Informasjonssikkerhetskrav ifbm skytjenester

Skytjenester Formål med kravene: sikre regulering av leverandør som tilbyr tjenester i skyen (SaaS).		Veiledning til krav	
1	Leverandør skal ha en etablert prosess for å identifisere, vurdere og prioritere trusselbildet. Det bør også arbeides aktivt for å begrense sårbarheter.	Kravet skal sikre at leverandør skal gjennomføre trussel- og sårbarhetsvurderinger.	R1 ISO 27001
2	Leverandør skal yte bistand dersom kommunen ønsker å avslutte avtalen. Leverandør skal legge til rette for at kommunens data blir overført til kommunen eller til tredjepart utpekt av kommunen.	Kravet skal sikre at kommunen ikke havner i en lock-in situasjon, ved at de ikke får ut informasjonen som er lagt inn i tjenesten i et hensiktsmessig format.	R2
3	Data som overføres over nettverk skal sikres. Dette gjelder både data som overføres til og fra tjenesten, internt i tjenesten og data som utveksles med andre tjenester.	Kravet skal sikre mot endring og avlytting av data under overføring.	R3 ISO 27002 13
4	Leverandør skal forhindre uautorisert tilgang til sitt datasenter, samt beskytte mot tyveri, skade, tap og at utstyr svikter for å sikre kontinuerlig drift.	Kravet skal sikre den fysiske adgangen i leverandørens datasenter.	R4 ISO 27002 11
5	Det skal defineres, velges, dimensjoneres og implementeres passende kryptografiske mekanismer av en tilstrekkelig nøkkeladministrasjonsinfrastruktur for å sikre sikker drift av tjenestene. Dette gjelder data i ro så vel som datastrømmer.	Kravet skal sikre lagret informasjon ved hjelp av kryptografi.	R5 ISO 27002 10
6	Leverandør skal skille kommunens tjenester og data fra andre kunder.	Kravet skal sikre separasjon mellom kundene.	R6 ISO 27002 12
7	Leverandør skal dokumentere hvordan data slettes, og hvordan slettede data ikke kommer på avveie eller kan gjenskapes.	Kravet skal sikre at leverandør sletter kommunes data, for eksempel i forbindelse med opphør av avtalen.	R7 ISO 27002 8

8	Tjenesten skal være tilgjengelig for kommunen når kommunen har behov for det. Leverandør skal garantere oppetid og dokumentere historisk oppetid/tilgjengelighet.	Kravet skal sikre at tjenesten er tilgjengelig ved behov.	R8 ISO 27002 17
9	Leverandør skal ha en prosess for å håndtere endringer for å sikre at endringer som kan påvirke sikkerheten identifiseres og håndteres, og at uautoriserte endringer kan oppdages.	Kravet skal sikre at leverandør har en prosess for endringshåndtering.	R9 ISO 27002 12
10	Alle handlinger som utføres av leverandøren skal logges. Loggen skal ikke kunne manipuleres. Kommunen skal ha tilgang til loggene etter behov. Kommunen har rett til å revidere leverandørens virksomhet knyttet til behandling av kundens data, eller å få innsyn i revisjonsrapporter fra en uavhengig tredjepart med revisjonsrett.	Kravet skal sikre sporbarhet i tjenesten.	R10 ISO 27002 12
11	Løsningen å ha tilstrekkelig isolasjonsstyrke og robusthet i tilgangskontroll.	Kravet skal sikre god tilgangskontroll og autentisering.	R11 ISO 27002 9
12	Leverandør skal ha en tilstrekkelig sikkerhetsovervåking av tjenesten og rutiner for varsling av hendelser. Leverandør skal på forespørsel gi kunden 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 overføres til kommunen på forespørsel.	Kravet skal sikre at leverandør har en god prosess for håndtering av eventuelle sikkerhetsbrudd, herunder varsling til kommunen.	R12 ISO 27002 12 ISO 27002 16