andre vanlige brukere. Roller bidrar til å redusere risiko ved å begrense hva de ulike rollene kan gjøre i tjenesten.	
5.3	Alle registrerte brukere i tjenesten skal være unike og personlige.	I de fleste løsninger er det viktig at vi vet hvem som har gjort hva. Fellesbrukere bør derfor unngås. Dersom tjenesten inneholder personopplysninger, så er det også et krav om at den registrerte skal kunne få vite hvem som har sett på vedkommendes opplysninger.	ISO 27002 9.2
5.4	Dersom tjenesten tilbyr autentisering over usikrede nett, så skal sterk autentisering støttes og aktiveres.	Kravet er spesielt viktig dersom tjenesten skal gjøres tilgjengelig over Internett. Datatilsynet er for eksempel tydelig på at dersom et skolesystem med mange elever er tilgjengelig over Internett, så skal systemet sikres med sterk autentisering. Tofaktorautentisering er eksempel på sterk autentisering.	ISO 27002 9.4
Kryptografi Formål med kravene: sikre at leverandøren bruker kryptografi for å beskytte informasjon.		Veiledning til krav	Referanse
6.1	Leverandør skal ha en dokumentert prosess for bruk av kryptografiske kontroller, og håndtering av kryptografiske nøkler.	Kryptering er et viktig teknisk sikringstiltak. Kravet sikrer at leverandøren har et godt regime rundt sine krypteringsløsninger.	ISO 27002 10.1
6.2	Leverandør skal kunne implementere kryptografiske tiltak (for eksempel kryptering av databasen) der risikovurderinger konkluderer med at det er nødvendig.		
Fysisk og miljømessig sikkerhet Formål med kravene: begrense fysisk tilgang til lokaler, servermiljø og informasjonssystemer.		Veiledning til krav	Referanse
7.1	Leverandør skal ha tilstrekkelig fysisk sikring knyttet til sine datarom, som adgangskontroll, brannsikring,	Kravet skal ivareta sikring av lokaler hvor kommunens data befinner seg. Tilgang til datarom skal kun gis de som har et tjenstlig behov. Kravet dekker også andre	ISO 27002 11.1

	ventilasjon og redundant strømforsyning. Dokumentasjon skal legges frem på forespørsel.	elementer, som brannslukkingsapparat, alarm og nødstrøm.	
Driftssikkerhet Formål med kravene: sikre at leverandøren har korrekt og sikker drift av sine informasjonssystemer.		Veiledning til krav	Referanse
8.1	Leverandør skal ha en dokumentert prosess for endringshåndtering, som sikrer at kommunen blir varslet ved eventuelle endringer og/eller vedlikehold av løsning som krever nedetid.	Kravet skal sikre at leverandør har en god endringsprosess som sikrer at endringer i tjenesten ikke medfører nedetid, bortfall av data eller endring av data. I tillegg stilles det krav om at kommunen skal varsles ved endringer, slik at brukerne ved når endringer skjer og dermed kan planlegge for at tjenesten er utilgjengelig.	ISO 27002 12.1
8.2	Leverandør skal en dokumentert prosess for testing av endringer i tjenesten, samt overføring av endringer fra testmiljø til produksjonsmiljø.	Kravet skal sikre at leverandør kvalitetssikrer endringer i tjenesten, og at det skal gjøres ved å bruke testmiljø og produksjonsmiljø.	ISO 27002 12.1
8.3	Leverandørens testmiljø skal være atskilt fra produksjonsmiljøet. Testmiljøet skal ikke benytte kommunens produksjonsdata.		ISO 27002 12.1
8.4	Leverandør skal separere kommunens data fra andre kunders data, fysisk eller logisk.	Kravet skal sikre at kommunens data skal være tilstrekkelig atskilt fra annen data, og dermed at kommunens data ikke «lekker» over til andre kunder, eller omvendt.	ISO 27002 12.1
8.5	Leverandør skal ha en dokumentert prosess for kapasitetsstyring, som sikrer tilgjengelighet på tjenesten ved varierende behov.	Kravet skal sikre at leverandør har tilstrekkelig kapasitet i sin tjeneste til å håndtere perioder med høy belastning. Dette ble aktualisert ifbm koronasituasjonen, hvor tjenester ble tilnærmet utilgjengelig på grunn av økt bruk (for eksempel VPN-løsninger). God kapasitetsstyring er derfor viktig for å kunne garantere tilstrekkelig kapasitet, selv i perioder med høy belastning.	ISO 27002 12.1

8.6	Tjenesten skal være hensiktsmessig sikret mot ondsinnet kode og datainnbrudd.	Kravet er et generelt krav om at leverandør skal ha gode sikkerhetstiltak på plass.	ISO 27002 12.2
8.7	Leverandør skal ha en dokumentert prosess for sikkerhetskopiering.	Kravet skal sikre at leverandør tar sikkerhetskopier av kommunens data. Kommunen bør definere hvor mye tid som kan gå tapt dersom behov for gjenoppretting må gjennomføres, da det er viktig for å sette opp riktige tidsintervaller for sikkerhetskopiering.	ISO 27002 12.3
8.8	Leverandør skal jevnlig verifisere innhold i sikkerhetskopier og teste gjenoppretting av data for å verifisere kvaliteten på sikkerhetskopiene.	Kravet skal sikre at leverandøren klarer å gjenopprette sikkerhetskopier dersom nødvendig.	ISO 27002 12.3
8.9	Leverandør skal oppbevare sikkerhetskopier fysisk eller logisk atskilt fra produksjonsmiljøet.	Det har vært flere tilfeller hvor angrep på kommunens servermiljø også har omfattet sikkerhetskopier, for eksempel i Østre Toten i 2020. Ved å definere sperrer mellom produksjonsmiljø og sikkerhetskopiene øker sannsynligheten for gjenoppretting.	ISO 27002 ??.?
8.10	Leverandør skal etablere og ha ansvaret for overvåking av tjenesten, dataoverføringer og grensesnitt. Avvik skal rapporteres til kommunen.	Kravet skal sikre at leverandør har et overvåkingsregime på plass.	ISO 27002 12.4
8.11	Leverandør skal sikre en forsvarlig og systematisk overvåking av hele leveranseprosessen av tjenesten.	Kravet skal sikre at leverandør overvåker alle elementer som inngår i leveransen av tjenesten.	ISO 27002 12.4
8.12	Leverandør skal logge alle forsøk på autorisert og uautorisert tilgang til tjenesten, samt relevante sikkerhetshendelser som er tilknyttet løsningen.	Kravet skal sikre at leverandør oppdater forsøk på ulovlig bruk av tjenesten (for eksempel passordgjetting), samt gi god sporbarhet hvis leverandøren får en sikkerhetshendelse. Gode logger er viktig i forbindelse med styring av informasjonssikkerhetsbrudd.	ISO 27002 12.4
8.13	Leverandør skal sikre følgende logging ved aksess av data i tjenesten: 1) hvem som aksesserte, 2) når data ble aksessert, 3) hvilke data som ble aksessert, og 4) ved endring skal alle data/felter som ble endret logges.	Kravet er spesielt viktig ved behandling av personopplysninger. Formålet er å ha god sporbarhet på hvem som har gjort hva, og når det har skjedd. Kravet henger sammen med kravet om personlige brukerkontoer.	ISO 27002 12.4

8.14	Leverandør skal sikre at logger beskyttes mot uautorisert innsyn, endring og sletting.	Logger kan være viktig bevismateriale som må sikres.	ISO 27002 12.4
8.15	Leverandør skal ha en dokumentert prosess for sikkerhetsoppdateringer som dekker alle komponenter i tjenesten.	Kravet skal sikre at leverandør gjennomfører kontinuerlige sikkerhetsoppdateringer (patcher) av sine systemer og tjenester.	ISO 27002 12.5
8.16	Leverandør skal sørge for jevnlig sikkerhetstesting av tjenesten. Dokumentasjon av test med tiltak skal kunne fremlegges på forespørsel.	Kravet skal sikre at leverandør gjennomfører sikkerhetstester eller penetrasjonstester av sitt miljø og sine tjenester. Slik testing er viktig for å avdekke om det finnes sårbarheter som må tettes.	ISO 27002 ??.?
8.17	Datautstyr som er i kontakt med kommunens informasjon skal være tilstrekkelig sikret.	Manglende sikkerhet på utstyret til leverandørens ansatte kan resultere i at trusselaktører får innpass i utstyret og dermed kommunens data.	ISO 27002 ??.?
Kommunikasjonssikkerhet Formål med kravene: sikre at leverandøren har god kommunikasjonssikkerhet.		Veiledning til krav	Referanse
9.1	Leverandør skal ha utarbeidet konfigurasjonskart som viser sikkerhetskontroller og teknisk beskrivelse av informasjonssystemene, inkludert dataflyt.	Kravet skal sørge for at kommunen får oversikt over hvordan kommunens data flyter i tjenesten. Kommunen er blant annet pålagt å gjøre en egen risikovurdering og i mange tilfeller også en personvernkonsekvensvurdering (DPIA). Et slikt konfigurasjonskart vil være nødvendig for å forstå hvordan tjenesten er designet/bygget opp, og vil dermed være et nyttig underlag for risikovurderingene.	ISO 27002 13.1
9.2	Alle grensesnitt for nettjenester (web, APIer, endepunkter) skal være sikret mot uautorisert tilgang.	Kravet skal sikre at leverandør implementerer sikkerhetstiltak for alle grensesnitt som eksponerer kommunens data. APIene har for eksempel ved flere tilfeller vært dårlige sikret enn selve websiden.	ISO 27002 13.1
9.3	All datakommunikasjon over usikre nettverk (for eksempel Internett) skal være kryptert i henhold til beste praksis. Trafikk i klartekst skal ikke forekomme.	Kravet skal sikre at overføring av kommunens data alltid skjer gjennom krypterte nettverk. Det reduserer risikoen for at en trusselaktør klarer å fange opp trafikk og	ISO 27002 13.2

		dermed få tilgang til for eksempel personopplysninger. Det kan for eksempel gjøres gjennom falske trådløse nettverk.	
9.4	Alle som behandler kommunens produksjonsdata, skal ha signert taushetserklæring.	Kravet skal sikre den juridiske forpliktelsen som følger av at leverandørens ansatte behandler kommunens data.	ISO 27002 13.2
Anskaffelse, utvikling og vedlikehold av systemer Formål med kravene: sikre at leverandør ivaretar informasjonssikkerhet i systemenes livsløp.		Veiledning til krav	Referanse
10.1	Tjenesten skal være utviklet etter sikker utviklingsmetodikk.	Kravet skal sikre at leverandør har hatt fokus på informasjonssikkerhet gjennom hele utviklingsløpet.	ISO 27002 14.2
Leverandørforhold Formål med kravene: sikre at underleverandører har kontroll på informasjonssikkerheten.		Veiledning til krav	Referanse
11.1	Leverandør skal beskrive hvilke underleverandører som brukes, og hvilke roller og oppgaver de har i forbindelse med leveranse av tjenesten.	Kravet skal sikre at kommunen har kontroll på hvem som er involvert i behandlingen av kommunens data. Det er også viktig i forbindelse med behandling av personopplysninger, da kommunen må sikre et gyldig overføringsgrunnlag til land utenfor EØS-området.	ISO 27002 15.1
Styring av informasjonssikkerhetsbrudd Formål med kravene: sikre at leverandøren håndterer eventuelle informasjonssikkerhetsbrudd.		Veiledning til krav	Referanse
12.1	Leverandør skal ha en dokumentert prosess for hendelseshåndtering, inklusive registrering, kategorisering og rapportering av hendelser. Prosessen skal ha en klar beskrivelse av hva som skal utløse rapportering til kommunen.	Kravet skal sikre at leverandør er i stand til å håndtere eventuelle sikkerhetsbrudd, og at kommunen blir informert.	ISO 27002 16.1

12.2	Leverandør skal ha et fungerende avvikssystem. Systemet skal fange opp og håndtere informasjonssikkerhetsavvik.	Kravet skal sikre at leverandøren har et regime for innmelding og håndtering av avvik. Avvik kan resultere i sikkerhetsbrudd.	ISO 27002 ??.?
Virksomhetskontinuitet Formål med kravene: sikre at leverandøren har robuste og redundante tjenester.		Veiledning til krav	Referanse
13.1	Leverandør skal ha tilstrekkelig beredskaps- og kontinuitetsplaner for å sikre tilgjengelig på tjenesten i henhold til SLA.	Kravet skal sikre at leverandør er i stand til å levere tjenesten ved uforutsette hendelser som strømbrudd, flom eller andre hendelser. Beredskaps- og kontinuitetsplaner er viktige for at leverandøren skal kunne oppfylle sine forpliktelser i SLA-avtalen.	ISO 27002 17.1
13.2	Tjenesten skal være beskyttet mot tjenestenektangrep.	Kravet er aktuelt dersom leverandør tilbyr tjenesten i sitt miljø (skytjeneste). Kravet skal sikre tilgang dersom trusselaktører gjennomfører tjenestenektingsangrep (ddos) mot leverandørens nettverk. Det er imidlertid sjelden mulig å gi fullverdig beskyttelse mot slike angrep.	ISO 27002 17.2
Samsvar Formål med kravene: sikre at leverandøren leverer innenfor lovverket og sine kontraktsforpliktelser.		Veiledning til krav	Referanse
14.1	Leverandør skal sikre at alle leveranser til kommunen skjer i henhold til norske lover og regler.	Kravet er et generelt krav om at leverandør skal følge norske lover og regler.	ISO 27002 18.1
14.2	Leverandør skal minimum en gang i året foreta en uavhengig gjennomgang av informasjonssikkerheten. Gjennomgangen skal sikre samsvar med policyer og standarder, samt teknisk samsvar.	Kravet skal sikre at leverandør får en tredjepart til å «se seg i kortene». En tredjepart kan være en innleid konsulent.	ISO 27002 18.2
14.3	Kommunen skal kunne gjennomføre revisjon av leverandøren eller dens underleverandør, enten selv eller gjennom tredjepart.	Kravet skal åpne for at kommunen kan iverksette revisjon av leverandøren.	ISO 27002 18.2