

Bilag 1 Vedlegg 1: Kravspesifikasjon

Overordnet beskrivelse av og krav til de ytelser Rammeavtalen gjelder

Leverandøren skal fylle inn sin besvarelse fra og med punkt 2 som forklart i punkt 1.

Utfylt dokument anses som SSA-R Bilag 1 Vedlegg 1.

1. Innledning

Bilag 1 Vedlegg 1 Kravspesifikasjon inneholder en beskrivelse av formål, behov og krav som skal dekkes av Rammeavtalen. Kravene er utarbeidet av Hedmark IKT som fra 1.1.2023 vil endre organisasjonsform og navn til Indigo IKT IKS (heretter kalt «**Kunden**» eller «**HIKT**»). I SSA-R Bilag 1 står det hvem HIKT kan bestille på vegne av, og slike virksomheter vil i avtaleperioden anses som Kunden i rammeavtalen.

1.1. Kravtyper og kravbesvarelse

Kravbeskrivelsen: Er Kundens beskrivelse av et behov, en ytelse eller en funksjon.

Kravtype: Alle kravene i denne kravspesifikasjonen vil være av en av følgende to kravtyper:

- **SKAL-krav – «S»:** Minimumskrav til tilbudte løsning. Manglende oppfyllelse av et SKAL-krav er normalt et vesentlig avvik fra kravspesifikasjonen og vil ofte medføre at tilbudet blir avvist. Det er begrensede muligheter for Leverandøren til å sørge for oppfyllelse gjennom forhandlinger og reviderte tilbud:
 - SKAL-krav blir ikke evaluert og tilhører derfor ingen av tildelingskriteriene
 - SKAL-krav skal besvares som "Oppfylt" eller "Ikke oppfylt", og utfyllende besvarelse kan bli etterspurt, for å kunne verifisere eller sannsynliggjøre at kravet oppfylles
 - HIKT understreker at det kun er SKAL– krav (S) som er minimumskrav i denne konkurransen.
 - Dersom annet ikke er oppgitt, skriv maksimalt en halv A4 side der oppfyllelse av et SKAL-krav skal beskrives eller forklares.
- **BØR-krav – «B»:** Evalueringskrav knyttet til tilbudte løsning. Kunden vil evaluere Leverandørens besvarelse av BØR-krav opp mot tildelingskriteriene angitt i konkurransegrunnlaget. Manglende oppfyllelse av BØR-krav vil ikke medføre avvisning av tilbudet.

1.2. Definisjoner

Begrep og forkortelser	Beskrivelse
Bruker	De personene som benytter Tjenesten. Omfatter innbyggere, medarbeidere og ansatte i virksomhetene.
Informasjonssikkerhet	Informasjonssikkerhet handler om å beskytte informasjon, informasjonsbærere og miljøet hvor informasjonen behandles, mot uønskede hendelser og handlinger. Dette innebærer at informasjon beskyttes mot uautorisert innsyn (konfidensialitet), uautorisert endring (integritet) og at den er tilgjengelig når det er behov for den (tilgjengelighet).
Klient	For Rammeavtalen benyttes alle definisjoner som inntatt i GDPR artikkel 4, se GDPR artikkel 4 nr. 7 for definisjon av Behandlingsansvarlig.

Begrep og forkortelser	Beskrivelse
Leveransen	Samlebegrep for alle Tjenester levert av Leverandøren gjennom Rammeavtalen.
Løsningen	Fellesbetegnelse på de systemer, løsninger og applikasjoner som utgjør Leveransen.
Personvern	Retten til et privatliv og retten til å bestemme over egne personopplysninger. Det er ikke alle verdier en virksomhet besitter som det bare er opp til virksomheten å avgjøre om skal beskyttes. Også verdier som må sikres pga. f.eks. offentlige krav, avtaler med andre eller symbolverdier som kan være attraktive terrormål, må derfor identifiseres (NSM).
Rammeavtalen	Denne rammeavtalen med bilag og vedlegg.
Responstid	Med responstid menes her tiden fra en hendelse oppstår til Leverandøren starter arbeidet med å finne en løsning eller svar på hendelsen.
SLA	Service Level Agreement (tjenesteavtale med standard tjenestenivå og standardiserte sanksjoner).
Virkedager	Alle dager i Norge som ikke er søndager eller lovfestede helge- og høytidsdager.

2. Kundens krav

2.1. Overordnede krav

Nr.	Kravbeskrivelse:	Krav type:
1	Leverandøren skal tilby lisenser for on premisse bruk av Commvault og NetApp. Leverandøren skal ha partnerstatus, eller tilsvarende, for Commvault og NetApp.	S
2	Leverandøren bør kunne tilby Support tilknyttet Commvault og NetApp og drift av Kundens backupløsning. Support omfatter eventuelle avtaler med underleverandører og eksternt supportapparat bør beskrives.	B

3	Leverandøren bes oppgi standard responstider ved feil, dokumentasjon for supportapparat, og eventuelle underleverandører skal beskrives. Leverandøren bes vedlegge standard SLA eller supportvilkår.	B
4	Kunden bør kunne forholde seg til én Leverandør ved support-henvendelser (Single Point Of Contact – «SPOC»).	B
5	Leverandøren bør ha kort responstid for support-henvendelser.	B
6	Konsulenter hos Leverandøren bør ha kompetanse og erfaring på produktet samt infrastruktur.	B
7	Leverandøren bør ha rutiner for sanksjoner ved forsinket ved mangelfulle leveranser.	B
8	Leverandøren bør ha 24/7-365 support inkludert vaktordning.	B
9	Leverandøren bør tilby opplæring.	B
10	Leverandøren bør tilby konsulenttjenester knyttet til drift og support av backup-tjenester basert på Commvault og NetApp.	B

2.2. Informasjonssikkerhet og personvern

Nr.	Kravbeskrivelse:	Krav type:
11	Leverandøren bør beskrive hvordan tilfredsstillende behandling av personopplysninger i tråd med personvernregelverket skal oppnås og gjennomføres.	B
12	Leverandøren bør tilfredsstillende de generelle kravene til behandling av personopplysninger som angitt i GDPR artikkel 5.	B
13	Nasjonal Sikkerhetsmyndighet (NSM) har utarbeidet grunn-prinsipper for IKT-sikkerhet som i skrivende stund er versjon 2.0. Her defineres et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenestene leverandøren tilbyr mot uautorisert tilgang, skade eller misbruk. IKT-sikkerhet hos Leverandøren bør være på nivå med grunnprinsippene som angitt av NSM eller bedre.	B
14	Leverandøren bør gjøre dokumentasjon eller opplysninger om Leverandørens informasjonssystem og sikkerhetstiltak tilgjengelige for Kunden.	B

15	Leverandøren bør ikke overlate personopplysninger til andre for lagring, bearbeidelse eller sletting uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra Kunden.	B
16	Leverandøren bør gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i forhold til risikoen for personopplysningssikkerheten, jf. GDPR artikkel 32 om informasjonssikkerhet.	B
17	<p>Leverandøren bør ha gode rutiner for gjennomføring av risikovurderinger minimum én gang pr. år, samt i forbindelse med særskilte hendelser som sikkerhetsbrudd, endringer av betydning for informasjonssikkerhet, nye sårbarheter, ev. underleverandører med videre.</p> <p>Resultatet av de gjennomførte risikovurderingene bør gjøres tilgjengelig for Kunden på forespørsel.</p> <p>Leverandøren bør uten ugrunnet opphold opplyse Kunden om alvorlige sikkerhetsbrudd, herunder feil og mangler av alvorlig karakter.</p>	B

2.3. Opsjon

18	Leverandøren bør tilby lisenser for backup av Microsoft Office 365 data (Commvault Backup Recovery for Mail and Cloud Applications) for å dekke ca. 22 000 brukere, hvorav ca. 10 000 brukere er elever og ca 3 000 brukere er lærere.	B
----	--	---