



SSA-L Bilag 1

Kundens kravspesifikasjon

System for timeregistrering

Saksnr. 24/13671

INNHold

1	OM KRAVSPESIFIKASJONEN	3
2	FORMÅL MED ANSKAFFELSEN	3
2.1	INNLEDNING	3
2.2	MÅL	3
3	OM KUNDEN	3
3.1	AVDELINGEN PARK- OG VEIDRIFT	3
3.2	DAGENS SITUASJON.....	4
4	OMFANG AV ANSKAFFELSEN	4
4.1	OMFANG AV NY SYSTEMLØSNING	4
4.2	SKALERBAR AVTALE OG ESTIMERT OMFANG AV BRUKERE	5
4.3	IMPLEMENTERING AV LØSNINGEN	5
5	FUNKSJONELLE KRAV	6
5.1	GENERELT	6
5.2	TIMEREGISTRERING OG PLANLEGGING KNYTTET TIL KATEGORIER	6
5.3	ARBEIDSPROSESSER OG BRUKERHISTORIER	8
5.4	KARTFUNKSJONALITET	9
5.5	KRAVTABELL FUNKSJONELLE KRAV	9
6	KRAV TIL TJENESTENIVÅ	13
7	TEKNISKE KRAV	13
8	KRAV TIL INFORMASJONSSIKKERHET	15
9	OPSJONER	27
10	DEMONSTRASJON I EVALUERINGSFASEN AV KONKURRANSEN	28
11	SUPPORT OG VEDLIKEHOLD	28

1 OM KRAVSPESIFIKASJONEN

Dette dokumentet inneholder kundens krav og mål til ny systemløsning.

Krav som i kravtabellene er merket A, er absolutte krav, som leverandørens tilbudte løsning må oppfylle. Dersom de absolutte kravene ikke er oppfylt, så må tilbudet avvises.

Krav som i kravtabellene er merket T, er krav som vil bli benyttet i evalueringen av tilbudene, jf. tildelingskriteriene i konkurransegrunnlaget.

2 FORMÅL MED ANSKAFFELSEN

2.1 Innledning

Bærum kommune har som strategi at etablering av nye IT-systemer skal skje ved anskaffelse av markedsbasert programvare som allerede er i bruk hos andre kunder. Løsningen skal være på norsk.

Det ønskes en standardløsning som krever begrenset grad av tilpasning. Det skal være en SaaS-løsning.

2.2 Mål

Det ønskes en moderne, brukervennlig og hensiktsmessig løsning som gir Park- og veidrift i Bærum kommune systemstøtte for timeregistrering, ressursstyring, oversikt over maskintimer og materielt forbruk. Løsningen skal ha gode rapporteringsmuligheter for oversikt og prosjektrekskap. I tillegg skal løsningen inneholde systemstøtte for dokumenthåndtering/-tilgjengeliggjøring, samt for å kunne håndtere viktige HMS-oppgaver.

3 OM KUNDEN

3.1 Avdelingen Park- og Veidrift

Park- og Veidrift, Bærum kommune, er ansvarlige for driften av kommunens grøntarealer og veigrunn. Mye arbeid utføres på oppdrag fra andre avdelinger/enheter i Bærum kommune. Avdelingen har løpende, rutinemessig, ordinær drift, samt arbeid som utføres ad hoc etter tilleggsbestillinger. Avdelingen bruker ulike maskiner og kjøretøy i sin drift (ca. 50 stk. totalt), samt ulike typer ressurser (f.eks. stein, jord, grus, sand, plantevernmidler).

Arbeidet kan i hovedsak organiseres knyttet til følgende kategorier/underkategorier:

Kategori nivå 1 - Prosjekter (som oftest større områder/arealer).

Underkategori nivå 2 - Anlegg (mindre områder/arealer innen et prosjekt).

Underkategori nivå 3 - Element (objekter)

Underkategori nivå 4 – Aktivitet (f.eks. beskjæring, kvisting, lusing, osv.)

Se punkt 5.2 for videre skissering.

3.2 Dagens situasjon

Det er behov for digital systemstøtte for å kunne kartlegge og danne oversikt over hva vi bruker av ressurser på driften. Systemstøtten er per i dag er omtrent ikke-eksisterende, og består av Office-programmer og manuelle prosesser.

Det er behov en systemløsning som gir oversikt over antall mannskap- og maskintimer, samt kostnader av materielt forbruk, til de enkelte prosjekter. Ny digital systemløsning skal sikre at arbeidet som utføres kan kvalitetssikres, dokumenteres og kategoriseres på riktig måte.

Ledere har i tillegg behov for å planlegge bruk av ressurser (mannskap og maskiner) både på kortere og lengre sikt. Ytterligere funksjonalitet for fremdriftsplanlegging vil også være ønskelig. Eksempel på dagens ressursplanlegging:

MANNKAPSPLAN UKE 44-45

Vidar, Stine & Ragnhild	Sandvika, Bekkestua	Siste finish i anleggene før vinteren. Div beskjæring Flytting av blomsterkar	Sjekk før&etter helg
	Sandvika, Kadettangen	Fjerne jordanker fra trær	
	Plan/bestilling sommerblomster-24	Lage oversikt sommerblomstkar + beplantning 2024	
Linn	Prioriterte anlegg, inkl Stabekk sentrum	Div skøtsel.	Sjekk Stabekk før&etter helg
	HOK&Strand	Kompost HOK / nedklipp syrinfelt Strandparken	
	Kolsås og Stabekkparken	K Foryngelsesbeskjæring, beskjæring lind v/steinring	
	Helset	Beskjære lindetrær. Kompost?	
Jan&Dan	Klargjøring brøyting	Sjekk maskiner. Dekkskift. Kjøre igjennom rodene. Rydde turveier som er i brøyteroden.	Liste over porter som skal utbedres
Jon	Transport	Flytte blomsterkar, hente vikeplog hos Stave. Div transport. Ansvar for singel.	Fortsette organisering på roden
Jan, Dan, Linn, Stine, Anders	Felling risikotrær	Kun det som er akutt Oppdrag via Driftsweb Egen liste	Samkjør m/Ambulerende og meld i fra hvis noe skal til VK
Anders	Storøya	Turstier og plen. Fjerne jernskrot/ledninger stranden mot Bjerkøya	Befaring svømmehallen 7.11 09:00
	Presterud	Rydding i syrinfelt. Elvegurus langs veggen. Rette opp sirkel?	
	Gyssestad	Bortkjøring epletre.	
Andy&Seb2	Skoler	Løvhåndtering. Beskjæring.	Sjekkliste
	Vøyenenga skole	Planting buskfelt (spirea betulifolia&fagus sylvatica)	Husk kompost
	BBS vest	Urner ryddes, flyttes pga brøyting, legge på vintergrønt?	
Angela	BBS øst	Avslutte for sesong. Siste dag 15.11	Flytte blomsterkar Willetrening
	HOK/Stabekk Helsehus/Bekkestua bbs	Div bestillinger/beskjære potentilla/løvrydding&grafitti	
	Tilleggsarbeider -23	Gjennomgang med Kirsti uke 45	
Christer&Jacob	Div anlegg	Løvhåndtering. Egne anlegg og på bestilling. Bestillingsjobber	Husk Vallerhjemmet

Tidligere forsøk med ulike systemer har vist at det må være et svært brukervennlig system. Vi trenger et system som er tilpasset avdelingens drift, og som enkelt kan brukes ute på prosjektene i felt, ved hjelp av app på telefon eller smartbrett.

4 OMFANG AV ANSKAFFELSEN

4.1 Omfang av ny systemløsning

Ny systemløsning er tiltenkt å dekke følgende behov:

1. Timeregistrering for å få riktige prosjektrengskaper – gi oversikt over hva som brukes av ressurser på driften i avdelingen. Oversikt over hvem som gjør hva, og hvor.
2. Ressursplanlegging og styring av personell (mannsplanlegging/fremdriftsplan). Styring f.eks. ved å fordele oppgaver/ansvar via system.
3. Oversikt over antall maskintimer, samt kostnader av materielt forbruk.

4. Ressursstyring og oppfølging av maskiner, og services/servicebehov tilknyttet disse.
5. Kvantitative erfaringstall som gjør budsjettering, økonomisk oversikt, og fakturering mulig (i form av fakturagrunnlag).
6. Oversikt over kurs og sertifiseringer, f.eks. ift. HMS.
7. Dokumentasjon av HMS- og kvalitetsarbeid, f.eks. SJA, ulike typer logg og sjekklister, osv.
8. Avvikshåndtering og mangellister i prosjektene, med bilder og GPS-posisjonering i kart.
9. Tilgang til 3.part inn i systemet.
10. Deling og tilgjengeliggjøring av dokumenter for mannskap ute i felt.

Systemet skal kunne benyttes som en app på telefon/nettbrett, og være brukervennlig og enkelt.

4.2 Skalerbar avtale og estimert omfang av brukere

Systemet skal primært brukes av avdeling Park og Veidrift som vil ha ca. 30-40 samtidige brukere på fast basis (helårs), og i tillegg ca. 10-30 sesongarbeidere i sommersesong (ca. fra april til september). Sesongarbeidere kan typisk skiftes ut gjennom sesongen.

Avtalen skal være skalerbar og fleksibel mht. antall brukere og funksjonalitet, dvs. det må være mulighet til å legge til/slette flere brukere fortløpende, kontinuerlig etter Kundens behov, samt utvide og ev. redusere funksjonalitet. Se også punkt 8 om opsjoner. Det vil f.eks. kunne være ca. 10 ekstra samtidige faste brukere i avdelingen Idrett og Bad (ambulerende), og 2 ekstra sesongarbeidere, som har tilnærmet like bruksbehov som Park- og Veidrift. I tillegg kan det være eksterne leverandører som skal bruke tjenestene, (periodevis/ad-hoc), og forvaltere som primært har behov for lesetilgang og tilgang til data/rapporter.

Estimert antall brukere per år:	Avdeling
30-40	Park- og Veidrift faste ansatte
10-30	Park- og veidrift sesongarbeidere/eksterne brukere
10	Idrett og bad faste ansatte
2	Idrett og bad sesongarbeidere
3-10	Eiendomsforvaltning/Parkforvaltning, ev. andre
Totalt estimert ca. 30-90 brukere per år	

4.3 Implementering av løsningen

Implementeringsfasen påbegynnes umiddelbart etter kontraktsgenerering, eller etter avtale med Kunden med deltakere fra Leverandøren og Kunden.

Planlagt fremdrift for implementeringsfasen med milepælsfrister er beskrevet i SSA-L Bilag 3 Plan for etableringsfasen.

Det forutsettes tett samarbeid med Leverandøren i design og tilrettelegging av systemet og i planlegging av aktiviteter som må gjøres for å ta den nye løsningen i bruk.

Leverandøren skal i SSA-L Bilag 3 fremlegge en skisse til plan for implementeringsfasen, dersom ytterligere planlegging er nødvendig, eller dersom leverandøren ser behov for endringer fra foreløpig plan.

Opplæring

Som en del av implementeringsfasen skal Leverandøren gi alle systembrukere opplæring tilpasset deres roller og behov. Ledere, systemforvalter(e) og superbrukere må få opplæring i planleggings- og oppfølgingsverktøyene i systemet. Systemforvalter og superbrukere må få opplæring i å administrere systemet uavhengig av leverandøren. Leverandør må påregne at opplæringen helt eller delvis gjøres ute i felt med ansatte.

5 FUNKSJONELLE KRAV

Dette kapitlet inneholder omtale av funksjonelle krav som stilles til løsningen.

5.1 Generelt

Viktige prinsipper for ny systemløsning er:

- Brukervennlig.
- Løsningen og all dokumentasjon, hjelpetekster mv. rettet mot bruker skal være på norsk.
- Er i bruk hos andre kunder.
- Informasjon skal kun registreres én gang.
- Fremtidsrettet løsning som blir videreutviklet.
- Universell utforming.

5.2 Timeregistrering og planlegging knyttet til kategorier

Et sentralt behov er å enkelt kunne registrere arbeidede timer, fortløpende og i etterkant, for å få dokumentasjon på hvem som gjør hva (hvilken oppgave/aktivitet), og hvor arbeid utføres (objekt, adresse, geolokalisering e.l.). Timeregistrering skal kunne knyttes til kategorier (prosjekter) og underkategorier – for å kunne gi oversikt over timer per kategori/underkategori. Det samme gjelder også for ressursplanlegging.

Den ideelle systemløsningen gir fleksibilitet mht. nivåer av kategorier og har mulighet for minst 4 nivåer av kategorier

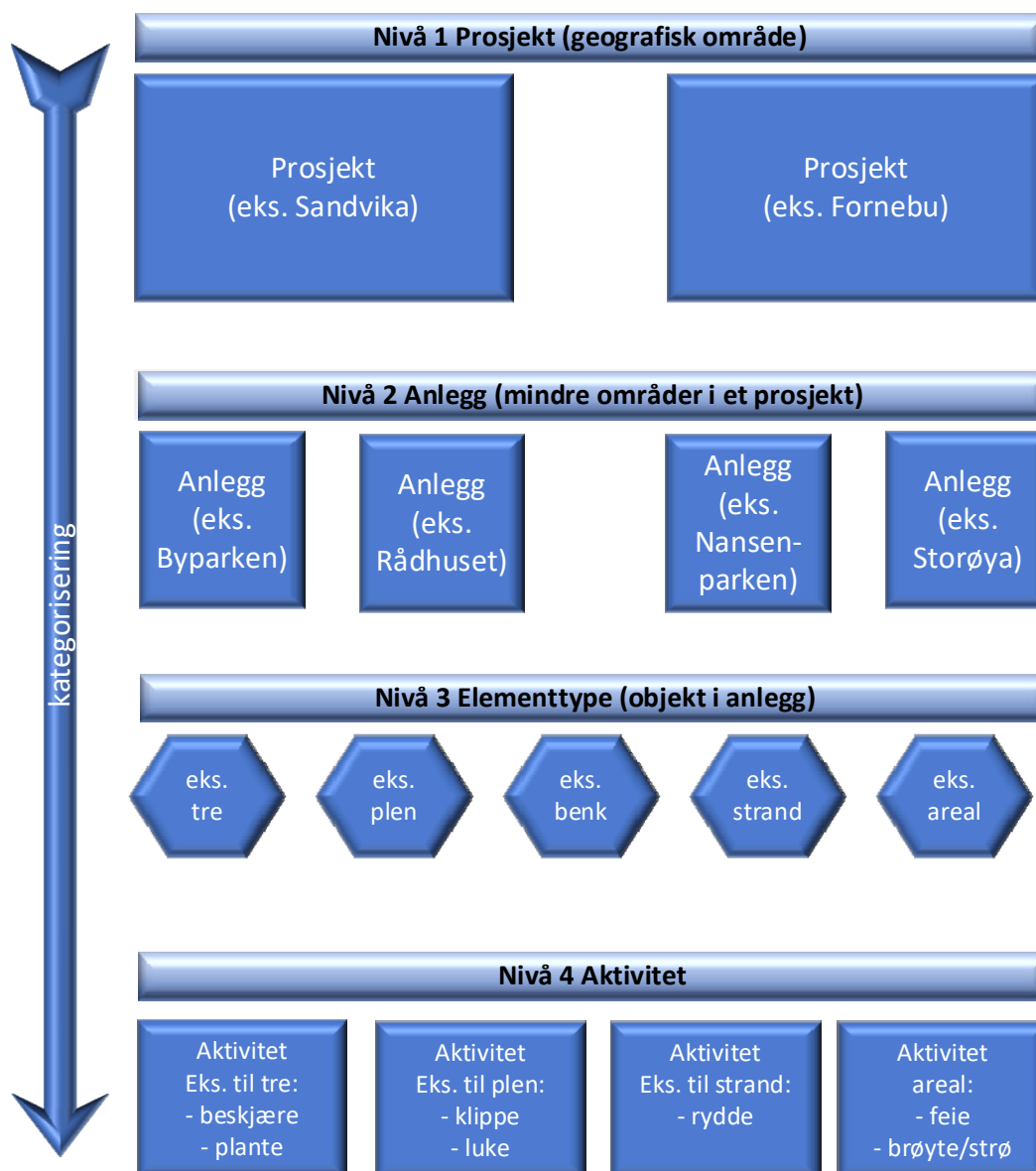
En mulig ideell kategori/underkategori-inndeling følger det som er skissert i punkt 3:

Nivå 1 – Prosjekter (som oftest større områder/arealer).

Nivå 2 – Anlegg (mindre områder/arealer innen et prosjekt).

Nivå 3 – Element (objekter)

Nivå 4 – Aktivitet



En eventuell inndeling i færre kategori-nivåer (f.eks. 3) kan også være et alternativ. I tillegg til disse kategoriene så er det viktig at det skilles på faste oppdrag og ad-hoc tilleggsbestillinger, samt ordinær arbeidstid og overtid.

Kunden har ca. 6-800 anlegg som er beskrevet i systemløsningene ISY-Park (Norconsult Information Systems) og Plania (Vitec). Det må påregnes en form for import av data fra disse anleggsregistre til ny systemløsning i implementeringsfasen. Det er ønskelig å kunne importere adresse og geografisk område (polygonfeature) per anlegg. Annen informasjon som det kan være aktuelt å tilpasse nytt system med, og ev. importere informasjon om er:

- Maskinlister, inklusive informasjon om attributer/kapasitet på maskiner.
- Materiell/ressurser.
- HMS/kvalitet/oppdragsbeskrivelser/rutiner.

5.3 Arbeidsprosesser og brukerhistorier

Nedenfor beskrives typiske arbeidsprosesser og brukerhistorier som Kunden ønsker at ny systemløsning støtter opp om på beste mulige måte. Fra brukerhistoriene er det utledet skal-krav (A) og bør-krav (T/tildelingskrav), som er i tabell i punkt 5.5. Løsningen skal støtte opp om de absolutte skal-kravene (A). Det vil videre bli gjenstand for evaluering under tildelingskriteriet for kvalitet, hvor godt løsningen støtter opp om brukerhistoriene og bør-kravene (T).

Ansatt i felt (typisk gartner, anleggsgartner, veiarbeider):

- Jeg vet at jeg skal jobbe på et prosjekt/anlegg og jeg vet hva jeg skal gjøre. I løpet av dagen kan jeg jobbe på et sted med en ting, f.eks. klippe gress ved et anlegg, men jeg kan også arbeide raskt og gjøre mange ulike oppgaver ved mange forskjellige anlegg. I løpet av arbeidsdagen, og på slutten av arbeidsdagen, vil jeg raskt og enkelt kunne registrere hva jeg har gjort, på hvilke(t) anlegg denne dagen.
- Jeg vil ha en innloggingsmetode som er enkel, rask og sikker. Jeg skal ikke registrere sensitiv personlig informasjon. Jeg kan ikke gjøre en komplisert innlogging ofte.
- De prosjekter/anlegg/elementer/aktivitetene jeg ofte pleier å registrere, kommer opp som hurtigvalg (favoritter) slik at jeg ikke trenger å lete etter de.
- I løpet av dagen kommer jeg til et anlegg som jeg ikke har vært ved på en stund, da har jeg behov for å sjekke et dokument som forteller meg om kvalitetsstandarden for anlegget.
- Jeg skal gjøre en oppgave jeg ikke har gjort på en stund med en maskin og trenger å sjekke HMS-regler for denne typen arbeid.
- Jeg skal jobbe med en maskin i løpet av dagen, f.eks. brøyte snø ved en barnehage. Jeg vil raskt og enkelt kunne registrere både hva jeg har gjort og hvor, og hvilken maskin som er benyttet, i hvor mange timer.
- Etter at det er brøytet skal jeg strø. Jeg vil kunne registrere hvor mye strøsand jeg ca. har brukt ved hvert anlegg og samlet sett i løpet av dagen.
- Jeg skal jobbe med en maskin på forskjellige steder i løpet av dagen og jeg vil kunne enkelt se hvor jeg skal være (på hvilke anlegg) og hvilken kjørerute som er best i løpet av dagen.
- Jeg fikk ikke gjort jobben min da det stod parkerte biler i veien. Jeg vil kunne legge inn dette som et avvik, knyttet til anlegget, ta bilde av det og dokumentere hvor det skjedde.
- Jeg mottok en arbeidsoppgave via systemløsningen som måtte gjøres raskt, et tre falt over veien og måtte fjernes da det sperret adkomst. Systemløsningen varslet meg om at en ny oppgave var kommet og gir meg enkelt mulighet til å registrere tiden jeg brukte på dette.
- Jeg kan enkelt se på systemløsningen hva jeg skal gjøre i dag, dersom jeg har behov for å vite det.
- Det er fint om jeg kan se hvor jeg skal være/hvor oppgaven skal utføres, på et kart.
- Lederen min ringte meg og gav meg en oppgave jeg måtte gjøre, jeg må kunne registrere tiden som jeg har brukt på dette, og på hvilket anlegg det var, selv om oppgaven ikke lå i kalenderen min.
- Dersom jeg glemmer å registrere timene mine har systemet en funksjon som minner meg på at jeg må registrere. Jeg bør kunne registrere timer for de to foregående dagene.

Tredjepart (f.eks. Parkforvaltning/Eiendomsforvaltning og eksterne leverandører av tjenester/arbeidskraft)

- Jeg jobber med parkforvaltning og trenger tidvis lesetilgang til systemet, og tilgang til rapporter.
- Jeg er en ekstern leverandør som arbeider på oppdag fra Park- og Veidrift. Jeg trenger å bruke deres systemer for å registrere timene jeg har arbeidet, hvilke maskiner/kjøretøy jeg har brukt og ressurser jeg har benyttet.

Leder

- Jeg vil enkelt kunne planlegge faste oppdrag og tilleggsarbeider for mine ansatte for de nærmeste ukene. Jeg trenger også samtidig å planlegge bruken av maskiner/kjøretøy for de ansatte.
- Jeg trenger å se når ansatte har fri/fravær for å kunne planlegge.
- Dersom planer endrer seg, kan jeg enkelt endre dette i systemet. Jeg kan legge til både faste oppdrag og tilleggsarbeider, og om jeg ønsker, så kan jeg sende varsel til den ansatte om at planen er endret, og/eller at nye oppgaver må utføres.
- Jeg skal planlegge at en eller flere ansatte skal jobbe med en eller flere maskiner på ulike anlegg. Jeg vil gjerne kunne ha mulighet til å planlegge deres arbeidsdag i form av en «arbeidsrute» med mulighet til å se i kart hvilke anlegg de skal innom den dagen, og sette opp en enkel kjørerute/prioritering av i hvilken rekkefølge det skal arbeides. Dersom det også er mulig å hensynta maskinkapasiteten (drivstoff/ladetid) ville det være fint.
- Jeg vil enkelt få oversikt over:
 - Hva mine ansatte har gjort (hvilke oppgaver), hvor (på hvilket anlegg/prosjekt), ev. også med hvilke elementer, denne uken, denne måneden og dette året, eller en tidsperiode som jeg spesifiserer selv.
 - Hvor mange timer som er brukt på ulike prosjekter/anlegg/elementer/oppgaver i løpet av en viss tidsperiode, både på kategorier hver for seg, og aggregerte kategorier (f.eks. 7 ulike anlegg).
 - Antall timeverk (knyttet til kategorier/underkategorier) som er henholdsvis *faste oppgaver*, og som er *tilleggsarbeider* (ad hoc bestillinger).
 - Kostnader og materialbruk knyttet til de ulike anlegg.
- Når noen spør hvor mye det koster å drifte et område (prosjekt/anlegg) med alt det innebærer, som bruk av mannskap, maskin/kjøretøy, og ressurser, så vil jeg kunne ha mulighet til å få oversikt over dette på en enkel måte.
- Jeg vil raskt kunne få oversikt over HMS-avvik og hvilke kategorier de er knyttet til.
- Jeg vil raskt kunne få oversikt over der vi ikke fikk gjort det vi skulle (kvalitetsavvik) og hvilke kategorier de er knyttet til.
- Det bør kunne være mulig for meg å begrense hvor langt tilbake i tid en ansatt kan registrere timer, for å hindre uriktig etterregistrering.

5.4 Kartfunksjonalitet

Ved registrering av avvik knyttet til drift (kvalitet) og HMS er det svært nyttig at disse kan geolokaliseres. Ved timeregistrering er det tilstrekkelig at timen knyttes til et prosjekt/underprosjekt med definert adresse/lokasjon, og for planlegging av oppgaver er det nyttig å kunne bruke kartfunksjonalitet. Kunden har egen kartløsning med egne kartlag som brukes i driften som gjerne ønskes benyttet, tilgjengeliggjøring kan skje f.eks. ved embedding av Kundens kartløsning i løsningen¹, lenke til Kundens kartløsning, eller ved å vise kundens kartlag (WMS-format) i egen kartløsning.

5.5 Kravtabell funksjonelle krav

Det gjøres oppmerksom på at absolutte krav (A) er krav som leverandørens tilbudte løsning må oppfylle. Dersom de absolutte kravene ikke er oppfylt, må tilbudet avvises.

¹ [Bruk av kommunekart.com-skript i eksterne websider](#)

Bør-krav (T/tildelingskrav) vil være gjenstand for evaluering, og tilbudt ytelse i henhold til kravene bes beskrives i bilag 2A, 2B og i demo.

Nr.	(A/T)	Beskrivelse
1. Generelle krav		
1.1	A	Løsningen skal være på norsk, herunder all dokumentasjon rettet mot bruker, hjelpetekster mv.
1.2	A	Løsningen skal være en skyløsning (SaaS).
1.3	T	Løsningen er brukervennlig og intuitiv med oversiktlig oppbygging, få tasteklikk, mulighet for hurtigtaster/favorittknapper/favorittmenyer, og ryddig design. Løsninger er tilpasset Kundens behov.
1.4	T	Løsningen bør kunne ivareta alle nødvendige brukerroller i prosessene beskrevet i kravspesifikasjonen på en effektiv måte.
1.5	T	Løsningen bør i størst mulig grad gi tilgang til funksjonalitet og oversikt via app på telefon og nettbrett, inklusive bl.a. lesetilgang og mulighet for registrering/endringer.
1.6	T	Løsningen bør gi tilgang til alle systemfunksjoner, og oversikt over system, via pc.
1.7	T	Løsningen bør være skalerbar og fleksibel mht. antall brukere.
1.8	T	Løsningen bør være skalerbar og fleksibel mtp. kategorier for type prosjekter, anlegg, elementer, arbeid, forbruksvarer osv.
1.9	T	Løsningen bør ha en brukervennlig funksjonalitet for å importere både lister og dokumenter. Dette omfatter lister med informasjon om anlegg, maskiner, materiell og ressurser, samt dokumenter som HMS- og kvalitetsrapporter, oppdragsbeskrivelser og rutiner. Andre importmuligheter, som for eksempel direkte import fra andre systemer via API kan også beskrives her.
1.10	T	Løsningen bør kunne gjenbruke alle relevante data slik at ingen informasjon må registreres mer enn en gang.
1.11	T	Løsningen er fremtidsrettet, blir kontinuerlig oppdatert, og utviklet videre i årene fremover.
2. Registrering av timer for personell og maskiner, og registrering av forbruksvarer		
2.1	A	Ansatte skal enkelt kunne registrere arbeidede timer, fortløpende og i etterkant, for å få dokumentasjon på hvem som gjør hva.
2.2	T	Timeregistrering kan knyttes til kategorier (prosjekter) og underkategorier (anlegg, elementer, aktivitet).
2.3	T	Timeregistrering kan skje ifb. med, eller uten, en oppgave.
2.4	T	Timeregistrering inkluderer mulighet til å sette opp regler for ordinært arbeid (fastpris- kontrakt) og tilleggsarbeider (interne kontrakter).
2.5	T	Timeregistrering bør inkludere regler for overtid og tillegg.
2.6	T	Timeregistrering bør inkludere hvor arbeid utføres, enten ved å registreres på anlegg/prosjekt (arve registrering fra kategori/underkategori), adresse, geolokalisering e.l.).

2.7	T	Timeregistrering bør gi mulighet til å legge inn avspasering, og ev. annet fravær.
2.8	T	Det bør være mulig å registrere forbruksvarer som f.eks. materiell, jord, grus, planter, gjødsel, drivstoff etc. (kvanta og varekostnad), med knytning til kategorier/underkategorier lik pkt. 2.2. Dette bør kunne skje samtidig som arbeidstimer registreres.
2.9	T	Det bør være mulig til å legge ved bilder av kvitteringer/annen dokumentasjon ved registrering av forbruksvarer for revisjon/kontroll.
2.10	T	Det bør være mulighet for lagerstyring.
2.11	T	Det bør være mulighet for å kunne registrere maskintimer opp i mot kategorier/underkategorier, og ev. være mulighet for å registrere mann og maskin samtidig, slik at en kan få oversikt over bruk av maskinene.
3. Ressursstyring og fremdriftsplanlegging		
3.1	A	Leder skal kunne fordele ansvar for oppgaver (aktiviteter), via system (app/sms), til enkeltpersoner og gruppevis. Oppgaver skal kunne knyttes til kategori og underkategori.
3.2	T	Ansatte bør lett kunne se hva de skal gjøre fremover via systemets app på telefon/nettbrett.
3.3	T	Løsningen gir leder oversikt over hva den enkelte ansatte, og grupper av ansatte, skal gjøre, ev. også hvor, fremover i tid.
3.4	T	Løsningen bør kunne gi leder overordnet oversikt over hvilke aktiviteter (oppgaver) som skal utføres i gitte perioder i året, og av hvem og eventuelt hvor.
3.5	T	Løsningen bør ha funksjon for varsling når en ansatt mottar en arbeidsoppgave (aktivitet) eller ved endring av arbeidsoppgave. Varsel kan mottas som pushvarsel i app, på e-post og SMS.
3.6	T	Ansatt/leder bør enkelt kunne legge inn/se historisk og fremtidig timeregistrering (inklusive fravær som ferie, avspasering, sykefravær osv.).
3.7	T	Det bør være mulig å legge mannskapsplaner lenger frem i tid, f.eks. et år, slik at det er mulighet for fremdriftsplanlegging ift. prosjekt/aktivitet/sesong/år.
3.8	T	Det bør være mulig å kunne bruke kart til å planlegge arbeidsoppdrag og lage enkle "kjøreruter".
3.9	T	Det bør være mulighet for ressursplanlegging av kjøretøy/maskiner .
3.10	T	Det bør være mulig å ha oversikt over service og vedlikehold for kjøretøy og maskiner, mtp. hva som er gjort når, og mulighet til planlegging av service/vedlikehold.
3.11	T	Det bør være mulighet til å få varsler når det er tid for vedlikehold/service.
3.12	T	Det bør være mulig å lagre og tilgjengeliggjøre maskindokumentasjon på ett sted som f.eks. manualer, EU-kontroll ol.
4. HMS og Kvalitet		
4.1	A	Løsningen skal gi systemstøtte for sentrale HMS-oppgaver, med mulighet til å kunne utarbeide diverse skjema/maler og sjekklister, som f.eks. -HMS-plan og kvalitetsplan (inkludert mulighet til å legge inn/opprette interne rutiner). -HMS-håndbok. - SJA.

4.2	T	Løsningen gir mulighet for å registrere og ha oversikt over kurs og sertifiseringer for den enkelte ansatt.
4.3	T	Løsningen gir systemstøtte for å lagre og tilgjengeliggjøre viktige dokumenter (for ansatte ute i felt). Dokumentene kan være knyttet til HMS, og/eller utførende oppdrag, f.eks. kontrakter, kravspesifikasjon og tilleggsbestillinger.
4.4	T	Det bør være mulig å lagre og tilgjengeliggjøre maskindokumentasjon på ett sted som f.eks. manualer, EU-kontroll ol.
4.5	T	Løsningen gjør det mulig å registrere avvik knyttet til HMS, og avvik knyttet til drift (kvalitet). Avvikene skal kunne inkludere bilder, geolokalisering i kart og/eller adresse, og det skal være mulighet til å enkelt knytte avvik opp mot kategori/underkategori.
5. Data og rapporter		
5.1	T	Løsningen har gode funksjoner for å sammenstille data, og opprette/lage/laste ned rapporter og prosjektrengskap. Leder kan ta ut overordnet og detaljerte prosjektrengskaper, f.eks. mht. antall timer/maskiner/forbruksvarer/avvik per kategori/underkategori (f.eks. prosjekt/anlegg/aktivitet og element) og i tidsintervaller. Det er fleksibilitet mht. hvilke variabler som kan benyttes, og på den måten kan leder "skreddersy" rapporter etter behov.
5.2	T	Løsningen gir mulighet til å kunne se historikk over flere år.
5.3	T	Løsningen gjør det mulig å få oversikt/rapporter over avvik både ift. drift (kvalitet) og HMS på kategori/underkategori og overordnet for avdelingen.
5.4	T	Løsningen bør ha funksjonalitet for å kunne samle data og sammenstille kvantitative erfaringstall - fra personell, maskin og forbruksmaterieil, som muliggjør budsjettering, økonomisk oversikt, og fakturagrunnlag. Løsningen bør kunne produsere et grunnlag for estimering av kostnader og/eller utarbeide tilbud knyttet til prosjekt/anlegg/element/ aktiviteter.
5.5	T	Løsningen bør kunne gi oversikt over forbruksvarer brukt per kategori/underkategori og i ulike tidsintervaller.
5.6	T	Løsningen bør kunne gi oversikt over kjøretøy/maskintimer per kategori/underkategori og i ulike tidsintervaller.
5.7	T	Det bør kunne være: - Mulighet for å hente data via API f.eks. for å lage egne dashboard og/eller deler data med andre interessenter hos Kunden. - Mulighet for å laste ned data og rapporter som f.eks. csv, Excel og pdf filer. - Mulighet for å lage regler for å sende rapporter til andre interessenter hos Kunden.
5.8	T	Det bør være mulighet til å geografisk avgrense rapportering, f.eks. se alt arbeid (timer/aktiviteter/ressurser) som er benyttet på et geografisk område, over en viss periode.
6. Annet		
6.1	T	Lese og registreringstilgang til tredjepart inn i systemet Brukere utenfor Bærum kommune bør også kunne motta bestillinger på oppdrag, lese dokumenter, registrere timer, forbruksmaterieil, maskinbruk, avvik osv. Eksterne bør kunne bruke systemet likt interne ansatte. Det er mulig å få oversikt over andelen arbeid utført/ev. ressurser/forbruksvarer som er brukt av eksterne vs. interne.

6 KRAV TIL TJENESTENIVÅ

Krav til tjenestenivå fremgår av **SSA-L Bilag 4 Tjenestenivå med standardiserte kompensasjoner**. Leverandøren skal i videre i SSA-L bilag 4 legge frem en tjenestenivåavtale (SLA) som ivaretar minimumskravene som Kunden har angitt i bilagsteksten.

7 TEKNISKE KRAV

For anskaffelsen gjelder tekniske krav som følger av nedenstående tabell.

Det gjøres oppmerksom på at absolutte krav (A) er krav som leverandørens tilbudte løsning må oppfylle. Dersom de absolutte kravene ikke er oppfylt, må tilbudet avvises.

Bør-krav (T/tildelingskrav) vil være gjenstand for evaluering, og tilbudt ytelse i henhold til kravene bes beskrives i bilag 2B Leverandørens utfylte spesifikasjonsskjema.

Nr.	(A/ T)	Beskrivelse
1. Generelle tekniske krav		
1.1	A	Leverandøren og løsningen skal oppfylle de til enhver tid gjeldende obligatoriske krav i «Referansekatalog for IT-standarder i offentlig sektor». Referansekatalog er spesifisert på Digitaliseringsdirektoratet sine sider.
1.2	A	Det skal ikke være behov for nettleseutvidelser (plug-ins), som f.eks. flash, hta, activeX
1.3	T	Løsningen bør være HTML5 basert
1.4	T	Løsningen bør ikke ha behov for å installere Java på server, eller klient.
1.6	A	Løsningen skal støtte siste versjon av alle moderne nettlelere for PC som Microsoft Edge, Apple Safari og Google Chrome.
1.7	A	Løsningen skal fungere likt på innebygget nettleser i Apple iOS (Safari - iPhone og iPad). Android (Chrome) og på PC (Microsoft Edge).
1.8	A	Mobil-applikasjonen til løsningen er til enhver tid kompatibel og fullt støttet på siste versjon av iOS og Android, og distribueres gjennom offisielle App Store.
1.9	T	Løsningen har støtte for distribusjon av konfigurasjon fra MDM. Løsningen kan motta all nødvendig konfigurasjon fra Kundens MDM-løsning.
1.10	T	Løsningens databaser kan oppgraderes til nye versjoner uten at løsningen blir påvirket (gjelder løsninger med en database)
1.11	T	Nedetider og andre meldinger om tjenesten blir kommunisert og vist til sluttbruker og Kunden sentralt
1.12	T	Løsningen kan eksportere data (i et maskinlesbart format). F.eks. ved bytte av leverandør.

1.13	A	All kommunikasjon skal være kryptert med anerkjente, gyldige, sikre protokoller. F.eks forbindelser mellom server og bruker/klient, innad i Kundens eget nettverk og over Internett. Eksempelvis HTTPS og kryptert med SSL/TLS 1.2. og sRTP. Kravet gjelder både for skyløsning og på lokal server.
1.14	A	Dersom det lagres passord i løsningen, så er disse være kryptert, ref. sikkerhetskrav 1.6.4.
2. Provisjonering, autentisering og autorisering for ansatte/styrte brukere		
2.1	T	Innlogging kan integreres mot Kundens katalogtjeneste (AD/Azure) for tildeling av tilganger (roller).
2.2	T	Beskriv løsning for føderasjon / Single sign-on (SSO) av brukere, herunder også hvilke standarder/metoder som benyttes (SAML2/OIDC osv.)
2.3	T	Beskriv støtte for MFA
2.4	T	Løsningen bør ha API (ref. 5.1) for bruker opprettelse og deaktivering, samt tilgangsstyring
2.5	T	Løsningen bør ha API (ref. 5.1) for organisasjonsstruktur
2.6	A	Løsningen skal ha tilgangsstyring som støtter «separation of concerns» (SoC) Brukere kan ha en eller flere roller, hvor tilganger som noen roller gir må separeres fra andre roller. Inkluderer også tilganger til ulike moduler/deler av løsningen (f.eks. tilgang til varslingssystem) der hvor det er aktuelt.
2.7	T	Mobile enheter og eventuelle apper bør støtte biometrisk pålogging
3. Autentisering og autorisering for eksterne/ ikke-styrte brukere		
3.1	T	Det bør være enkelt å administrere roller og tilganger til løsningen.
3.2	T	Beskriv støtte for MFA for eksterne/ikke styrte brukere.
3.3	T	Passordet kan byttes enkelt av bruker
3.4	T	Passordets kvalitet og varighet kan konfigureres.
3.5	T	Tvunget skifte av passord er teknisk mulig.
4. Tekniske krav til brukervennlighet		
4.1	A	Løsningen skal ha god responstid på alle vanlige transaksjoner og handlinger ved normal drift og full utnyttelse. Løsningen skal være skalerbar til datamengde, transaksjoner og antall brukere. I dette ligger at økning i volum på de nevnte tre områdene ikke skal medføre dårligere ytelse for sluttbruker.
4.2	T	Løsningen er uavhengig av leverandør/-er av utstyr slik som pc, skjerm, mobil og nettbrett (plattformuavhengig).
5. Integrasjon for datautveksling		
5.1	T	API-er er basert på åpne standarder, eksempelvis REST, SOAP, XML og JSON, og skal være tilstrekkelig sikret for den informasjonen som er lagret i løsningen.
5.2	T	API-ene skal ha oppdatert dokumentasjon som beskriver bruken og innholdet av API-et som skal kunne forstås av en utenforstående utvikler.
5.3	T	Det er prosesser/rutiner for varsling av nedetid, endringer av funksjonalitet/grensesnitt, melding av feil, utveksling og håndtering av hemmeligheter som sertifikater, nøkler og passord.
5.4	T	Tilbudt løsning gir mulighet til å lese og skrive direkte til sin informasjon gjennom API-er som gjør en kvalitetsvalidering, uten at dette skjer gjennom fagsystemets eget brukergrensesnitt.

8 KRAV TIL INFORMASJONSSIKKERHET

Kommunen er overordnet ansvarlig for at informasjonssikkerheten og personvernet ivaretas i de løsningene som kommunen anskaffer og benytter og som inneholder kommunens data.

Ved bruk av skytjenester er det spesielt viktig at kommunen stiller krav til informasjonssikkerhet og personvern, ettersom kommunen ikke selv kan sikre disse tjenestene og dermed er avhengig av Leverandørens tilnærming til informasjonssikkerhet og personvern.

Trusselbildet endrer seg stadig og krever nye tiltak, både tekniske og organisatoriske. Leverandøren må derfor ha gode rutiner og prosesser for å kontinuerlig kunne ivareta informasjonssikkerheten og personvernet, samt også ha en sikkerhetsarkitektur som ivaretar konfidensialitet, integritet og tilgjengelighet. Leverandøren må kunne fange opp, varsle om og håndtere sikkerhetshendelser, både organisatoriske og tekniske.

Skytjenester består ofte av lange og komplekse verdikjeder. Hendelser i verdikjeden kan medføre utilgjengelighet på løsningen og kommunens data. Leverandøren må derfor ha gode beredskaps- og kontinuitetsplaner som ivaretar kommunens krav til tilgjengelighet.

Personvernlovgivningen stiller også en rekke krav til databehandlere. Leverandøren må derfor ha nødvendig kunnskap, rutiner og prosesser for å kunne ivareta disse kravene. Dette gjelder også for kravene til innebygget personvern og personvern som standardinnstilling i løsninger, ettersom løsningen utvikles og forvaltes av leverandør i skyen.

Utfyllende krav til informasjonssikkerhet er beskrevet i nedenstående kravtabeller. Leverandørens ivaretagelse av kravene vil være gjenstand for en helhetlig evaluering, og bes beskrives i bilag 2B Leverandørens utfylte spesifikasjonsskjema.

1.1 Styringssystem for informasjonssikkerhet Formål med kravene: sikre at leverandøren har et eget styringssystem.	Utdyping av krav
---	------------------

1.1.1	<p>Leverandør har et styringssystem for informasjonssikkerhet (ISMS)</p> <p>Leverandøren bes beskrive</p>	<p>Kravet skal sikre at leverandør har et helhetlig og aktivt forhold til informasjonssikkerhet. Styringssystemet vil diktere at leverandør involverer ledelsen, gjennomfører risikovurderinger og implementerer tilstrekkelige sikringstiltak.</p> <p>Styringssystemet skal:</p> <ul style="list-style-type: none"> a) Dekke hele den tilbudte løsningen b) Beskrive ansvar og oppgaver på alle nivåer c) Sikre at ansvarsforholdene er kjent for alle i organisasjonen d) Dokumentere alle sikkerhetstiltak (organisatoriske, fysiske og tekniske) e) Fastsette sikkerhetsmål for virksomheten f) Sørge for at sikkerhetsstrategi for å nå sikkerhetsmålene er utarbeidet g) Sikre at Ledelsens gjennomgang av sikkerheten (sikkerhetsrevisjon) gjennomføres og dokumenteres minimum årlig h) Sikre at det er etablert en prosedyre for oppfølging av resultatet (avvik) av den årlige sikkerhetsrevisjonen
1.1.2	<p>Leverandør har etablert og forvalter tilstrekkelige sikkerhetstiltak for å ivareta informasjonssikkerheten for behandlingen av informasjonen i løsningen</p>	<p>Sikkerhetstiltak skal være dokumentert i organisasjonens sikkerhetskatalog (eller andre sikkerhetsdokumenter)</p>
1.1.3	<p>Leverandør gjennomfører løpende/regelmessig teknisk risikovurdering av tilbudt løsning. Risikovurderingene kan fremvises på forespørsel.</p>	<p>Risikovurderinger er nødvendig for å kunne vurdere risikobildet og iverksette nødvendige sikkerhetstiltak. Nivå for akseptabel risiko skal være fastsatt og rutiner for gjennomføring av risikovurderinger skal være utarbeidet, dette inkludert oppfølging av tiltak.</p>

<p>1.2 Organisering av informasjonssikkerhet</p> <p>Formål med kravene: sikre at leverandøren har en sikkerhetsorganisasjon med tydelige roller og ansvar.</p>	<p>Utdyping av krav</p>
---	-------------------------

1.2.1	Leverandør har dokumentert sin sikkerhetsorganisasjon. Dokumentasjonen inkluderer 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 Kunden.
-------	---	---

1.3 Personellsikkerhet Formål med kravene: sikre at leverandørens ansatte har tilstrekkelig informasjonssikkerhetskompetanse til å forvalte Kundens informasjon.		Utdyping av krav
1.3.1	Leverandør har 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.

1.4 Informasjonsforvaltning Formål med kravene: sikre at leverandøren tar eierskap til informasjon og informasjonssystemene, herunder Kundens informasjon.		Utdyping av krav
1.4.1	Leverandøren har oversikt over utstyr og systemer som er involvert i leveransen til Kunden.	Kravet skal sikre at leverandør har oversikt og kontroll på sitt utstyr, slik at for eksempel en bærbar maskin med Kundens opplysninger ikke kommer på avveier.
1.4.2	Leverandøren har en dokumentert policy for akseptabel bruk av utstyr og informasjonssystemer.	Kravet skal bidra til å regulere hva de ansatte kan bruke sitt utstyr til.
1.4.3	Avhending/sletting av medier, herunder backupmedier, skjer på en tilstrekkelig sikker måte.	Kravet skal sikre at flyttbare medier og backupmedier slettes før de avhendes.
	Leverandøren bes beskrive	

1.5 Tilgangskontroll/aksesskontroll Formål med kravene: begrense tilgang til informasjon og informasjonssystemer.		Utdyping av krav
---	--	------------------

1.5.1	Leverandøren har en dokumentert prosess for tilgangsstyring, herunder oppretting, endring og sletting av brukere. Bruk av privilegerte kontoer begrenses. Leverandøren bes beskrive	Kravet skal sikre at leverandør har god kontroll på tilgangsstyringen sin.
1.5.2	Løsningen har rollebasert tilgangsstyring Leverandøren bes beskrive	Kravet går ut på at løsningen skal skille mellom forskjellige roller. Noen kan for eksempel være administratorer, mens andre vanlige brukere. Roller bidrar til å redusere risiko ved å begrense hva de ulike rollene kan gjøre i løsningen.
1.5.3	Alle registrerte brukere i løsningen er unike og personlige.	I de fleste løsninger er det viktig at vi vet hvem som har gjort hva (sporbarhet). Fellesbrukere bør derfor unngås.
1.5.4	Dersom løsningen tilbyr autentisering over usikrede nett, så støttes og aktiveres sterk autentisering, dette for alle typer roller/brukere. Leverandøren bes beskrive	Kravet er spesielt viktig dersom løsningen 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. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonsikkerhet-internkontroll/sterk-autentisering/

1.6 Kryptografi Formål med kravene: sikre at leverandøren bruker kryptografi for å beskytte informasjon.		Utdyping av krav
1.6.1	Leverandør tilbyr kryptering av data i hvile på det nivå som vurderes nødvendig for type data og (for eksempel kryptering på databasenivå eller filnivå) der dette konkluderes med at er nødvendig. Leverandøren bes beskrive	Kravet om kryptering av data i hvile går utover det å bare kryptere disker. Ved å kryptere disker hindrer man data på avveier ved tyveri eller usikker avhending av utstyr. Ved behandling av særlige kategorier av personopplysninger, eller data om sårbare individer (eksempelvis barn), må data også krypteres i tabeller i databasen og det må i tillegg etableres en robust og sikker nøkkelhåndtering. Helst tilsvarende "Always encrypt" tankesettet til MS. Dette er også slik man kan lese artikkel 32, det skal kunne sikres vedvarende konfidensialitet for denne type data.

1.6.2	Ved overføring av data over usikrede nett (f.eks. internett) er overføringen kryptert	All kommunikasjons over offentlige og /eller usikrede nett skal være kryptert, algoritmene som benyttes skal være anerkjente, oppdaterte og iht. dagens standarder
1.6.3	Leverandør har 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.
1.6.4	Ved lokal brukerdatabase i løsning er passordene kryptert, saltet eller hashet	Sikker forvaltning av passord er en viktig egenskap ved alle datasystemer, slik at passord ikke enkelt kan avsløres/avdekkes

1.7 Fysisk og miljømessig sikkerhet Formål med kravene: begrense fysisk tilgang til lokaler, servermiljø og informasjonssystemer.		Utdyping av krav
1.7.1	Leverandør har tilstrekkelig fysisk sikring knyttet til sine datarom, som adgangskontroll, brannsikring, ventilasjon og redundant strømforsyning. Dokumentasjon skal legges frem på forespørsel.	Kravet skal ivareta sikring av lokaler hvor Kundens data befinner seg. Tilgang til datarom skal kun gis de som har et tjenstlig behov. Kravet dekker også andre elementer, som brannslukkingsapparat, alarm og nødstrøm.

1.8 Driftssikkerhet Formål med kravene: sikre at leverandøren har korrekt og sikker drift av sine informasjonssystemer.		Utdyping av krav
1.8.1	Leverandør har en dokumentert prosess for endringshåndtering, som sikrer at Kunden 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 løsningen ikke medfører nedetid, bortfall av data eller endring av data. I tillegg stilles det krav om at Kunden skal varsles ved endringer, slik at brukerne ved når endringer skjer og dermed kan planlegge for at løsningen er utilgjengelig.
1.8.2	Leverandør har en dokumentert prosess for testing av endringer i løsningen, samt overføring av endringer fra testmiljø til produksjonsmiljø.	Kravet skal sikre at leverandør kvalitetssikrer endringer i løsningen, og at det skal gjøres ved å bruke testmiljø og produksjonsmiljø.
1.8.3	Leverandørens testmiljø er atskilt fra produksjonsmiljøet.	Det er viktig å ikke benytte produksjonsdata i test, hovedsakelig grunnet krav til/brudd på konfidensialitet

	Testmiljøet benytter ikke Kundens produksjonsdata.	
1.8.4	Leverandør separerer Kundens data fra andre kunders data, fysisk eller logisk. Leverandøren bes beskrive (samme krav som 1.15.5, her generelt eller "on prem")	Kravet skal sikre at kundens data skal være tilstrekkelig atskilt fra annen data, og dermed at Kundens data ikke «lekker» over til andre kunder av leverandøren, eller omvendt.
1.8.5	Leverandør har en dokumentert prosess for kapasitetsstyring, som sikrer tilgjengelighet på løsningen ved varierende behov.	Kravet skal sikre at leverandør har tilstrekkelig kapasitet i sin løsning til å håndtere perioder med høy belastning. God kapasitetsstyring er viktig for å kunne garantere tilstrekkelig kapasitet, selv i perioder med høy belastning.
1.8.6	Løsningen er hensiktsmessig sikret mot ondsinnet kode og datainnbrudd. Leverandøren bes beskrive	Kravet er et generelt krav om at leverandør skal ha gode sikkerhetstiltak på plass ifm. f.eks. utviklingsmetodikk, sikkerhetstesting, penetrasjonstesting etc.
1.8.7	Leverandør har en dokumentert prosess for sikkerhetskopiering. Leverandøren bes beskrive	Kravet skal sikre at leverandør tar sikkerhetskopier av Kundens data og om Kundens behov ivaretas (hyppighet, varighet, antall kopier, granulering osv.).
1.8.8	Leverandør verifiserer jevnlig innhold i sikkerhetskopier og tester gjenoppretting av data.	Kravet skal sikre at leverandøren klarer å gjenopprette sikkerhetskopier dersom nødvendig.
1.8.9	Leverandør oppbevarer sikkerhetskopier atskilt fra produksjonsmiljøet og sikrer de mot skadevare. Leverandøren bes beskrive	Det har vært flere tilfeller hvor angrep på Kundens servermiljø også har omfattet sikkerhetskopier, for eksempel i Østre Toten i 2020. Ved å definere sperrer mellom produksjonsmiljø og sikkerhetskopiene øker sannsynligheten for gjenoppretting.
1.8.10	Leverandør sikrer en forsvarlig og systematisk overvåking av løsningen, dataoverføringer og grensesnitt. Avvik rapporteres til Kunden.	Kravet skal sikre at leverandør overvåker alle elementer som inngår i leveransen av løsningen.
1.8.11	Leverandør logger alle forsøk på autorisert og uautorisert tilgang til løsningen, samt relevante sikkerhetshendelser som er tilknyttet løsningen.	Kravet skal sikre at leverandør oppdater forsøk på ulovlig bruk av løsningen (for eksempel passordgjetting), samt gi god sporbarhet hvis leverandøren får en sikkerhetshendelse. Gode logger er viktig i forbindelse med styring av informasjonssikkerhetsbrudd.

1.8.12	<p>Leverandør sikrer følgende logging ved aksess av data i løsningen:</p> <ol style="list-style-type: none"> 1) hvem som aksesserte 2) når data ble aksessert 3) hvilke data som ble aksessert 4) ved endring og/eller sletting skal alle data/felter som ble endret/slettet logges. <p>Leverandøren bes beskrive</p>	<p>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.</p>
1.8.13	<p>Leverandør sikrer at logger beskyttes mot uautorisert innsyn, endring og sletting.</p> <p>Leverandøren bes beskrive</p>	<p>Logger skal ikke kunne slettes før etter en gitt periode (varighet må kunne endres over tid for løpende å kunne tilpasse lovendringer på området) . Det skal kunne settes opp automatisk sletting av logger for å ivareta prinsippet om lagringsbegrensning. Logger kan være viktig bevismateriale som må sikres.</p>
1.8.14	<p>Sikkerhetslogger kan overføres til Kunden på forespørsel.</p>	<p>Dette for at Kunden skal kunne korrelere logger på tvers og bedre avdekke anomaliteter.</p>
1.8.15	<p>All support fra leverandør mot Kunden og som innbefatter at leverandør potensielt får tilgang til personopplysninger i systemet skjer kun etter avtale med Kunden. All slik aktivitet logges. Kundens godkjente løsninger benyttes ved fjernaksess til skjerm eller server hos Kunden.</p>	<p>Kravet skal sikre standardisering av support inn mot Kunden.</p>
1.8.16	<p>Leverandør har en dokumentert prosess for sikkerhetsoppdateringer som dekker alle komponenter i løsningen.</p>	<p>Kravet skal sikre at leverandør gjennomfører kontinuerlige sikkerhetsoppdateringer (patcher) av sine systemer og løsninger.</p>
1.8.17	<p>Leverandør sørger for jevnlig sikkerhetstesting av løsningen. Dokumentasjon av test med tiltak kan fremlegges på forespørsel.</p>	<p>Kravet skal sikre at leverandør gjennomfører sikkerhetstester eller penetrasjonstester av sitt miljø og sine løsninger. Slik testing er viktig for å avdekke om det finnes sårbarheter som må tettes.</p>
1.8.18	<p>Datautstyr som er i kontakt med Kundens informasjon er tilstrekkelig sikret.</p>	<p>Manglende sikkerhet på utstyret til leverandørens ansatte kan resultere i at trusselaktører får innpass i utstyret og dermed Kundens data.</p>

1.9 Kommunikasjonssikkerhet Formål med kravene: sikre at leverandøren har god kommunikasjonssikkerhet.		Utdyping av krav
1.9.1	Leverandør har utarbeidet konfigurasjonskart (skisse) som viser sikkerhetskontroller og teknisk beskrivelse av informasjonssystemene, inkludert dataflyt.	Kravet skal sørge for at Kunden får oversikt over hvordan Kundens data flyter i løsningen. Kunden 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 løsningen er designet/bygget opp, og vil dermed være et nyttig underlag for risikovurderingene.
1.9.2	Dersom leverandør skal sende e-poster på vegne av Kunden, så har de ha satt opp SPF (sender policy framework) og DKIM (Domain keys identified mail). Leverandøren bes beskrive	Kravet skal trygge brukeren ved å benytte Kundens standard avsenderdomener /-adresser. Normalt benyttes domenet @baerum.kommune.no som avsender.
1.9.3	Alle grensesnitt for netjtjenester (web, APIer, endepunkter) er tilstrekkelig sikret mot uautorisert tilgang.	Kravet skal sikre at leverandør implementerer sikkerhetstiltak for alle grensesnitt som eksponerer Kundens data. Dette slik at eksempelvis APIene ikke blir dårligere sikret enn selve websiden.
1.9.4	All datakommunikasjon over usikre nettverk (for eksempel Internett) er kryptert med anerkjente protokoller. Trafikk i klartekst forekommer ikke.	Kravet skal sikre at overføring av Kundens data alltid skjer gjennom krypterte nettverk. Det reduserer risikoen for at en trusselaktør klarer å fange opp trafikk og dermed få tilgang til personopplysninger og andre kritiske data.
1.9.5	Alle som behandler Kundens produksjonsdata har signert taushetserklæring.	Kravet skal sikre den juridiske forpliktelsen som følger av at leverandørens ansatte behandler Kundens data.

1.10 Anskaffelse, utvikling og vedlikehold av systemer Formål med kravene: sikre at leverandør ivaretar informasjonssikkerhet i systemenes livsløp.		Utdyping av krav
1.10.1	Løsningen er utviklet etter sikker utviklingsmetodikk. Leverandøren bes beskrive	Kravet skal sikre at leverandør har hatt fokus på informasjonssikkerhet gjennom hele utviklingsløpet.

1.11 Leverandørforhold Formål med kravene: sikre at underleverandører har kontroll på informasjonssikkerheten.		Utdyping av krav
1.11.1	Leverandør har beskrevet hvilke underleverandører som brukes, hvilket lands jurisdiksjon de er underlagt, og hvilke roller og oppgaver de har i forbindelse med leveranse av løsningen. Leverandøren bes beskrive (Henvis evt. til vedlegg 1 i databehandleravtalen)	Kravet skal sikre at Kunden har kontroll på hvem som er involvert i behandlingen av Kundens data. Det er også viktig i forbindelse med behandling av personopplysninger, da Kunden må sikre et gyldig overføringsgrunnlag til land utenfor EØS-området.

1.12 Styring av informasjonssikkerhetsbrudd Formål med kravene: sikre at leverandøren håndterer eventuelle informasjonssikkerhetsbrudd.		Utdyping av krav
1.12.1	Leverandør har 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 Kunden.	Kravet skal sikre at leverandør er i stand til å håndtere eventuelle sikkerhetsbrudd, og at Kunden blir informert ved hendelser.
1.12.2	Leverandør har 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.

1.13 Virksomhetskontinuitet Formål med kravene: sikre at leverandøren har robuste og redundante tjenester.		Utdyping av krav
1.13.1	Leverandør har tilstrekkelig beredskaps- og kontinuitetsplaner for å sikre tilgjengelighet på løsningen i henhold til SLA.	Kravet skal sikre at leverandør er i stand til å levere løsningen ved uforutsette hendelser som strømbrydd, flom eller andre hendelser. Beredskaps- og kontinuitetsplaner er viktige for at leverandøren skal kunne oppfylle sine forpliktelser i SLA-avtalen.

	Leverandøren bes beskrive	
1.13.2	Løsningen er beskyttet mot tjenestenektangrep. Leverandøren bes beskrive	Kravet er aktuelt dersom leverandør tilbyr løsningen 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.

1.14 Samsvar Formål med kravene: sikre at leverandøren leverer innenfor lovverket og sine kontraktsforpliktelser.		Utdyping av krav
1.14.1	Leverandør sikrer at alle leveranser til Kunden skjer i henhold til norske lover og regler.	Kravet er et generelt krav om at leverandør skal følge norske lover og regler (GDPR og andre relevante lover).
1.14.2	Leverandør foretar minimum en gang i året en uavhengig gjennomgang/revisjon 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.
1.14.3	Kunden skal kunne gjennomføre revisjon av leverandøren eller dens underleverandør, enten selv eller gjennom tredjepart.	Kravet skal åpne for at Kunden kan iverksette revisjon av leverandøren.

1.15 Skytjenester Formål med kravene: sikre regulering av leverandør som tilbyr tjenester i skyen (SaaS).		Utdyping av krav
1.15.1	Leverandør har en etablert prosess for å identifisere, vurdere og prioritere tiltak iht. trusselbildet. Det bør også arbeides aktivt for å begrense sårbarheter.	Kravet skal sikre at leverandør gjennomfører trussel- og sårbarhetsvurderinger.

1.15.2	Leverandør yter bistand dersom Kunden ønsker å avslutte avtalen. Leverandør legger til rette for at Kundens data blir overført til Kunden eller til tredjepart utpekt av Kunden.	Kravet skal sikre at Kunden ikke havner i en lock-in situasjon, ved at de ikke får ut informasjonen som er lagt inn i løsningen i et hensiktsmessig format.
1.15.3	Leverandør forhindrer uautorisert tilgang til sitt datasenter, samt beskytter mot tyveri, skade, tap og at utstyr svikter, for å sikre kontinuerlig drift.	Kravet skal sikre den fysiske adgangen i leverandørens datasenter.
1.15.4	Det er implementert kryptografiske mekanismer med nøkkeladministrasjon etter god praksis for å sikre data i ro og sikker drift av tjenestene. Leverandøren bes beskrive	Kravet skal sikre lagret informasjon ved hjelp av kryptografi.
1.15.5	Leverandør separerer Kundens tjenester og data fra andre kunder, fysisk eller logisk. Leverandøren bes beskrive (samme krav som 1.8.4, her sky)	Kravet skal sikre at Kundens data skal være tilstrekkelig atskilt fra annen data, og dermed at Kundens data ikke «lekker» over til andre kunder, eller omvendt.
1.15.6	Leverandør dokumenterer hvordan data slettes, og hvordan slettede data ikke kommer på avveier eller kan gjenskapes. (Se også krav 1.4.3)	Kravet skal sikre at leverandør sletter Kundens data, for eksempel i forbindelse med opphør av avtalen.
1.15.7	Løsningen har høy tilgjengelighet etter avtale. Historisk oppetid/tilgjengelighet kan dokumenteres.	Kravet skal sikre at løsningen er tilgjengelig ved behov og etter avtale.
1.15.8	Leverandør har en prosess som håndterer endringer, sikrer at endringer som kan påvirke sikkerheten identifiseres og håndteres og at uautoriserte endringer oppdages. (Se også/samme som krav 1.8.1)	Kravet skal sikre at leverandør har en prosess for endringshåndtering.

1.15.9	Alle handlinger som utføres av leverandøren logges. Loggen kan ikke kunne manipuleres. Kunden kan ha tilgang til loggene etter behov.	Kravet skal sikre sporbarhet i løsningen.
--------	---	---

2.1 Personvernkrav Formål med kravene: sikre at leverandøren leverer innenfor rammene av personopplysningsloven. Disse kravene supplerer databehandleravtalen.		Utdyping av krav
2.1.1	Leverandør har kunnskap om, og opptrer i henhold til, relevante artikler i GDPR, herunder artikkel 28.	Et generelt krav om at leverandør skal forstå og levere i henhold til GDPR.
2.1.2	Leverandør sørger, gjennom planlagte og systematiske tiltak, for tilfredsstillende personopplysningsikkerhet i samsvar med GDPR artikkel 32, jf. personopplysningsloven § 1 (jf. GDPR artikkel 28 nr. c).	Et generelt krav om at leverandør skal sikre personopplysningene gjennom relevante sikringstiltak.
2.1.3	Løsningen er utviklet i henhold til prinsippene om innebygd personvern og personvern som standardinnstilling, jf. GDPR artikkel 25. Det innebærer at løsningen for eksempel: <ul style="list-style-type: none"> - benytter nedtrekksmenyer til fordel for fritekstfelter - benytter dataminimering - benytter pseudonymisering (hvor mulig) - begrenser tilgangsstyring (tjenstlig behov) - ha ledetekst ved alle eventuelle fritekstfelter Leverandøren bes beskrive	Kravet sikrer at løsningen har innebygd personvern (privacy by default og privacy by design). For innebygget personvern se https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/innebygd-personvern---hva-er-det/
2.1.4	Leverandør signerer Kundens databehandleravtale (fortrinnsvis).	Det er viktig at Kunden som behandlingsansvarlig tar eierskap til innholdet i en databehandleravtale. Videre vil dette medføre en smidigere og raskere prosess.

2.1.5	I løsningen er det enkelt å søke opp informasjon om enkeltbrukere og gi mulighet for innsyn, retting og sletting av informasjon, jf. GDPR kap. 3, Den registrertes rettigheter.	Dette for å ivareta innsynsforespørsler og utfordringer ved dette. Det bør derfor være tilrettelagt for Kunden å gjøre slike søk/oppslag i løsningen.
2.1.6	Personopplysninger i løsningen lagres og behandles innen EU/EØS og i henhold til gjeldende personvernlovgivning.	Bruk av underleverandører som ev. overfører personopplysninger til 3. land , eller som er underlagt 3. lands jurisdiksjon, skal avtales skriftlig med behandlingsansvarlig på forhånd. Ved overføring av personopplysninger til 3. land skal leverandør benytte godkjente EU-overføringsmekanismer eller ha iverksatt nødvendige tiltak. Ved overføring til utlandet, uavhengig av om det er innenfor eller utenfor EU/EØS, skal leverandør gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsensnivå knyttet til aktuelle underleverandører. Merk: EU-kommisjonen har fattet en beslutning om at noen land og områder utenfor EU/EØS har et tilstrekkelig beskyttelsesnivå for personopplysninger (en såkalt adekvansbeslutning). Overføringer til slike land og områder kan skje uten et særskilt overføringsgrunnlag, eller ytterligere vurderinger om beskyttelsesnivå.
2.1.7	Leverandør har en rutine for varsling til Kunden uten ugrunnet opphold ved hendelser knyttet til informasjonssikkerhet og personvern.	Dette slik at Kunden evt. får varslet tilsynet iht. til GDPR art. 33.1

3.1	Spesielle krav for anskaffelsen Formål med kravene: sikre at leverandøren leverer iht. Kundens spesielle behov i denne anskaffelsen	Utdyping av krav
3.1.1	Løsningen bør ivareta krav til universell utforming	https://www.uutilsynet.no/veiledning/nettsteder-og-apper/711

9 OPSJONER

Kunden har følgende opsjoner i avtalen:

Nr.	Krav
1.	<p>Flere brukere med begrensede tilganger</p> <p>Punkt 4.2 skisserer at det kan være potensielle brukere av systemet som kun skal ha begrensede tilganger (fast og helårlig bruker). Det skal i SSA-L bilag 6B Prisskjema punkt 3 oppgis pris for per bruker med kun begrensede tilganger i systemet, f.eks. kun lesetilgang og tilgang til innregistrerte data/rapporter. Dersom prisen er det samme som ordinær bruker i punkt 2 i Prisskjema, skal pris på dette fortsatt oppgis.</p>
2.	<p>Fremtidig funksjonalitet/integrasjoner</p> <p>Det er utfordrende å forutse fremtidige behov og muligheter for funksjonalitet og integrasjoner. I tillegg er det variasjoner rundt hvilke funksjonaliteter de ulike leverandørene i markedet i dag tilbyr inkludert i sine systemer. Vi ønsker derfor at avtalen tar høyde for at vi kan anskaffe ytterligere opsjoner i form av videreutvikling av funksjonalitet/moduler/integrasjoner (også ev. fra underleverandører eller tredjeparter) som naturlig hører sammen og som kan støtte løsningen der vi ser at det kan være hensiktsmessig i avtaleperioden, jf. SSA-L Kontrakt punkt 3.6. Noen eksempler på mulige fremtidige integrasjoner kan f.eks. være integrasjon med Bærums Kart (Nor Kart), og integrasjon med kommunens øvrige timeregistrering/- lønssystem.</p> <p>Arbeid knyttet til dette, skal godtgjøres i henhold til timesats for «tilleggsarbeider som prises etter medgått tid» i punkt 3 i SSA-L bilag 6B Prisskjema, med mindre annet avtales mellom partene.</p>

10 DEMONSTRASJON I EVALUERINGSFASEN AV KONKURRANSEN

Vi ønsker å invitere tilbyderne til å gi en demo av sin tilbudte løsning under evalueringsfasen. Demo av løsningen skal være et tillegg til løsningsbeskrivelse i leverandørens tilbud, og bidra til å gi et best mulig grunnlag for å vurdere tilbudenes oppfyllelse av krav som er beskrevet i dette dokumentet.

Demo ønskes utført med utgangspunkt i de ulike brukerhistoriene/behovene beskrevet i punkt 5, og målet er at demo viser hvordan Kundens behov blir løst.

Invitasjon til demo vil bli sendt ut i evalueringsfasen.

11 SUPPORT OG VEDLIKEHOLD

Supportløsning og versjonsoppgraderinger i «systemets levetid» skal være inkludert i anskaffelsen.

Dette omfatter:

- Support under og etter implementering – retting av småfeil og tilpasninger.
- Vedlikehold av systemet – oppdateringer når leverandør videreutvikler og oppdaterer systemet.
- Statusmøter med leverandør – info om nyheter.
- Brukerforum – seminarer/konferanser/kurs/opplæring/webinarer arrangert av leverandør.
- Versjonsoppdateringer – fremtidige versjoner.