Kravspesifikasjon Lnett AS - Overordnede krav

Nr	Krav-kode	Krav	Leverandør svar J = Ja, ligger i løsningen JU = Ja, vil utvikles N = Nei	Leverandørbeskrivelse (eller referanse til andre beskrivelser)
		Overordnede krav til sikkerhet i løsningen		
1	A	Leverandøren skal gjennom kontraktsperioden kunne dokumentere at det arbeides systematisk med kvalitet og informasjonssikkerhet og bekrefte at de følger kravene som er stilt i kvalifiseringen jf. ISO 27001 og 9001 eller tilsvarende standarder eller rutiner.		
2	A	Leverandøren skal dokumentere at løsningen utvikles i henhold til 'best practise' som ivaretar kvalitet i produktutviklingsprosessen.		
3	A	Kundens data skal lagres og behandles innenfor EU/EØS-området. Tjenesten og alle dens komponenter skal behandle, lagre og transportere data innenfor EFTA, EØS/EU. Beskriv overordnet dataflyt.		
4	A	Leverandøren og underleverandører som benyttes for å oppfylle kontrakten, skal medvirke til og stille sine systemer til disposisjon, slik at norske beredskapsmyndigheter kan føre tilsyn for å sikre at etterlevelse og taushetsplikt for kraftsensitiv informasjon overholdes.		
5	A	Løsningen skal ha funksjonalitet for å sikre at data, dokumenter og filer som lastes opp eller ned, kontrolleres for potensiell skadevare.		
6	A	Leverandøren skal dokumentere at det arbeides systematisk med sikkerhetsoppgraderinger og utvikling av løsningen. Krav til dokumentasjon: Leverandørens beskrivelse, eller vedlagt produkt roadmap og/eller realease strategi for oppdateringer/sikkerhetspatcher.		
7	A	Leverandøren skal sikre at det ikke gis uautorisert tilgang til kundens data. Dokumenter hvordan kravet oppfylles, herunder tiltak for å segregere data og hvordan kunden sin spesifikke konfigurasjon og datalagring er skilt fra andre leietakere/kunder. Beskriv også hvordan separasjonen vil bli støttet på plattform- og infrastrukturnivå.		
8	A	Løsningen skal beskytte konfidensialiteten, integriteten og tilgjengeligheten til kundens data fra uautorisert tilgang eller modifikasjon av tredjeparter.		
9	A	All data som overføres mellom løsningen og kundens tredjepartssytemer skal krypteres basert på anerkjente krypteringsstandarder. Beskriv hvilken standard som benyttes og revisjonsnummer.		
10	A	Alle data som ligger i løsningen skal lages kryptert etter anerkjente standarder for sikker kryptering. Beskriv hvilken standard som benyttes og revisjonsnummer, samt hvordan kunden sikres kontroll med bruk av krypteringsnøkler.		
11	A	Leverandøren skal dokumentere sine rutiner og kontroll for nøkkeladministrasjon av krypteringsnøkler. Beskriv hvem som har tilgang til nøklene og hvordan det sikres et skille mellom administrasjon av krypteringsnøkler og bruk av krypteringsnøkler. Beskriv hvordan logger kan gjøres tilgjengelig for kunden.		

12	A	Leverandørens skal sørge for at alle endringer inkl. kundespesifikke endringer er forsvarlig testet før det flyttes til produksjonsmiljø. Beskriv testprosedyrer og arbeidsmetodikk for å redusere feil når spesifikke tilpasninger implementeres i løsningen.		
13	A	Alle integrasjoner i løsningen skal beskyttes med tilstrekkelig sikkerhet slik at uautorisert tilgang forhindres.		
14	A	Leverandør skal sikre at underleverandører blir gjenstand for de samme sikkerhetskrav som leverandøren selv påtar seg.		
15	A	Alle endringer som kan påvirke tjenestens sikkerhet skal identifiseres, og håndteres for å hindre utilsiktede hendelser. Beskriv prosessene for oppdateringer og oppgraderinger av løsningen.		
16	A	Løsningen skal ha single-sign-on (SSO) for pålogging fra Microsoft Entra ID (Entra ID, tidligere Azure AD).		
17	A	Løsningen skal støtte multifaktorautentisering.		
18	A	Leverandøren skal ha rutiner for varsling uten ugrunnet opphold til kunden og tredjeparts driftsleverandører ved sikkerhetshendelser. Beskriv prosedyre for varsling til kunden uten ugrunnet opphold, herunder hvordan slike hendelser håndteres internt hos leverandøren.		
19	B	Leverandøren skal sikre at hendelser og aktiviteter som f.eks. av- og pålogging, skrive- og lesetilgang, logges og gjøres tilgjengelig for kunden på forespørsel. Beskriv rutiner for dette og hvor lenge loggene lagres.		
20	B	Løsningen skal gjennomgå periodisk ekstern penetrasjonstesting og/eller andre sikkerhetsvurderingsmetoder i regi av leverandør i kontraktsperioden for å verifisere at løsningen opprettholder det avtalte sikkerhetsnivå og avdekke evt. svakheter i løsningen. Vis dokumentasjon på at dette er gjennomført.		
21	B	På kundens forespørsel skal leverandøren tilgjengeliggjøre løsningen for penetrasjonstesting enten i regi av kunden eller at leverandøren selv gjennomfører dette. Leverandøren skal kostnadsfritt stille nødvendig personell til disposisjon for å få gjennomført testingen.		
22	B	Leverandøren skal beskrive hvordan sårbarhets- og risikovurderinger brukes som en del av Informasjonssikkerhets og kvalitetsarbeidet ved utvikling og drift av løsningen. Vurderingen skal også dekke tredjeparts ytelser (underleverandører). Dersom leverandøren har ISMS (Information Security Management System) eller tilsvarende rutiner ber vi om beskrivelse av hvordan risiko- og sårbarhets vurderinger brukes i arbeidet.		
23	B	Leverandøren skal hindre uautorisert fysisk adgang til datasenter som oppbevarer kundens data. Beskriv hvordan dette ivaretas. Beskriv hvem som eier og driver datasentre og infrastruktur som brukes til produksjon av tjenesten, hvilke fysiske og miljømessige sikkerhetstiltak som er på plass og hvilke sikkerhetsstandarder for datasentre leverandøren overholder. Dokumenter hvor data lagres og i hvilken geografisk plassering data lagres, både sikkerhetskopierte data og data i produksjon.		
		Løsningens tilgjengelighet		

24	A	Leverandøren skal sikre tilgjengelighet på løsningen ved å ha rutiner for back up og gjenoppretting av kundens data og tjenester. Beskriv hvor ofte det tas back up, hvor lenge sikkerhetskopiene lagres og hvordan sikkerhetskopiene sikres mot uautorisert tilgang og de rutiner som foreligger for disaster recovery.		
25	A	Løsningen må kunne gjenopprettes innen max. 8 timer (innenfor normal arbeidstid mellom kl. 08-16 på arbeidsdager)		
26	A	Leverandøren skal sikre at løsningen er tilgjengelig med en opptid 24/7/365 på minimum 98 %. Dokumenter løsningens tilgjengelighet på servernivå.		
27	A	Leverandøren skal sikre at løsningen er tilgjengelig i tidsrommet kl. 08-16.		
28	A	Planlagt vedlikehold skal gjennomføres utenfor tidsrommet kl. 08-16. Dersom planlagt vedlikehold må gjennomføres i angitt tidsrom skal kunden varsles minimum 5 dager før.		
29	B	Leverandøren skal sikre at løsningen er tilgjengelig med minst mulig latency/tid på transaksjoner. Dokumenter løsningens standard latency/tid på transaksjoner.		
		Krav til integrasjon		
30	A	Leverandøren er ansvarlig for at løsningen kan integreres mot Microsoft Dynamics 365 Finance (D365 Finance).		
31	A	Leverandøren er ansvarlig for at løsningen kan integreres mot Microsoft 365. Beskriv hvordan sluttbrukeropplevelsen kan integreres med Microsoft 365 tjenester.		
32	A	Leverandøren skal beskrive behov for assistanse fra kunde mht. nødvendige ressurser og støtte for å sikre tilstrekkelig bistand slik at implementering av og integrasjoner av løsningen lykkes.		
33	B	Utover de integrasjonskrav (A-krav) som er nevt over skal leverandøren også beskrive og gi anbefalinger til hvordan løsningen kan best settes opp for å sikre samhandling med andre av kundens eksisterende systemer. Vedlegg C gir oversikt over kundens eksisterende systemlandskap og indikerer de systemene som anses som relevante for integrasjon eller annen direkte dataoverføringer mot løsningen på sikt. Beskriv i hvilken prioritet de nevnte systemer bør implementeres i løsningen for å få best mulig utbytte tidligst mulig.		
34	B	Løsningen skal være API-sentrisk. Beskriv hvordan løsningen støtter dette og hvordan API'ene er dokumenter		
35	B	Kunden og kundens tredjeparts IT-driftsleverandør skal ha tilgang til oppdatert dokumentasjon av den leverte løsningen. Beskriv hvordan kunden og kundens tredjeparts IT-driftsleverandør vil få tilgang til oppdatert dokumentasjon av den leverte løsningen.		
		Kundens brukerrettigheter i løsningen		
36	A	Kunden skal ha redigerings rettigheter som gjør det mulig å endre og konfigurere daglige endringer i løsningen (eks. sette opp enkle arbeidsflyter, legge til/redigere verdier i datafelt, revidere/legge til nye maler, sjekklister etc.) uten ekstern støtte. Beskriv hvilke endringer som kan gjøres av kunden uten ekstern støtte.		
37	A	Kunden skal selv kunne legge inn nye brukere og styre brukertilgang i løsningen.		
38	B	Løsningen skal ha funksjonalitet som gjør det mulig å ha tilgangsstyring på bruker og gruppenivå, f.eks. for porteføljeansvarlig, programansvarlig, prosjektleder, prosjektteam og til "alle" medarbeidere hos kunden med behov for lesetilgang. Beskriv hvordan dette håndteres i løsningen.		

		Øvrige krav		
39	A	Alle supporthenvendelser til løsningen skal gå gjennom kundens supportportal som driftes av tredjeparts IT-driftsleverandør. Leverandør må inngå en OLA avtale (operational level agreement) med slike tredjeparter.		
40	A	Leverandører skal sikre at løsningen er tilgjengelig for kunden med avtalt funksjonalitet.		
41	A	Leverandøren skal beskrive løsningens systemdesign og funksjonalitet i form av en systemarkitekturskisse eller tilsvarende. Denne skal gi kunden en oversikt over løsningens hovedkomponenter og hvordan disse samhandler og kommuniserer med hverandre. Med hovedkomponenter menes eksempelvis applikasjoner, databaser og tjenester og lignende.		
42	A	Kundens data skal være mulig å eksportere/importere til løsningen i åpne formater (eks. CSV, Excel etc.). Eventuelle kostnader skal synliggjøres og legges inn i prisskjema.		
43	A	Løsningen skal håndtere personopplysninger i samsvar med gjeldende personvernlovgivning.		
44	A	Kunden eier egne data i løsningen. Kunden skal beholde eierskapet til sine data under hele kontraktsforholdet, og etter at kontrakten er avsluttet til data er flyttet og/eller slettet fra tjenesten.		
45	A	Leverandøren skal sikre at kundens data ikke brukes til egne formål eller videreformidles til andre parter uten samtykke fra kunden. Dette gjelder også metadata om kundens informasjon (trafikkvolum, tidspunkt, hyppighet, kommunikasjonspunkt osv.)		
46	A	Endringer i leverandørens løsning skal varsles innen rimelig tid før endringen implementeres i løsningen. Oppdatert dokumentasjon skal sendes til kundens og tredjeparts driftsleverandører. Angi eksisterende rutiner for varsling av kunder mht. endringer i løsningen.		
47	A	Leverandøren skal sikre at kunden beholder rettigheter til all data som produseres i løsningen.		
48	A	Hvis klientprogram kreves, skal det være mulig å distribuere med Microsoft Intune.		
49	A	Løsningen skal aksesseres fra de mest vanlige nettlesere. Leverandøren skal spesifisere hvilke eventuelle nettlesere som ikke kan benyttes.		
50	A	Løsningen skal ha en hjelpefunksjon hvor brukerne kan finne tips, råd, støttemateriell og informasjon om hvordan de ulike funksjonene kan benyttes.		
51	A	Leverandøren skal ha tilstrekkelig personell ute i kundens virksomhet ved gjennomføringen av implementeringen av løsningen. Dokumenter hvor mange ressurser leverandøren tenker er tilstrekkelig og antall timer som forventes i tilknytning til dette for ca. 50 brukere i kundens virksomhet.		
52	A	Leverandøren skal i tilknytning til implementeringsfasen tilby opplæring onsite før implementering i form av workshop. Beskriv hvilken opplæring som kan tilbys og beskriv ressurspådrag og antall timer for dette.		

53	A	I tilknytning til go live skal leverandøren ha personell tilgjengelig for støtte og opplæring onsite. Beskriv hvilken opplæring som tilbys, og beskriv ressurspådrag og antall timer for dette.		
54	B	Leverandøren skal jevnlig gi kunden en oversikt over lisensbruk og gi innspill til kost effektiv lisensadministrasjon. Beskriv rutiner for varsling av lisensvolum før kunden når maksimalt antall lisenser.		
55	B	Løsningens språk foretrekkes på norsk men skal som et minimum inkludere engelsk. Vennligst beskriv oppfyllelse av tilpasning til norsk.		
56	B	Løsningens eksisterende datamodell skal dokumenteres. Det skal være mulig å tilpasse datamodellen i løsningen. Beskriv hvordan kunden kan tilpasse denne med eks. egendefinerte felt og objekter, herunder hvordan endring/tilpassing av datamodellen påvirker løsningens støtte og oppgrader barhet.		