Generelle krav til informasjonssikkerhhet og personvern ved kjøp av skytjenester

Krav-ID	Krav	Dokumentasjonskrav	Beskrivelse
K1	Leverandøren skal ha en løpende prosess for å identifisere, vurdere og håndtere sårbarheter i tjenesten.	Beskriv prosessen for trussel- og sårbarhetsvurderinger. Beskriv også hvordan sårbarheter håndteres og hvilke prosedyrer med tidsrammer som brukes for de ulike typer av sårbarheter.	
K2	Leverandøren skal yte bistand til Kunden dersom Kunden ønsker å avslutte avtalen. Leverandøren skal legge til rette for at Kundens data blir overført til Kunden eller til tredjepart utpekt av Kunden.	Beskriv hvilken bistand som ytes i forbindelse med avslutning av avtalen og hvilke aktiviteter med ansvarsmatrise for de ulike aktivitetene dersom Kunden ønsker å flytte Tjenestene. Beskriv hvilke forutsetninger som legges til grunn for slik bistand og hvilke begrensninger som gjelder. Bistanden skal prises i Prisbilaget.	
K3	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.	Beskriv hvordan data under overføring beskyttes, herunder beskyttelse av nettverk og bruk av kryptering.	
K4	Leverandør skal forhindre uautorisert tilgang til sine datasenter samt beskytte mot tyveri, skade, tap og at utstyr svikter for å sikre kontinuerlig drift.	Beskriv hvilke fysiske sikringstiltak som benyttes i de datasenter som brukes for å levere tjenesten slik at uvedkommende ikke får tilgang til data, systemer og utstyr.	
K5	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 (data at rest) så vel som data i bevegelse (data in transit).	Beskriv hvordan plattform og lagrede data sikres ved bruk av kryptering. Beskriv hvordan krypteringsnøkler håndteres. Hvordan sikrer man skille mellom administrasjon av krypteringsnøkler og bruk av krypteringsnøkler.	
K6	Leverandøren skal skille kundens tjenester og data fra andre kunder.	Beskriv hvordan kundenes tjenester og data skilles fra hverandre og hvordan kunden kan forsikre seg om denne separasjonen.	
K7	Leverandøren skal kunne dokumentere hvordan leverandøren sletter data og hvordan leverandøren sikrer at slettede data ikke kommer på avveie eller kan gjenskapes.	Beskriv hvilke tiltak og prosedyrer som er etablert for sletting av data og for å sikre at data som er slettet ikke blir tilgjengelig for andre eller kan gjenskapes. Beskriv også hvordan du sikrer at slettede data ikke blir tilgjengelig ved utskifting og fornyelse av infrastruktur.	
K8	Tjenesten skal være tilgjengelig for kunden når kunden har behov for tjenesten. Leverandøren skal kunne garantere oppetid og dokumentere historisk oppetid/tilgjengelighet.	Beskriv den garanterte tilgjengelighet og dokumenter oppetidsgarantien med historiske data. Dersom det brukes ulike tilgjengelighetsgarantier, så skal disse beskrives og hvilke betingelser som gjelder for de ulike garantiene. Beskriv hvilke tiltak og prosedyrer som er etablert for å sikre tjenestens robusthet og tilgjengelighet.	
K9	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.	Beskriv prosessen for endringshåndtering for både utvikling, integrasjoner, applikasjoner, nettverk og systemkomponenter. Beskriv også hvordan endringshåndtering ivaretas i hele verdikjeden for tjenesten. Beskriv i tillegg hvordan leverandøren sikrer at det kun er autoriserte endringer som blir implementert i tjenesten.	
K10	Alle handlinger som utføres av leverandøren skal logges. Loggen skal ikke kunne manipuleres. Kunden skal få tilgang til loggene på forespørsel. Kunden 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.	Beskriv hvordan og på hvilket detaljnivå handlinger utført av leverandøren som kan endre eller eksponere data logges, og hvordan loggene sikres mot manipulasjon. Beskriv hvordan kunden får tilgang til disse loggene. Beskriv kundens rett til revisjon av leverandørens virksomhet knyttet til behandling av kundens data.	
K11	Løsningen skal ha tilstrekkelig isolasjonsstyrke og robusthet i tilgangskontroll. Leverandør skal tilby verktøy for administrasjon av kundens brukere og deres tilganger og ha tilstrekkelig støtte for bruk av eksterne identitetstilbydere.	Beskriv hvordan løsningen kan sikre at kunden kan autentiseres, autoriseres og administrere tilganger for personer, prosesser eller applikasjoner, og hvordan slik tilgang kan etterprøves (audit). Dette inkluderer muligheter for Single Sign-on (SSO), multifaktor autentisering (MFA), føderasjon med eksterne identitetstilbydere, integrasjon med identitetshåndteringsløsninger (IdM) og aksessloggmuligheter.	
K12	Leverandøren skal ha tilstrekkelig sikkerhetsovervåkning av tjenesten og rutiner for varsling ved hendelser. Leverandør skal på forespørsel gi kunden tilgang til revisjonsrapporter for vurdering av sikkerhetsovervåkningen, vurdering av tilgangsstyringen til systemer og komponenter for leverandørens egne administratorer og hvilke prosedyrer og rutiner de har for varsling. Sikkerhetslogger gjøres tilgjengelig for kunden på forespørsel.	Beskriv prosesser, rutiner og funksjonalitet som utgjør sikkerhetsovervåkingen av løsningen, og beskrive hvilke type loggdata som kan tilgjengeliggjøres for kunden (definerte og valgfrie sikkerhetsalarmer, sikkerhetsadvarsler og sikkerhetsloggingstjenester). Leverandøren skal beskrive hvordan sikkerhetslogger, alarmer og advarsler kan integreres med Kundens egen sikkerhetsovervåking. Leverandøren bes beskrive hvordan de bruker ekstern penetrasjons- og sikkerhetstesting eller andre mekanismer for testing og kontroll av applikasjons- og infrastruktursikkerhet.	