



Elektronisk logistikk- og kvalitetsstyringssystem for Sterilavdelingen ved OUS

Saksnummer: 2018/691

T Bilag 1C: Kundens tekniske krav

Innholdsfortegnelse

0. Innledning.....	4
<i>Om kravene i og besvarelse av dette bilaget.....</i>	<i>4</i>
1. Krav til teknologi	4
1.1 Overordnede arkitekturprinsipper og systembeskrivelse.....	4
1.2 Skalérbarhet og ytelse.....	9
1.3 Infrastruktur og plattform.....	12
1.3.1 Generelle krav til infrastruktur og plattform.....	12
1.3.2 Lisensieringsteknologi	14
1.3.3 Kritikalitet	15
1.3.4 Nettverk.....	16
1.3.5 Server.....	18
1.3.6 Webserver	20
1.3.7 Database.....	21
1.3.8 Arbeidsflate og klientapplikasjon	22
1.3.9 Lagring, backup og arkivering.....	27
1.3.10 Utskrift.....	28
1.4 Maskinvare og periferutstyr.....	29
1.5 Integrasjon og interoperabilitet	30
1.5.1 Generelle krav til integrasjon	32
1.5.2 Autorative datakilder.....	34
1.5.3 Integrasjon med maskiner benyttet i sterilprosessering.....	36
1.5.4 Integrasjon med administrative fagsystemer.....	37
1.5.5 Integrasjon med kliniske fagsystemer	38
1.5.6 Integrasjon med andre systemer.....	40
1.6 Informasjonssikkerhet.....	41
1.6.1 Generelle krav til autentisering og autorisering.....	42
1.6.2 Krav til bruk av løsning for Identity and Access Management	46
1.6.3 Logging.....	48
1.6.4 Nettverk og kommunikasjon	49
1.6.5 Integrasjonsgrensesnitt	50
1.6.6 Kryptering.....	50
1.6.7 Antivirus og antimalware	51
1.7 IKT-relatert drift og forvaltning.....	51
1.7.1 Generelle krav til IKT-relatert drift og forvaltning.....	52

1.7.2	Fjernaksess og eksterne tilganger	53
1.7.3	Oppdatering, oppgradering og vedlikehold	55
1.7.4	Driftsteknisk overvåking og logging.....	56

0. Innledning

Om kravene i og besvarelse av dette bilaget

Dokumentet «SSA-T Bilag 1» og dokumentet «SSA-T Bilag 2» inneholder generell informasjon hvordan dokumentene skal besvares.

1. Krav til teknologi

1.1 Overordnede arkitekturprinsipper og systembeskrivelse

Sykehuspartner er Kundens tjenesteleverandør, og drifter og forvalter Kundens infrastruktur og IKT-plattform på vegne av Kunden. Kundens samlede IKT-infrastruktur og IKT-plattform omtales i dette dokumentet som «Kundens tekniske plattform». Kundens tekniske plattform er nærmere beskrevet i dokumentene:

- «SSA-T Bilag 3a – Kundens tekniske plattform»
- «SSA-T Bilag 3b – Kundens tekniske plattform - Integrasjon»
- «SSA-T Bilag 3c – Kundens tekniske plattform - Identitet og tilgangsstyring»

Der det i dokumentet henvises til «SSA-T Bilag 3 – Kundens tekniske plattform», uten eksplisitt å nevne 3a, 3b eller 3c, gjelder da henvisning til Bilag 3a, 3b og 3c samlet.

Kundens tjenesteleverandør drifter og forvalter i tillegg store deler av Kundens systemportefølje. Ansvarsmessige og merkantile forhold mellom Kunden og Kundens tjenesteleverandør reguleres på et overordnet nivå i en tjenesteavtale inngått mellom partene. I tillegg reguleres ansvarsmessige og merkantile forhold mellom partene i ett sett tjenestebeskrivelser, som omhandler de enkelte systemene. Dette medfører at kravene som stilles systemet må ivareta både Kunden og Kundens tjenesteleverandørs behov vedrørende etablering, drift og forvaltning av systemet.

Kunden og Kundens tjenesteleverandør forplikter seg til å etterleve føringer nedfelt i Nasjonal IKTs overordnede Arkitekturprinsipper i spesialisttjenesten, jfr. «SSA-T Bilag 1 - vedlegg 1 – NIKT Arkitekturprinsipper i Spesialisthelsetjenesten».

Tilbudt system skal etableres i Kundens etablerte infrastruktur og på Kundens eksisterende IKT-plattform. Tilbudt system skal integreres og samhandle med eksisterende og fremtidige maskiner som benyttes ifm. sterilprosessering, eksempelvis autoklaver, vaskedekontaminatorer og sveisemaskiner. Systemet skal i tillegg integreres og samhandle med både eksisterende og fremtidige administrative og kliniske fagsystemer, eksempelvis Kundens ERP-system (Oracle OeBS) og kundens PAS/EPJ og/eller operasjonsplanleggingssystem.

OUS er etablert på en egen IKT-plattform og infrastruktur separat fra de andre helseforetakene i Helse Sør-Øst, hvor det er enkelte tekniske og sikkerhetsmessige forskjeller i IKT-plattformen og infrastrukturen mellom helseforetakene. Det vil derfor være nødvendig å etablere en egen, separat instans av systemet for OUS fra de andre helseforetakene i Helse Sør-Øst, dersom andre helseforetak gjør avrop på avtalen.

OUS IKT-plattform og infrastruktur er under kontinuerlig modernisering og endring. Det pågår samtidig en prosess for modernisering og konsolidering av de ulike infrastrukturene og IKT-plattformene i Helse Sør-Øst, slik at disse over de neste årene vil være mer enhetlig etablert, driftet og forvaltet. Da det fortsatt er mange uklarheter i omfanget og betydningen av disse endringene for OUS, er kravene til systemet beskrevet utfra dagens eksisterende infrastruktur, med de *kjente* endringene som vil komme frem mot innføringstidspunktet av systemet.

Det er viktig at tilbudt løsning kan etableres iht. de krav og føringer som er gitt av de overordnede føringene og begrensningene beskrevet i «SSA-T Bilag 3 – Kundens tekniske plattform» og kravene i denne kravspesifikasjonen.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T1.1	Leverandøren skal bekrefte at den har gjort seg kjent med og har forstått arkitekturprinsippene beskrevet i dokumentet «SSA-T Bilag 1 - Vedlegg 1 – NIKT Arkitekturprinsipper i Spesialisthelsetjenesten». Merknad: Helse Sør-Øst forplikter seg til å overholde Nasjonal IKTs overordnede Arkitekturprinsipper i spesialisthelsetjenesten, jfr. «SSA-T Bilag 1 - Vedlegg 1 – NIKT Arkitekturprinsipper i Spesialisthelsetjenesten». Arkitekturprinsippene er kortfattede og konsise regler som skal bidra til at spesialisthelsetjenesten utvikles i tråd med rammene gitt av spesialisthelsetjenestens visjoner og mål, lover og forskrifter, samt teknologiske muligheter.	O	
T1.2	Leverandøren skal bekrefte at den har gjort seg kjent med og har forstått beskrivelsen av Kundens infrastruktur og IKT-plattform beskrevet i dokumentene: • «SSA-T Bilag 3a – Kundens tekniske plattform» • «SSA-T Bilag 3b – Kundens tekniske plattform - Integrasjon» • «SSA-T Bilag 3c – Kundens tekniske plattform - Identitet og tilgangsstyring» Merknad: Kunden har en etablert infrastruktur og IKT-plattform beskrevet i SSA-T Bilag 3-dokumentene, som legger en rekke føringer og begrensninger for nye systemer som skal etableres hos Kunden.	O	

	Kundens infrastruktur og IKT-plattform er etablert iht. prinsippene i Nasjonal IKTs overordnede Arkitekturprinsipper i spesialisthelsetjenesten, samt andre føringer, prinsipper og målsettinger definert av Helse Sør-Øst, Kunden og Kundens tjenesteleverandør.		
T1.3	Systemet skal etableres som et internt system i Kundens eksisterende infrastruktur og IKT-plattform. Merknad: Kunden tillater ikke at systemet etableres eksternt, eksempelvis i en ekstern skytjeneste eller i datasenter kontrollert av Leverandør, Produsent eller annen 3.part.	O	
T1.4	Leverandøren skal fremlegge et overordnet løsningsdesign og kortfattet systemdokumentasjon for løsningen.	O	
T1.5	Løsningsdesign og kortfattet systemdokumentasjon i kravpunkt T1.4 bør på en tydelig og oversiktlig måte vise systemets relevante hovedkomponenter, overordnet dataflyt, samt kommunikasjonsgrensesnitt internt og eksternt. Merknad: Det er meget viktig at dokumentasjonen gjenspeiler systemet, med en tilhørende illustrasjon, slik den er tenkt etablert i Kundens tekniske plattform, jfr. «Bilag 3 – Kundens tekniske plattform». Dokumentasjonen bør inkludere alle komponenter, eksempelvis teknisk utstyr, klient-PC, servere, lagring, nettverk, konvertere m.m. som inngår i systemets totale løsning. Evt. enkeltkomponenter som ikke er i samsvar med Kundens tekniske plattform bør beskrives, inklusiv hvordan disse avviker.	H	B
T1.6	Leverandøren skal fremlegge en detaljert oversikt over relevant nettverksmessig dataflyt for systemet. Merknad: Med «relevant» menes dataflyt som benytter eller traverserer Kundens datanettverk, og derfor kan kreve at brannmursregler må tilrettelegges for at det tilbudte systemet skal fungere i Kundens infrastruktur og IKT-plattform.	O	
T1.7	Dokumentasjon over all relevant nettverksmessig dataflyt i kravpunkt T1.6 bør på en tydelig og oversiktlig måte vise detaljert	H	B

	dataflyt mellom systemets enkeltkomponenter iht. utarbeidet dokumentasjon fra kravpunkt T1.4 og T1.5, med eksisterende komponenter og andre tjenester i Kundens nettverk, samt fra hvilken komponent trafikken er initiert (trafikkretning).		
T1.8	Systemet bør benytte en trelagsarkitektur for å begrense eksponering av bakenforliggende database mot klientapplikasjon. Leverandøren bes utdype slik støtte, og beskrive evt. komponenter i systemet hvor dette ikke støttes.	H	B
T1.9	Systemet bør etableres uten avhengigheter til eksterne tjenester, eksempelvis skytjenester, webportal eller grensesnitt (API) utenfor Kundens nettverk, eksempelvis hos Leverandør eller Produsent. Merknad: Kunden krever kontroll og sporbarhet på all ekstern kommunikasjon til og fra systemet. Dersom systemet er avhengig av ekstern kommunikasjon, bes Leverandøren utdype besvarelsen og dokumentere til hvilket formål slik kommunikasjon er påkrevet, samt leverandør av og navn på alle eksterne tjenester.	H	B
T1.10	Dersom systemet er avhengig av <i>eksterne</i> tjenester, eksempelvis skytjenester, webportal eller grensesnitt (API), bør tilbudet også inneholde relevant løsningsdesign og risikovurdering for leverandørens infrastruktur som systemet er avhengig av.	M	B
T1.11	Systemet bør støtte <i>internt</i> etablerte skytjenester (Private Managed Cloud). Leverandøren bes utdype systemets støtte for etablering på internt etablerte skytjenester, samt evt. plattformer som er støttet. Merknad: Det er p.t. ikke etablert en intern skytjeneste i Kundens tekniske plattform, men det forventes at dette i fremtiden vil etableres og tas i bruk.	L	B
T1.12	Systemet bør være prosessorientert, og ha tilstrekkelig grad av fleksibilitet til å kunne tilrettelegges til Kundens arbeidsprosesser og arbeidsflyt ved innføring, samt ved fremtidige endringsbehov i organisasjon, roller og arbeidsflyt.	H	B

	Leverandøren bes kort utdype hvilken støtte systemet har for slik tilrettelegging og fleksibilitet, samt av hvem og hvordan endringer kan utføres.		
T1.13	Systemet bør ha tilstrekkelig grad av fleksibilitet til å tilrettelegge visning av relevant informasjon og funksjonalitet utfra kombinasjonen rolle, lokalitet, hendelser og/eller steg i en arbeidsprosess. Leverandøren bes kort utdype hvilken støtte systemet har for slik tilrettelegging og fleksibilitet.	H	B
T1.14	Systemet bør være modulært for å sikre at det enkelt kan legges til, erstattes eller fjernes moduler i systemet ved fremtidige endringsbehov. Leverandøren bes utdype systemets evt. støtte mht. modulbasert oppbygning, hvilke moduler som evt. inngår i systemet eller kan kjøpes som tilvalg, samt overordnet hvilken funksjonalitet som dekkes i hvilken modul.	H	B
T1.15	Duplisering av data på tvers av systemer bør kun forekomme dersom virksomhetsmessige behov tilsier at dette er den beste løsningen. Merknad: Dersom tilbyder fraviker fra kravet, beskriv hvorfor det eventuelt er en hensiktsmessig metode. Kunden foretrekker at det benyttes oppslag mot kilde eller andre systemer når systemet ikke selv eier dataelementene.	H	B
T1.16	Systemet bør støtte bruk av containertjenester, eksempelvis Docker eller Kubernetes. Leverandøren bes utdype hvilke containertjenester som evt. støttes. Merknad: Containertjenester benyttes i dag i liten grad i Kundens tekniske plattform, men det forventes at dette i fremtiden i større grad vil tas i bruk.	L	B
T1.17	Visning av informasjon i brukergrensesnittet og oppdateringer av data systemet behandler bør foregå i sanntid og uten tidsforsinkelser.	H	B

	Leverandøren bes utdype hvorvidt systemet eller deler av systemet har tidsforsinkelser i form av oppfriskning av data i brukergrensesnitt på gitte tidsintervaller, asynkron datautveksling eller jobber som må kjøres for at brukergrensesnittet eller data systemet behandler kan oppdateres.		
T1.18	Systemet bør være utviklet med et moderne og enhetlig benyttet utviklingsspråk og -rammeverk. Merknad: Leverandøren bes utdype: • hvilket utviklingsspråk og rammeverk som er benyttet ved utvikling av systemet • evt. hvilken versjon av rammeverk som er benyttet • evt. avvikende utviklingsspråk/rammeverk og versjoner benyttet i forskjellige komponenter i systemet Leverandøren bes spesielt utdype hvorvidt det er forskjeller i utviklingsspråk, rammeverk eller versjoner av rammeverk som er forårsaket av at enkelte komponenter i systemet ikke er modernisert, eller hvor Leverandøren har en pågående prosess for å modernisere systemet. Evt. pågående prosesser for modernisering bør gjenspeiles i veikart (roadmap).	M	B
T1.19	Systemet skal sikre dataintegritet i de tilfeller hvor flere brukere jobber med samme datasett på samme tid.	O	
T1.20	Kunden ønsker å fremme bærekraftig bruk av IKT gjennom systemets livssyklus. Leverandøren bes utdype hvordan leverandøren jobber etter prinsipper etablert mht. Grønn IT (www.ikt-norge.no/bransjenormer-guider/gronn-it/)	M	B

1.2 Skalérbarhet og ytelse

Skalérbarhet defineres i denne sammenheng som systemets evne til å håndtere endringer, eksempelvis antall brukere, samtidige brukere, antall integrerte maskiner som benyttes i sterilprosessering eller datavolum, uten at det påvirker ytelsen til systemet eller andre komponenter og tjenester i infrastrukturen og IKT-plattformen forøvrig.

Ytelse defineres som systemets evne til å jobbe og respondere raskt, for å sikre effektiv bruk og en god brukeropplevelse.

Kravene til skalérbarhet og ytelse gjelder alle komponenter og funksjoner i systemet, eksempelvis klientapplikasjon, applikasjonstjenester, mobile løsninger, integrasjonsgrensesnitt og databaser.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T2.1	Systemet bør skalére mht. <i>samtidige</i> brukere uten at det påvirker systemets ytelse. Merknad: Antall samtidige brukere vil avhenge av endelige beslutninger vedrørende integrasjon med operasjonsplanlegger. Dette vil dermed kunne redusere behovet for antall samtidige brukere i systemet. Kunden estimerer <u>inntil</u> 100-200 <i>samtidige</i> brukere på systemet når systemet er tatt i full bruk. Leverandør bes utdype evt. begrensninger i <i>samtidige brukere</i>, hvordan dette berøres av lisensmodell og hvordan systemet teknisk bør tilrettelegges for å sikre skalérbarhet mht. <i>samtidige</i> brukere, f.eks. i intervaller av 50-100, 100-150, 150-200, 200+ brukere.	H	B
T2.2	Systemet bør være tilrettelagt for å kunne skalére mht. <i>totalt antall</i> brukere uten at det påvirker systemets ytelse. Merknad: Totalt antall brukere vil avhenge av endelige beslutninger vedrørende integrasjon med operasjonsplanlegger. Som en del av et integrasjonsmål bilde ønskes deler av funksjonaliteten vedr. bestilling av sterile varer lagt til operasjonsplanleggeren. Dette vil dermed kunne redusere behovet for totalt antall brukere av systemet. Kunden estimerer i størrelsesorden <u>inntil</u> 1000-1200 brukere på systemet når systemet er tatt i full bruk. Leverandør bes utdype evt. begrensninger i <i>totalt antall</i>, hvordan dette berøres av lisensmodell og hvordan systemet teknisk bør tilrettelegges for å sikre skalérbarhet, mht. <i>totalt antall</i> brukere, f.eks. i intervaller av 100-200, 200-500, 500-1000, 1000+ brukere.	H	B

T2.3	Systemet bør ha støtte for å skaléres opp eller ned ved behov, eksempelvis ved endring i: • antall lokasjoner hvor systemet benyttes • antall brukere • antall operasjoner • antall bestillinger av sterilt utstyr • antall brikker og instrumenter systemet sporer • datavolum for annen data som behandles i systemet • endring av bruk Leverandør bes beskrive evt. begrensninger i systemets skalérbarhet. Merknad: Dette inkluderer eksempelvis hvordan systemets skalérbarhet berøres av lisensmodell, og hvordan systemet er tilrettelagt for skaléring ved endring av fremtidige behov.	H	B
T2.4	Systemet bør være uten begrensninger mht. antall <i>samtidige</i> klient-PCer som kan benytte systemet, iht. Kundens skaléringsbehov. Leverandør bes utdype evt. begrensninger.	H	B
T2.5	Systemet bør være uten begrensninger mht. <i>totalt antall</i> klient-PCer eller brukere systemet kan distribueres til, iht. Kundens skaléringsbehov. Leverandør bes utdype evt. begrensninger.	H	B
T2.6	Systemet bør være uten kjente feil, mangler eller utfordringer med hensyn til skalérbarhet og ytelse, eksempelvis ved økende antall brukere, lokasjoner, operasjoner, bestillinger, instrumenter eller data som behandles i systemet. Leverandøren bes utdype evt. kjente utfordringer ved skalérbarhet, samt anbefalinger for å unngå fremtidige skaléringsutfordringer.	H	B
T2.7	Leverandøren bør beskrive normal oppstartstid av evt. klientapplikasjon fra applikasjonen startes til bruker kan jobbe i systemet. Leverandør bes utdype vedr. normal oppstartstid av klientapplikasjonen, og faktorer som kan påvirke dette.	M	B
T2.8	Systemet bør være tilrettelagt på en måte som gjør at bruker med ordinære brukerrettigheter ikke kan starte prosesser eller	H	B

	funksjoner som gir merkbar redusert ytelse for andre brukere eller prosesser i systemet. Leverandør bes utdype evt. prosesser og funksjoner bruker kan starte som kan medføre redusert ytelse.		
T2.9	Systemet bør være tilrettelagt på en måte som gjør at regelmessige automatiserte eller manuelt igangsatte prosesser, eksempelvis rapportuttrekk, logging, overvåkingsagenter, backup, arkivering, analyse, indeksering, ryddejobber o.l. ikke påvirker systemets ytelse ovenfor systemets brukere. Leverandør bes utdype evt. prosesser og funksjoner som medfører redusert ytelse, og anbefalinger for å redusere muligheten for at dette påvirker bruken av systemet.	H	B
T2.10	Leverandøren bør beskrive typiske datavolum i dataflyten ved normal bruk av systemet, eksempelvis ved oppstart, innlogging, eller bestemte brukeroperasjoner i systemet. Merknad: Kunden ønsker å avklare om det er spesielle hendelser eller brukeroperasjoner ved normal bruk av systemet som medfører overføring av store datamengder, eksempelvis mellom klientapplikasjon og applikasjonstjenester/database som dermed kan redusere systemets ytelse.	H	B
T2.11	Leverandøren bør beskrive systemets krav til båndbredde.	H	B

1.3 Infrastruktur og plattform

Sykehuspartner er Kundens tjenesteleverandør, og drifter Kundens infrastruktur og IKT-plattform, beskrevet i «Bilag 3 – Kundens tekniske plattform».

Gjennom Tjenesteleverandørens avtaleverk er målsetningen at alle systemkomponenter som inngår i et system skal støtte en såkalt «N/(N-1)»-livssyklus. Dette betyr at det benyttes siste eller nest siste versjon av alle maskinvare- og programvarekomponenter.

1.3.1 GENERELLE KRAV TIL INFRASTRUKTUR OG PLATTFORM

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.1	Leverandør bør beskrive alle relevante komponenter (operativsystem, klientapplikasjoner, databaseplattform, webservere, serverprogramvare, 3.partskomponenter o.l.) som <u>ikke</u> leveres som	H	B

	en del av systemet, eller som avviker fra Kundens standarder beskrevet i «SSA-T Bilag 3 – Kundens tekniske plattform». Merknad: Dette kan eksempelvis være nettleser, utvidelse til nettleser, webserver, databaseplattform, Java, Flash, Silverlight, Microsoft Office, .NET Framework, C++ Redistributable, MDAC o.l. Leverandøren bes evt. utdype komponentens formål, samt leverandør, komponentnavn og versjon av komponentene for alle deler av systemet.		
T3.2	Systemet bør etableres uten avhengighet til bestemte versjoner av Microsoft Office på Kundens klientplattform. Leverandøren bes utdype evt. avhengigheter, avhengighetens formål, produkt i Office-pakken og versjon som kreves. Merknad: Avhengighet til produkter i Office-pakken er ikke ønskelig, da det medfører utfordringer tilknyttet vedlikehold og oppgradering av Office-pakken på Kundens klientplattform.	H	B
T3.3	Klientapplikasjoner bør virke uten bruk av Java runtime, ActiveX-kontroller, Flash, Silverlight eller utvidelser til nettleser installert på Klient PC. Ved evt. behov skal dette beskrives og begrunnes. Merknad: Kunden tillater av sikkerhetsmessige årsaker ikke Java-runtime installert lokalt på klient PC. Java-runtime kan tilrettelegges for applikasjoner distribuert gjennom App-V (virtualisert), men dette er ønskelig å unngå. Det er ikke ønskelig med avhengigheter til ActiveX-kontroller, Flash eller Silverlight, da disse allerede har mistet, eller er i ferd med å miste støtte i moderne nettlesere.	H	B
T3.4	Systemet bør overholde støtte for N og N-1 livssyklus for alle systemets komponenter. Leverandøren bes utdype slik støtte, og beskrive metodikk for å sikre at systemet oppdateres for å støtte nye versjoner. Merknad:	H	B

	Dette gjelder eksempelvis komponenter og tjenester: • levert av Kundens tjenesteleverandør, og ikke inngår i leveransen av systemet • levert av Leverandøren som en del av systemet • levert av 3.part		
T3.5	Alle komponenter som inngår i systemet skal synkronisere klokken mot sentral NTP-server i Kundens tekniske plattform.	O	
T3.6	Systemet skal ha støtte for norske tegnsett, eksempelvis UTF-8 eller ISO/IEC 10646.	O	

1.3.2 LISENSIERINGSTEKNOLOGI

For Kunden og Kundens tjenesteleverandør er det viktig å vite hvilke tekniske løsninger som benyttes for lisenshåndtering, og hvordan dette berører drift og forvaltning av systemet.

Det ikke ønskelig å benytte fysiske lisensdongler pga. utfordringer med dette i et virtualisert driftsmiljø. Det er heller ikke ønskelig med distribuerte lisensfiler til brukerens arbeidsflate, da dette medfører økt kompleksitet ved drift og vedlikehold av Kundens arbeidsflater, samt ved drift og forvaltning av systemet.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.7	Eventuelle lisensieringsmekanismer bør være basert på sentral lisens og sentralisert lisensforvaltning.	H	
T3.8	Leverandøren bør beskrive systemets eventuelle lisensieringsmekanismer, inklusiv leverandørens tekniske krav til dette. Merknad: Dette inkluderer eksempelvis: • bruk av lisensdongler eller andre fysisk tilkoblede enheter for lisensiering, samt tilkoblingsgrensesnitt (USB eller tilsvarende) • bruk av klientlisenser som krever installasjon på Kundens arbeidsflate • bruk av lisensserver, inklusiv leverandørens krav til denne	H	B
T3.9	Systemet bør ved midlertidig bortfall av lisensieringsmekanisme fungere uten at dette påvirker bruken av systemet.	H	B

	Leverandøren bes beskrive evt. konsekvenser for bruk av systemet ved bortfall av lisensieringsmekanisme.		
--	--	--	--

1.3.3 KRITIKALITET

Kundens evne til å opprettholde effektiv og forsvarlig pasientbehandling vil raskt kunne påvirkes ved bortfall av systemet.

Systemet planlegges etablert som et «Kritikalitet 1 – Høyt kritisk»-system. Kritikalitetsnivået legger føringer for hvordan systemet må etableres for å sikre høyest mulig grad av tilgjengelighet, raskest mulig re-etablering og begrense datatap ved bortfall av tjenesten.

Endelig konfigurasjon av løsningen for etablering av systemet vil avklares i videre prosess for utarbeidelse av løsningsdesign for valgt system.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.10	Leverandøren bør utdype hvordan systemet kan og bør etableres for å tilrettelegges for en høy kritikalitetsgrad, med begrenset nedetid og datatap ved bortfall av tjenesten. Merknad: Det er spesielt viktig at leverandøren utdyper hvordan systemet teknisk kan tilrettelegges for å understøtte kritikalitetsnivået, eksempelvis gjennom bruk av redundans, lastbalansering og clustring av alle kritiske komponenter i tjenesten. Det er også viktig at leverandøren utdyper konsekvens ved bortfall av noder eller hvor enkeltknoter tas ned ifm. vedlikehold av systemet eller underliggende infrastruktur.	H	B
T3.11	Systemet skal ha støtte for redundant etablering.	O	
T3.12	Leverandøren bør beskrive systemets støtte for redundant etablering, og beskrive evt. enkeltkomponenter i systemet som ikke kan etableres redundant og begrunne dette.	H	B
T3.13	Systemet skal ha støtte for etablering med lastbalansering.	O	
T3.14	Leverandøren bes beskrive systemets støtte for lastbalansering, og beskrive evt. enkeltkomponenter i systemet som ikke kan etableres med lastbalansering og begrunne dette.	H	B
T3.15	Systemets databaser bør ha støtte for å kjøres i high-availability cluster.	H	B

	Leverandøren bes utdype hvordan systemet kan etableres med slik støtte, samt evt. komponenter og moduler i systemet som ikke kan etableres i et high-availability cluster og begrunne dette.		
T3.16	Leverandøren bør beskrive failovertider for følgende situasjoner: • Bortfall av applikasjonsnoder • Bortfall av databasenoder • Bortfall av enkeltmoduler i nettverk • Bortfall av andre eventuelle komponenter som inngår i systemet	H	B
T3.17	Leverandøren bør beskrive sin anbefaling, med hensyn til forskjellige scenarier for re-etablering av tjenesten, når brudd eller tap av data inntreffer.	H	B
T3.18	Systemet bør ha støtte for tilrettelegging med en «nødløsning» ved bortfall av systemet over en lengre tidsperiode. Leverandøren bes overordnet beskrive en mulig og anbefalt løsning. Merknad: For enkelte høyt kritiske systemer etablert hos Kunden, er det etablert «nødløsning» for å understøtte manuell drift ved bortfall av tjenesten over en lengre tidsperiode. Dette kan eksempelvis gjøres ved en automatisk synkronisering til en lokalt etablert database. Dette gjelder også for systemer som er etablert i High Availability-cluster. Formålet er å eksempelvis muliggjøre utskrift av brikkelister, bestillinger o.a. viktig informasjon som er nødvendig for å manuelt understøtte steriliseringsprosesser og sikre leveranser til Operasjonsavdelingen mens produksjonssystemet er utilgjengelig over en lengre tidsperiode.	M	B

1.3.4 NETTVERK

Kundens tjenesteleverandør er ansvarlig for og drifter Kundens nettverksinfrastruktur med tilhørende nettverkskomponenter som svitsjer, rutere, brannmurer o.l.

Kundens nettverk er klaggjort for IPv6, men dette er p.t. ikke tatt i bruk. Gjeldende protokoll er IPv4.

Kundens nettverk benytter Network Access Control (NAC, IEEE 802.1x) som stenger ned LAN-tilgang for ukjente eller inaktive nettverkstilkoblede enheter på både kablet og trådløs infrastruktur. Kunden har også standardisert brannmursregulering mellom nettverkssoner, hvor inaktive TCP-sesjoner av sikkerhetsgrunner termineres etter 60 minutter. Dette legger krav på evt. utstyr som skal kobles opp i Kundens nettverk, og Leverandør må ta hensyn til dette i sitt tilbud.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.19	Systemet skal støtte IPv4.	O	
T3.20	Systemet bør støtte IPv6.	L	
T3.21	Evt. trådløst utstyr som medfølger leveransen bør benytte Kundens eksisterende trådløse nettverksinfrastruktur. Beskriv eventuell støtte eller avvik fra dette.	H	B
T3.22	Systemet bør konfigureres med Kundens egne IP-adresseserier. Merknad: Dersom den systemet ikke støtter bruk av Kundens egne IP-adresseserier skal et slikt avvik dokumenteres og begrunnes. Dokumentasjonen skal inneholde nødvendige IP-adresser/IP-ranger og TCP-/UDP-portnumre for tjenester som tilgjengeliggjøres.	H	B
T3.23	Systemet bør støtte faste TCP og UDP porter. Leverandøren bes beskrive hvorvidt faste eller dynamiske porter/port-ranger benyttes, samt spesifisere de portene som skal åpnes for i kundens brannmur, inklusiv trafikkretning.	H	B
T3.24	Systemet bør benytte oppdragsgivers nettverk uten å stille leverandørspesifikke begrensninger eller tekniske krav til dette. Leverandøren bes utdype eventuelle begrensninger og krav til oppdragsgivers nettverk. Merknad: Dette kan eksempelvis inkludere: • hvorvidt den samlede, tilbudte løsningen må stå i ett og samme VLAN, eller kan den segmenteres i flere VLAN? • hvorvidt en løsning segmentert over flere VLAN, vil medføre konsekvenser for evt. sertifiseringer og godkjenninger av systemet?	H	B
T3.25	Leverandøren bør beskrive systemets krav til latency i nettverket.	H	B
T3.26	Systemet bør håndtere brudd i nettverkskommunikasjon mellom de ulike komponentene i systemet, slik at funksjonaliteten i størst mulig grad opprettholdes mens systemet gjenoppretter sin	H	B

	nettverkskommunikasjon uten behov for manuelle brukeroperasjoner. Merknad: Sikkerhetsmekanismer i Oppdragsgivers nettverk lukker inaktive nettforbindelser på lag2 & lag3 (hhv. MAC og IP), og det kan oppstå pakketap som medfører brudd i nettverkskommunikasjonen. Leverandørens eventuelle krav og konsekvenser gitt av disse mekanismene må dokumenteres med tanke på design og tilhørende sikkerhetsgodkjenning.		
T3.27	Ved kommunikasjonsbrudd mellom ulike komponenter i systemet, bør kommunikasjonen og systemets funksjonalitet <u>automatisk</u> gjenopprettes når nettverkskommunikasjon er gjenopprettet. Leverandøren bør beskrive evt. avvik fra dette. Evt. enkeltkomponenter som ikke støtter automatisk gjenoppretelse av kommunikasjon og funksjonalitet skal beskrives og begrunnes.	H	B
T3.28	All kommunikasjon bør tåle pakketap med påfølgende retransmisjon. Leverandøren bør beskrive evt. begrensninger og mulige feilsituasjoner i systemet ved pakketap.	H	B
T3.29	Systemet bør støtte DNS navneoppslag (FQDN) fremfor IP-adresser.	H	
T3.30	Systemet bør fungere uavhengig av WINS eller Windows hosts-fil.	H	

1.3.5 SERVER

Kundens tjenesteleverandør drifter Kundens serverplattform, og er basert på bruk av Windows Server og Linux RHEL-servere i et VMware virtualiseringsmiljø. Bruk av fysiske servere unngås hvor mulig.

Operativsystemene støttet er Windows Server 2019, og Linux RHEL 7.5, samt foregående versjon (N og N-1).

Tjenester kan leveres i sentrale datasenter (SDS), felles for alle helseforetakene i Helse Sør-Øst, eller i Kundens lokale datasenter (SHKR). For tjenester etablert i SDS vil disse etableres i Kundens avgrensede sikkerhetssoner, logisk og sikkerhetsmessig adskilt fra andre helseforetak. Endelig plassering av valgt system vil avklares i videre prosess med utarbeidelse av løsningsdesign.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.31	Systemet bør implementeres på virtuell serverplattform driftet av Kundens tjenesteleverandør.	H	B

	Leverandøren bes utdype slik støtte, og dokumentere evt. sertifiseringer systemet har på virtualiseringsteknologi.		
T3.32	Systemet bør implementeres uten bruk av fysiske servere. Merknad: Evt. fysiske servere vil driftes av Kundens tjenesteleverandør. Leverandøren bes begrunne evt. bruk av fysiske servere.	H	B
T3.33	Leverandøren bes utdype minimumskrav til alle servere som vil inngå i tjenesten. Merknad: Eksempel: RAM, CPU, operativsystem (HOST/GUEST), diskkapasitet, RAID-konfigurasjon o.l.	H	B
T3.34	Systemet bør fungere på Windows Server 2019 eller Linux Redhat RHEL 7.5 Leverandøren bes utdype hvile(t) operativsystem som støttes, samt leverandørspesifikke krav til versjon av operativsystem, patcher og avvikende konfigurasjon. Merknad: Dersom systemet støtter flere operativsystemer på servere, bør Leverandøren utdype og gi anbefaling vedr. valg av serverplattform, samt dokumentere evt. fordeler og ulemper mht. løsningsvalg.	H	B
T3.35	Systemet bør til enhver tid støtte siste patcher av operativsystemet på Kundens servere. Leverandøren bes utdype evt. begrensninger, og begrunne disse. Merknad: Det ønskes ikke avvikende patchegrad på servermiljøer	H	B
T3.36	Bruk og vedlikehold av programvare og tjenester installert på servere bør skje uten bruk av lokal administratorrettighet på operativsystemet. Leverandøren bes utdype eventuelle avvik og begrunne disse behovene.	H	B
T3.37	Alle programmer og systemtjenester på servere bør startes som servicer.	H	

	Merknad: Det er ikke ønskelig at programmer og tjenester på servere krever at en bruker er pålogget en sesjon på serverens desktop ved normal bruk.		
T3.38	Alle systemtjenester (servicer) bør startes automatisk ved omstart av server. Merknad: Det skal ikke være behov for manuelle rutiner rundt oppstart av tjenester etter en omstart av server.	H	
T3.39	Alle programmer som kjører som systemtjenester (servicer) på servere bør benytte brukere definert av Kundens tjenesteleverandør. Leverandøren bes utdype evt. avvik og begrunne disse. Merknad: Det tillates ikke globale brukere definert av eller hardkodet av leverandør, eller hvor passord kan hentes fra tilgjengelig dokumentasjon.	H	B

1.3.6 WEBSERVER

Kundens tjenesteleverandør drifter og forvalter Kundens webservere. Kravene besvares dersom systemet leveres som en webapplikasjon eller med webtjenester, eksempelvis API basert på bruk av webservicer og som krever en webserver.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.40	Leverandøren bør utdype hvilke webserverplattformer systemet støtter, eksempelvis Microsoft IIS eller Apache.	H	B
T3.41	Dersom systemet støtter flere webserverplattformer, bør Leverandøren utdype og gi anbefaling vedr. webserverplattform, samt dokumentere evt. forskjeller og begrensninger mellom løsningsvalgene.	H	B
T3.42	Leverandøren bør utdype evt. tilleggskomponenter, eksempelvis .NET runtime, PHP eller tilsvarende rammeverk og 3.partskomponenter som kreves installert på systemets webserver.	H	B

T3.43	Leverandøren bes utdype mekanismer som sikrer webserver og innhold mot uautorisert tilgang. Merknad: Dette inkluderer hvilke sikkerhetsmekanismer som er aktivert, samt hvilke mekanismer som kan aktiveres i tillegg.	H	B
-------	--	---	---

1.3.7 DATABASE

Kundens tjenesteleverandør drifter og forvalter Kundens databaseplattformer.

Databaseplattformene er basert på Microsoft SQL-Server 2016 og Oracle 12c (N og N-1). Microsoft SQL Server Always-On cluster og Oracle Maximum Availability Architecture (MAA) er støttet.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.44	Leverandøren bør utdype hvilke databaseplattformer systemet støtter, inklusiv produktnavn og versjon. Dersom systemet støtter flere databaseplattformer, bør utdyping gi anbefaling vedr. databaseplattform, samt evt. fordeler og ulemper mellom de ulike løsningsvalgene.	H	B
T3.45	Leverandøren bør beskrive evt. spesielle krav til konfigurasjon av databaseplattformen for bruk med systemet.	H	B
T3.46	Systemet bør ha støtte for etablering i et teknisk miljø med High Availability-design (HA), som inkluderer clustring av tjenester (database), speiling av data og eventuelt andre HA mekanismer. Leverandøren bes utdype slik støtte, og gi anbefaling basert på kritikalitetsnivået på tjenesten beskrevet i <i>kapittel 1.3.3 Kritikalitet</i>.	H	B
T3.47	Databasekoblinger for alle systemets komponenter bør være konfigurerbare. Leverandøren bes utdype evt. enkeltvis komponenter som ikke oppfyller dette kravet. Merknad: Det er ikke ønskelig med hardkodede/faste databasekoblinger programmert i løsningen.	H	B

T3.48	Databasekoblinger, med tilhørende brukernavn/passord, bør være kryptert i konfigurasjonsfiler. Leverandør bes utdype slik støtte, og evt. enkeltvis komponenter hvor det ikke støttes.	H	B
T4.49	Systemet bør etableres uten behov for lokalt oppsett av ODBC-drivere for databaseoppkobling på arbeidsflaten.	H	
T4.50	Databasen skal håndtere norsk tegnsatt, datoformat og klokkeslett ved registrering, visning og sortering av data.	O	

1.3.8 ARBEIDSFLATE OG KLIENTAPPLIKASJON

Kundens standard operativsystem er for øyeblikket Windows 7 64-bit på PC-klienter, og det pågår en prosess for omlegging fra Windows 7 til Windows 10 med planlagt ferdigstillelse i 1. kvartal 2020. Ifm. Windows 10-omleggingen planlegges det etablering av Windows 10-baserte nettbrett.

Windows 7-plattformen benytter RES One Suite fra Ivanti (www.ivanti.com, for Windows 10 har produktet endret navn til Ivanti Workspace Control) for administrasjon av klientarbeidsflater, inkludert tilgjengeliggjøring av klientapplikasjoner med alle tilhørende plugins/3.partskomponenter.

Distribusjon av applikasjoner gjøres fortrinnsvis via App-V, hvor applikasjonen knyttes til en bruker, alternativt via SCCM, hvor applikasjonen knyttes til en spesifikk PC klient.

I denne sammenheng benyttes begrepet applikasjon for komponenten eller komponentene i systemet som enten skal distribueres til brukerens arbeidsflate, eller som tilgjengeliggjøres som en webapplikasjon.

Begrepet arbeidsflate benyttes som et samlebegrep for Windows-basert stasjonær PC, bærbar PC, nettbrett og Citrix.

Det er igangsatt en prosess for etablering av en mobilplattform basert på Citrix Xen Mobile for sikker bruk av kliniske og administrative applikasjoner på mobiltelefoner og nettbrett med Android og IOS operativsystemer.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.51	Applikasjonen skal støtte både Windows 7 og Windows 10.	O	
T3.52	Leverandøren bør utdype eventuelle leverandørspesifikke minimumskrav til klient PC, for eksempel: RAM, CPU, OS, disk, RAID, tilkoblingskort o.l.	H	B
T3.53	Leverandøren bør beskrive evt. leverandørspesifikke krav til versjon av operativsystem, patcher og avvikende konfigurasjon.	H	B

T3.54	Applikasjonen bør fungere på Windows 10-baserte nettbrett. Beskriv hvordan slik støtte er tilrettelagt og evt. leverandørspesifikke krav til nettbrett.	M	B
T3.55	Applikasjonen bør fungere i Kundens Citrixmiljø. Utdyp evt. leverandørspesifikke krav til versjon av operativsystem, patcher og avvikende konfigurasjon.	H	B
T3.56	Applikasjonen skal til enhver tid støtte siste patcher av operativsystemet på Kundens arbeidsflater. Merknad: Det tillates ikke avvikende patchegrad på operativsystem på kundens standard arbeidsflater.	O	
T3.57	Applikasjonen bør tilgjengeliggjøres som en webapplikasjon. Beskriv hvordan slik støtte evt. er tilrettelagt, evt. hvilke funksjoner/moduler i systemet som har slik støtte og hvilke som krever en applikasjon på kundens arbeidsflate.	H	B
T3.58	Applikasjonens brukergrensesnitt bør være tilrettelagt for bruk med touch-skjermer. Leverandør bes utdype og eksemplifisere slik støtte. Merknad: På enkelte lokasjoner og steg i arbeidsprosessene er det ikke ønskelig eller praktisk å benytte tastatur og mus ved bruk av systemet, og det ønskes derfor bruk av touchskjermer. Utdypning bør eksempelvis inkludere hvordan brukergrensesnittet er tilrettelagt med store knapper, ikoner o.a. brukergrensesnittkontroller, som sikrer at bruker enkelt kan utføre de mest vanlige brukeroparasjoner med finger og uten bruk av pekepenn (stylus).	H	B
T3.59	Applikasjoner som krever installasjon for tilgjengeliggjøring på Kundens arbeidsflate skal støtte bruk av RES One Suite/Ivanti Workspace Manager for tilretteleggelse av applikasjonen på Kundens arbeidsflate.	O	
T3.60	Applikasjoner som krever installasjon for tilgjengeliggjøring på Kundens arbeidsflate bør leveres som MSI-pakker.	H	B

T3.61	Applikasjoner som krever installasjon for tilgjengeliggjøring på Kundens arbeidsflate skal kunne pakkes av Kundens tjenesteleverandør før den kan distribueres til Kundens arbeidsflater.	O	
T3.62	Applikasjoner som krever installasjon for tilgjengeliggjøring på Kundens arbeidsflate skal støtte distribusjon via App-V og/eller SCCM.	O	
T3.63	Applikasjoner bør støtte distribusjon via App-V. Leverandøren bør utdype hvilke distribusjonsmåter som er støttet for tilgjengeliggjøring av distribuerte applikasjoner, og evt. konsekvenser ved distribusjon som App-V-pakke vs. SCCM. Merknad: Kundens tjenesteleverandør prefererer distribusjon av applikasjonspakker via App-V. Ved behov kan applikasjoner installeres gjennom bruk av SCCM.	H	B
T3.64	Applikasjonen skal ved normal bruk kjøres med standard brukerrettigheter, eksempelvis uten bruk av lokale administrator rettigheter eller andre tilpasninger.	O	
T3.65	Leverandør bes utdype evt. avvik eller nødvendige tilpasninger på brukerrettigheter for normal bruk av applikasjonen.	H	B
T3.66	Systemet skal støtte bruk av både individuell pålogget bruker og fellesbruker (Funksjonsbruker) på operativsystemet. Merknad: Kunden har en standardisert løsning for arbeidsflater hvor det av arbeidsflytmessige årsaker ikke kan benyttes individuelt påloggede brukere på operativsystemet, benevnt «Funksjonsbruker». På arbeidsflater konfigurert med «Funksjonsbruker» er det ikke tillatt med tilgang til intranett, internett eller filshare. Det stilles krav til at applikasjonen som skal benyttes skal ha egen autentisering med bruk av individuelle brukere, og skal være integrert med sentral autentiseringsmekanisme.	O	
T3.67	Applikasjonen bør fungere uten begrensninger som skyldes pålogging på operativsystemet med fellesbruker (Funksjonsbruker).	H	B

	Leverandøren bes utdype evt. støtte og hvilke begrensninger tilknyttet bruk av fellesbruker (Funksjonsbruker) på operativsystemet medfører for applikasjonen.		
T3.68	Applikasjonen bør støtte «Bytt bruker»-funksjonaliteten i Windows 7 og Windows 10.	L	B
T3.69	Webapplikasjoner skal støtte Internet Explorer 11 på Windows 7 og Edge på Windows 10. Merknad: Internet Explorer 11 er standard nettleser på Windows 7. Gjennom planlagt utrulling av Windows 10 vil Microsoft Edge innføres som standard nettleser. Google Chrome er innført som sekundærnettleser på Windows 7 og videreføres som sekundærnettleser på Windows 10.	O	
T3.70	Leverandør bes utdype evt. funksjonalitet eller deler av systemet som ikke støttes eller er begrenset i Internet Explorer 11, Microsoft Edge og Google Chrome. Merknad: Leverandøren bes også utdype hvordan funksjonalitet som ikke støttes eller er begrenset evt. tilrettelegges på annen måte.	H	B
T3.71	Leverandør bes beskrive hvilke nettlesere og versjoner som støttes.	M	B
T3.72	Webapplikasjoner bør utvikles iht. HTML5-standarden.	H	
T3.73	Webapplikasjoner bør fungere uten bruk av 3.partskomponenter eller utvidelser til nettlesere (extensions/add-ons). Leverandøren bes utdype eventuelle behov for eventuelle 3.partskomponenter (utvidelser) som kreves i brukers nettleser, og begrunne behovet.	H	B
T3.74	Leverandøren bør beskrive eventuelle deler av systemet som er tilgjengelig på mobilplattform. Merknad: Kundens tjenesteleverandør er i ferd med å etablere en plattform for sikring og tilgjengeliggjøring av mobile tjenester i Kundens infrastruktur.	H	B

T3.75	Leverandøren bør beskrive hvilke operativsystem som støttes for eventuelle deler av systemet som er på mobilplattform, Dette inkluderer eksempelvis: • Operativsystemer • Versjoner av operativsystemer • Hvordan funksjonaliteten tilgjengeliggjøres (gjennom installert app eller webgrensesnitt) • Hvordan bruker autentiseres i løsningen.	H	B
T3.76	Applikasjonen bør støtte bruk av innebygd kamera for scanning av strekkode/GS1 Datamatrix ved bruk på mobile enheter som nettbrett og mobiltelefon.	H	B
T3.77	Applikasjonen bør støtte bruk av ulike skjermoppløsninger og aspekt-rater (f.eks. 4:3, 16:9). Merknad: Leverandøren skal beskrive evt. begrensninger som finnes i applikasjonen i forhold til skjermoppløsning og aspekt-rater.	H	B
T3.78	Applikasjonen bør støtte både visning i fullskjerm- og vindusmodus.	M	
T3.79	Applikasjonen bør støtte visning av forskjellig informasjon i brukergrensesnittet når applikasjonen benyttes i et flerskjerm-oppsett. Leverandøren bes utdype slik støtte, samt hvilke moduler/funksjoner i systemet som evt. kan/ikke kan fordeles på flere skjermer.	M	B
T3.80	Applikasjonen bør være sentralt konfigurierbar. Leverandøren bes beskrive funksjoner, komponenter eller periferutstyr benyttet med systemet som evt. krever et manuelt oppsett lokalt på arbeidsflaten, samt begrunne disse. Merknad: Det er ikke ønskelig å måtte gjøre lokale innstillinger på den enkelte arbeidsflaten applikasjonen er installert på, da dette vil medføre økt kompleksitet ved endringer og vedlikehold av applikasjonen.	H	B
T3.81	Applikasjonen bør ha en innebygd hjelpefunksjon med søkefunksjon.	H	

T3.82	Der relevant i systemet, skal applikasjonen ha en søkefunksjon for å kunne gjøre oppslag, eksempelvis på historikk, bestillinger, logger, brikker og instrumenter.	O	
T3.83	Leverandør bør kort og på et overordnet nivå utdype hvilke data som kan søkes i, eksempelvis historikk, bestillinger, logger, brikker og instrumenter.	H	B
T3.84	Systemets søkefunksjoner bør støtte prediktive søk. Merknad: Med prediktiv søk menes at relevante søkeord fremvises når bruker begynner å taste inn søkeord.	M	
T3.85	Systemet bør ha støtte for en avansert søkefunksjon. Leverandøren bes kort utdype hvilke muligheter avansert søkefunksjon gir, eksempelvis gjennom søk i kategorier, bruk av «wildcards» og boolske operatorer (dvs. AND, OR, NOT).	M	B

1.3.9 LAGRING, BACKUP OG ARKIVERING

Kunden ønsker å etterleve prinsippene om Data Lifecycle Management, hvor Backup/Restore er en sentral komponent for å ivareta datasikkerhet og dataintegritet. Målsetningen er å benytte sentralisert lagring og backup/restore i størst mulig grad.

Tjenester for lagring, backup og arkivering av data driftes av Kundens tjenesteleverandør.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.86	Systemet bør benytte lagringsløsninger som kan leveres av Kundens tjenesteleverandør. Utdyp eventuelle leverandørspesifikke krav til lagringsløsning. Merknad: Dette kan eksempelvis være lagringsprinsipper, filsystem, krav til diskvolum, krav til lese/skrivehastighet, o.l.	H	B
T3.87	Backup av disk, inklusive programvare, konfigurasjon, kalibrering o.l., på server skal kjøres mot eksisterende sentraliserte og automatiserte backuptjenester hos Kunden.	O	

T3.88	Leverandør bes utdype evt. leverandørspesifikke krav og anbefalinger til backup, eksempelvis begrensninger tilknyttet bruk av backupagent installert på servere tilhørende systemet.	H	B
T3.89	Backup av databaser skal kjøres mot eksisterende sentraliserte og automatiserte backuptjenester driftet av Kundens tjenesteleverandør.	O	
T3.90	Leverandør bes utdype evt. leverandørspesifikke krav og anbefalinger til databasebackup.	H	B
T3.91	Databaser som inngår i systemet skal ha støtte for både full og inkrementell backup (gjennom f.eks. loggbackup/loggshipping) av databaser.	O	
T3.92	Servere som inngår i systemet skal tillate bruk av snapshots for backup av virtuelle maskiner.	O	
T3.93	Systemet bør støtte automatisk arkivering av data ut fra konfigurerbare policyer til forskjellige nivåer i Kundens lagringsløsninger, samt manuell arkivering ved behov.	M	B

1.3.10 UTSKRIFT

Kunden har etablert en løsning for «pull print» (Follow-me print/sikker print) basert på Canon uniFLOW, med sentraliserte printservere og nettverkstilkoblede skrivere/multifunksjonsskrivere. For spesielle behov og bruksområder, eksempelvis tilknyttet arbeidsflyt eller for etikettskrivere, kan det opprettes lokale skrivere uten «pull print». Det foretrekkes at disse tilkobles nettverket og ikke benytter lokal tilkobling, eksempelvis via USB.

Kundens tjenesteleverandør vil normalt levere etikettskrivere for systemer som krever utskrift av etiketter.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T3.94	Systemet bør benytte Kundens «pull print»-tjeneste med nettverksskrivere som leveres av Kundens tjenesteleverandør. Utdyp eventuelle leverandørspesifikke krav til skrivere og evt. behov for lokalt etablerte/tilkoblede skrivere.	H	B
T3.95	Systemet bør støtte etikettskrivere som kan leveres av Kundens tjenesteleverandør. Utdyp eventuelle leverandørspesifikke krav til etikettskrivere og konfigurasjon av disse for bruk med systemet.	H	B

T3.96	Evt. skrivere som medfølger systemet, bør tilkobles nettverket. Merknad: Kunden foretrekker nettverksbaserte skrivere, og ikke lokaltilkoblede skrivere, eksempelvis tilkoblet via USB.	H	B
T3.97	Evt. drivere som medfølger leverandørspesifikke skrivere bør være Citrix sertifiserte.	H	

1.4 Maskinvare og periferiutstyr

Kundens tjenesteleverandør er Kundens hovedleverandør av all maskinvare, inklusiv klient PC'er, servere (virtuelle og fysiske), samt standardisert periferiutstyr, eksempelvis skrivere, etikettskrivere, strekkodelesere, mus, tastatur og skjermer.

Det er av driftsmessige årsaker ikke ønskelig at Leverandør stiller med maskinvare, periferiutstyr eller forbruksmateriell til slikt utstyr som en del av leveransen.

Varekatalogen til Kundens tjenesteleverandør revideres årlig, og hvilke konkrete produkter som er tilgjengelig i varekatalogen vil avhenge av rammeavtalene som er inngått med ulike leverandører ved tidspunktet for etablering av systemet i Kundens tekniske plattform.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T4.1	Systemet bør benytte maskinvare, eksempelvis PC klient, nettbrett og servere, som kan leveres av Kundens tjenesteleverandør, Leverandøren bes utdype eventuell maskinvare som er en del av leveransen, samt begrunne årsak til at dette må eller bør inkluderes.	H	B
T4.2	Systemet bør benytte periferiutstyr, eksempelvis touchskjermer, tastatur, mus, skrivere, etikettskrivere og strekkodelesere, som kan leveres av Kundens tjenesteleverandør. Leverandøren bes utdype eventuelt periferiutstyr som er en del av leveransen, merke, modell, tilkoblingsmulighet (trådløst, nettverk, Bluetooth, USB), samt begrunne årsak til at dette bør inkluderes. For utstyr som kan leveres av Kundens tjenesteleverandør, bes Leverandøren utdype eventuelle krav Leverandøren eller systemet setter til slikt periferiutstyr, eksempelvis støttede merker, modeller, standarder, strekkodeformater og utskriftsformat.	H	B

T4.3	Forbruksmateriell til periferiutstyr, eksempelvis papir, blekk, toner o.a., bør leveres av Kunden eller Kundens tjenesteleverandør.	M	
T4.4	Evt. periferiutstyr som medfølger leveransen bør tilfredsstille krav til vaskbarhet/sterilisering (Medical Grade) der dette skal brukes i «rene» soner. Leverandøren bes utdype hvorvidt eventuelt medfølgende periferiutstyr tilfredsstiller slike krav.	H	B
T4.5	Evt. strekkodelesere som eventuelt medfølger systemet skal støtte bruk av GS1 Datamatrix og GS1-128.	O	
T4.6	Leverandøren bes beskrive hvilke standarder evt. medfølgende strekkodelesere støtter.	H	B

1.5 Integrasjon og interoperabilitet

Systemet skal kunne integreres med Kundens maskiner som benyttes i sterilprosessering, samt sentrale kliniske og administrative systemer som benyttes hos Kunden. Dette vil eksempelvis være:

- maskiner som autoklaver, vaskedekontaminatorer, inkubatorer, sveisemaskiner o.a. som benyttes ifm. sterilprosessering
- operasjonsplanlegger, for bestilling og reservasjon av sterile flerbruksartikler for planlagte operasjoner
- elektronisk pasientjournal eller annet system for å sikre sporbarhet på benyttede sterile artikler til operasjon og pasient
- ERP-systemet (Oracle E-Business Suite, OeBS) for bestilling av sterile engangsartikler

I tillegg er det nødvendig å sikre at systemet som tilbys har tilgjengelige grensesnitt og kan integreres for utveksling av data med fremtidige maskiner, samt nye fag- og administrative systemer som vil etableres i fremtiden.

Det er i Helse Sør-Øst etablert en Regional Integrasjonsplattform, i hovedsak basert på Microsoft Biztalk, som benyttes for integrasjoner mellom ulike fag-, spesialist- og administrative systemer.

Integrasjonsplattformen benyttes både internt i helseforetaket, mellom helseforetak og med eksterne aktører, og inneholder proprietære og standardiserte integrasjonstjenester. Standardiserte integrasjonertjenester er bl.a. basert på standarder som HL7. Integrasjonsplattformen skal fortrinnsvis benyttes ved integrasjoner mellom systemer, ved bruk av internasjonale standarder og standardiserte grensesnitt for slik datautveksling.

Integrasjonsbehovene tilknyttet systemet er ikke endelig avklart, og det vil ved implementering av valgte system være nødvendig å ytterligere detaljere behov, prosesser, grensesnitt, protokoller, standarder, dataflyt og datasett for data som skal utveksles. Dette vil gjøres etter nærmere avtale med Leverandør. Det er derfor viktig for Kunden at systemet har tilstrekkelig grad av fleksibilitet, definerte grensesnitt og støttede standarder, for å

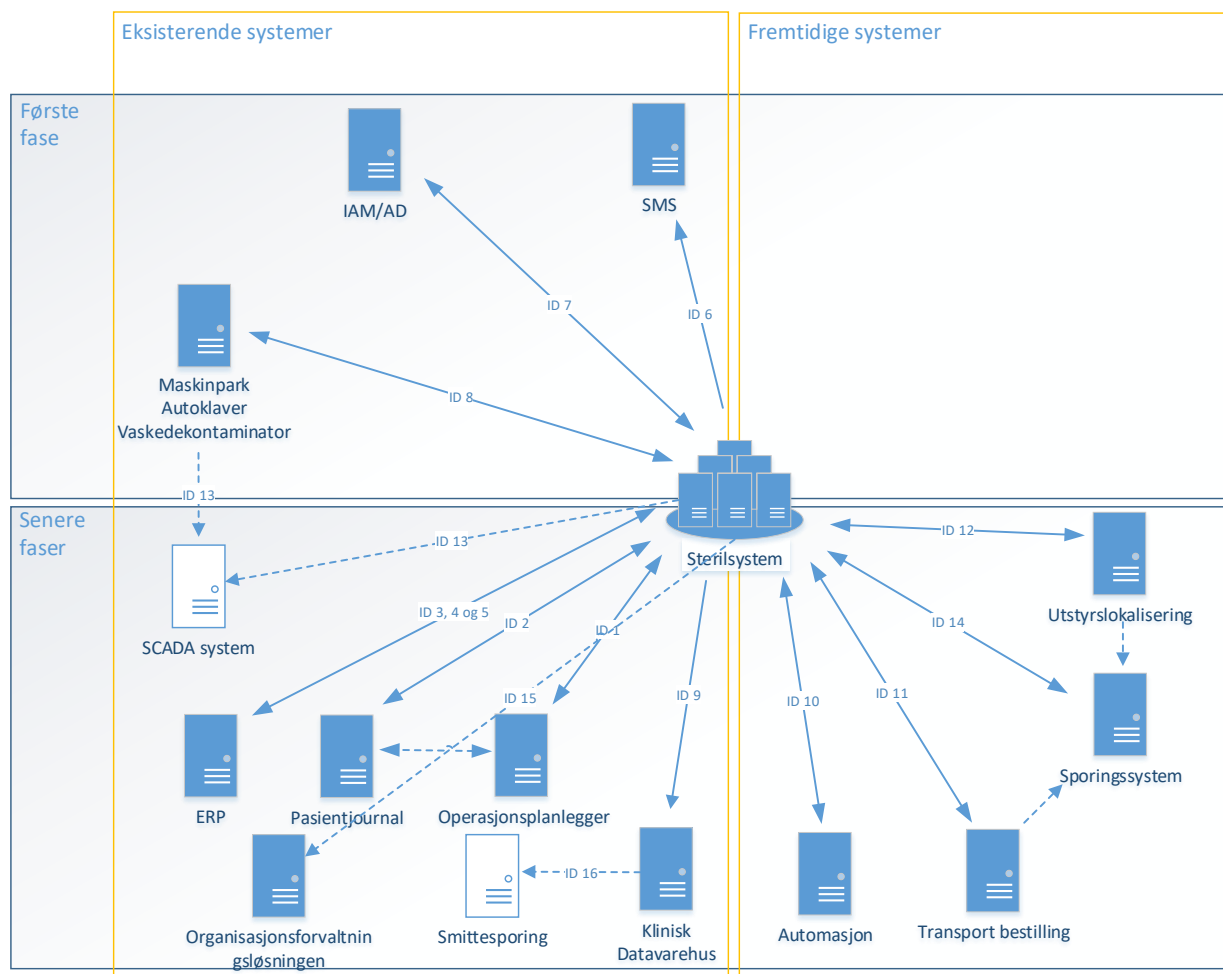
sikre at systemet er godt tilrettelagt for å dekke Kundens integrasjonsbehov med både eksisterende og fremtidig maskinpark, samt Kundens eksisterende og fremtidige kliniske administrative systemer.

Basisintegrasjoner med deler av Kundens tekniske utstyrspark, IAM/AD og evt. SMS-sending vil prioriteres ved innføring av systemet, mens resterende integrasjoner vil kunne komme i én eller flere faser som p.t. ikke er tidssatt.

Hensikten med de etterfølgende kravene er å sikre at systemet har nødvendig fleksibilitet mht. planlagte og fremtidige integrasjoner. Videre er det nødvendig å sikre at systemet støtter bruk av Regional Integrasjonsplattform, med tilstrekkelig grad av sikkerhet, logging og sporbarhet på data som utveksles mellom systemer. Det er derfor nødvendig å avklare viktige elementer som loggfunksjonalitet, sikkerhetsmekanismer, støttede standarder, kommunikasjonsprotokoller, meldingsformater og semantikk. Alle disse faktorene vil påvirke Kundens mulighetsrom for etablering av integrerte systemer, samt tidsforbruk og kostnad ved etablering av integrasjonene.

Det vil være avgjørende at Leverandøren viser evne og kapasitet til å ivareta sitt ansvarsforhold, og har en løsningsorientert tilnærming ved etablering, videreutvikling og vedlikehold av integrasjonene.

Det henvises til «SSA-T Bilag 3b – Kundens tekniske plattform - Integrasjon» og «SSA-T Bilag 1 – Vedlegg 2 – Oversikt over integrasjoner» for nærmere informasjon.



Figur 1 – Integrasjonsdiagram, integrasjonenes ID henviser til tabell i «SSA-T Bilag 1 – Vedlegg 2 - Oversikt over integrasjoner».

1.5.1 GENERELLE KRAV TIL INTEGRASJON

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T5.1	Regional integrasjonsplattform i Helse Sør-Øst bør benyttes for integrasjon med fag- og administrative systemer. Dersom systemet leveres med en egen, separat integrasjonsplattform ,skal denne beskrives og begrunnes.	H	B
T5.2	Leverandøren bør utdype hvordan systemet kan eksponere sine grensesnitt (API) som en tjenestetilbyder for Regional Integrasjonsplattform.	H	B

T5.3	Leverandøren bes utdype alle integrasjonstjenester og API som er inkludert i tilbudt system, med en overordnet beskrivelse av integrasjonstjenestens formål, støttede standarder og protokoller.	H	B
T5.4	Integrasjoner bør etableres iht. internasjonale standarder. Leverandøren bes beskrive evt. standarder som er støttet og for hvilke integrasjoner disse evt. gjelder.	M	B
T5.5	Leverandør bør redegjøre for hvilke standarder, integrasjonsgrensesnitt og hvilken informasjonsbredde som direkte støttes av systemet, samt hvilke integrasjonstjenester som krever tilpasning eller utvikling.	H	B
T5.6	Systemet bør støtte at integrasjoner etableres over synkrone protokoller, der systemet tilbyr eller utfører oppslag direkte i andre tjenester.	H	B
T5.7	Systemet bør sende og motta data gjennom webservices basert på REST og/eller SOAP. Leverandøren bes utdype slik støtte. Merknad: Det er ikke ønskelig med integrasjoner mellom komponenter i systemet eller integrasjoner mellom ulike systemer basert på utveksling av filer eller ved direkte database-til-database kommunikasjon. Evt. avvik fra kravet skal beskrives og begrunnes.	H	B
T5.8	Systemet bør utveksle data på standardiserte formater. Leverandøren bes utdype hvilke standardiserte formater som evt. støttes.	H	B
T5.9	Kommunikasjon mellom ulike komponenter som inngår i systemet levert av Leverandøren bør være kryptert. Merknad: Ved kommunikasjon over https bør TLS benyttes, jfr. <i>kravpunkt T6.45</i> .	H	
T5.10	Kommunikasjon mellom systemet og Kundens fag- og administrative systemer bør være kryptert. Merknad:	H	

	Ved kommunikasjon over https bør TLS benyttes, jfr. <i>kravpunkt T6.45</i> .		
T5.11	Ved integrasjoner hvor systemet leverer data til andre systemer, bør systemet ha mekanismer for å følge opp meldinger som feiler eller blir kvittert med negativ kvittering.	H	B
T5.12	Leverandøren bør bekrefte at alle leverte integrasjoner utvikles i henhold til lover, forskrifter og normen for informasjonssikkerhet i helsesektoren. Leverandøren bes utdype evt. enkeltintegrasjoner som avviker fra dette.	H	B
T5.13	Ved evt. støtte for varsler og informasjon sendt via SMS, bør Regional SMS-tjeneste benyttes. Leverandøren bes utdype slik støtte. Merknad: Systemet kan enten kalle en eksisterende internt etablert webservice eller skrive en XML-fil til et definert filområde i et predefinert format. Tjenesten sikrer at fakturering av forbruk skjer til riktig organisatorisk enhet hos Kunden. Bruk av webservice vil foretrekkes. Etablering av GSM-modem eller sending av SMS over tjenester tilgjengelig på internett tillates ikke.	H	B
T5.14	Leverandøren bør ved forespørsel fra Kunden fremlegge godt beskrevet dokumentasjon av systemets datamodell. Merknad: Kunden vil foretrekke godt dokumenterte API for integrasjonsformål, men det vil for eksempel ved integrasjon med Klinisk Datavarehus kunne være nødvendig å lage tilpassede datauttrekk fra systemet etter Kundens behov.	H	

1.5.2 AUTORATIVE DATAKILDER

Kundens PAS/EPJ-system (DIPS) er normalt autorativ datakilde (masterdatakilde) for klinisk informasjon relatert til pasienter og operasjoner. Kundens ERP-system (Oracle OeBS) er normalt autorativ datakilde for sterilt engangsutstyr. Det er p.t. uavklart om fremtidig system for operasjonsplanlegging vil inngå som en modul i DIPS eller vil være et separat system integrert med DIPS.

Ytterligere avklaringer om håndtering av autorative datakilder vil gjøres i samråd med Leverandøren i forbindelse med utarbeidelse av design og implementering av løsningen.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T5.15	Systemet bør anvende PAS/EPJ-systemet og/eller fremtidig operasjonsplanleggingssystem som autorativ datakilde for informasjon om pasient og operasjoner. Merknad: Det er ikke endelig besluttet hvorvidt PAS/EPJ skal være autorativ datakilde. Dette vil avklares i videre prosess.	H	
T5.16	Systemet bør anvende ERP-systemet som autorativ datakilde for informasjon om engangsartikler. Merknad: Alle engangsartikler har i ERP-systemet statiske artikkelnummer med generisk artikkelbeskrivelse. Det er ikke endelig besluttet hvorvidt PAS/EPJ skal være autorativ datakilde. Dette vil avklares i videre prosess.	H	
T5.17	Systemet bør anvende Organisasjonsforvaltningssystemet for organisasjonsdata og fullmakter	M	
T5.18	Systemet bør være autorativ datakilde for lastbærere, brikker og sterilt flerbruksutstyr.	H	
T5.19	For informasjonen systemet skal være autoritativ datakilde for, bør det være mulig å utføre CRUD-operasjoner (Create/Read/Update/Delete) gjennom et programmeringsgrensesnitt (API). Merknad: Leverandøren bes utdype slik støtte. Dette gjelder eksempelvis for brikke- og instrumentlister, hvor systemet forventes å være autorativ datakilde. For informasjon hvor systemet skal ivareta sporbarhet og etterrettelighet, vil kun Read-operasjoner kunne tillates.	H	B

1.5.3 INTEGRASJON MED MASKINER BENYTTET I STERILPROSESSERING

Systemet skal kunne kobles opp mot Kundens maskiner benyttet i sterilprosessering, eksempelvis autoklaver, vaskedekontaminatorer, ultralydvaskere, sveisemaskiner og inkubatorer. Formålet er å sikre logging og sporbarhet på prosessinformasjon fra utstyret, samt evt. annen relevant informasjon, eksempelvis lot/identitetsnummerering i vaske- og steriliseringsprosesser.

Deler av Kundens maskinpark er i dag ikke tilkoblet nettverket, ettersom ikke alle maskiner i Kundens maskinpark har tilkoblingsmuligheter. Enkelte maskiner med støtte for tilkobling til nettverket er i dag etablert i isolerte soner/nettverk, fysisk/sikkerhetsmessig avgrenset fra Kundens infrastruktur for øvrig. Ved implementering av systemet, vil Kunden gjennomføre flytting av maskiner som skal integreres til nye tilgangsstyrte/regulerte nettverkssoner i infrastrukturen før de kan integreres med systemet.

Det vil ifm. innføringen av systemet måtte utarbeides en helhetlig løsningsbeskrivelse for systemet, hvor nettverksmessig plassering av maskiner og integrasjoner av disse med systemet vil omhandles. Deler av maskinparken vil tilkobles ved innføringstidspunktet iht. Kundens prioriteringer, mens ytterligere tilkobling av maskiner vil skje gradvis over tid etter at systemet er etablert. Tilkobling vil skje iht. Kundens prioriteringer eller fortløpende ved anskaffelse av nye maskiner. Videre detaljering og prioriteringer vil gjøres ifm. planlegging av innføring av systemet.

For oversikt over eksisterende maskinpark som planlegges integrert i en tidlig fase, se vedlegg «SSA-T Bilag 1 – Vedlegg 3 - Oversikt over maskinpark». Vedlegget gir en oversikt over de ulike merker og modeller av Kundens maskiner ved tidspunktet for utarbeidelse av konkurransegrunnlaget, og det må forventes endringer i dette frem til innføringstidspunktet. Oversikten er dermed ikke uttømmende. Videre vil det være en naturlig utskifting og modernisering av maskinparken i løpet av kontraktperioden for systemet. Det vil for nye maskiner som anskaffes etter beslutning om valg av system er tatt, stilles krav om at maskiner som anskaffes skal støtte integrasjon med systemet.

Kundens maskinpark forventes på et senere tidspunkt å bli tilkoblet Kundens SCADA-system (Supervisory Control And Data Acquisition) for teknisk driftsovervåking, enten gjennom integrasjon direkte fra maskinen, gjennom styringssystemer medfølgende maskinen eller gjennom sterilsystemet.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T5.20	Systemet skal støtte integrasjon med maskiner, eksempelvis autoklaver og vaskedekontaminatorer.	O	
T5.21	Leverandøren bør dokumentere hvilken støtte for integrasjon som tilbys for merker/modeller av eksisterende autoklaver, vaskedekontaminatorer o.l. iht. oversikt i dokumentet «SSA-T Bilag 1 - Vedlegg 3 - Oversikt over maskinpark». Merknad:	H	B

	Det skal angis om merke/modell er støttet som en del av avtalen, delvis støttes, ikke kan støttes eller kan støttes ved evt. tilleggsutvikling av integrasjon.		
T5.22	Leverandøren bør vedlegge en komplett liste over maskiner og kontrollsystemer for styring og overvåking av maskiner som støttes. Listen bør inkludere systemnavn, merke, modell og evt. versjon. Merknad: Leverandøren bes også utdype evt. begrensninger i integrasjonen med kontrollsystemer eller utstyret, eksempelvis: • begrensninger i datasett • hvorvidt integrasjonen støtter uttrekk av sanntidsdata av prosessinformasjon eller kun etter maskinens prosesser er ferdig	H	B
T5.23	Leverandøren bør beskrive integrasjonsmekanismer og integrasjonsgrensesnitt for integrasjon med maskiner.	H	B
T5.24	Leverandøren bør beskrive hvordan integrasjonsgrensesnitt med maskiner vedlikeholdes ved endringer av kommunikasjonsprotokoll, f.eks. gjennom at det er inngått samarbeidsavtale med leverandører av maskiner, som sikrer tilgang på oppdaterte kommunikasjonsprotokoller.	H	B
T5.25	Systemet bør ha støtte for simulering av kommunikasjon med maskiner, eksempelvis autoklaver og vaskedekontaminatorer, for bruk i et testmiljø. Merknad: Leverandøren bes utdype eventuell støtte systemet har for simulering av maskiner i et testmiljø.	H	B
T5.26	Systemet bør kunne formidle eller tilgjengeliggjøre tekniske driftsdata fra integrerte maskiner til ett eller flere SCADA systemer. Leverandøren bes utdype slik støtte, og gi anbefalinger vedr. integrasjon.	M	B

1.5.4 INTEGRASJON MED ADMINISTRATIVE FAGSYSTEMER

Kunden benytter i dag Oracle E-Business Suite som sitt ERP-system. ERP-systemet vil håndtere bestilling av produkter fra leverandør og vil være autorativ datakilde for engangsartikler.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T5.27	Systemet skal ha støtte for integrasjon med Kundens ERP-system.	O	
T5.28	Systemet bør ha støtte for å hente nødvendige masterdata om sterile engangsprodukter fra Oracle E-Business Suite for bestilling og sporing av bruken av sterile engangsprodukter. Leverandøren bes utdype slik støtte, og gi anbefalinger vedr. integrasjon.	H	B
T5.29	Løsningen bør ha støtte for å sende en bestilling i XML format til Oracle E-Business Suite for sterile engangsartikler som skal bestilles igjennom ERP systemet. Leverandøren bes utdype slik støtte, og gi anbefalinger vedr. integrasjon.	H	B
T5.30	Løsningen bør ha støtte for å motta en digital pakkseddel i XML format og sammenstille den med pakkseddel fra andre kilder. Leverandøren bes utdype slik støtte, og gi anbefalinger vedr. integrasjon.	H	B
T5.31	Løsningen bør kunne motta avviksmelding på en bestilling sendt til ERP-systemet og benytte denne til videre varsling.	H	
T5.32	Løsningen bør ha støtte for å hente og benytte en oppdatert oversikt over organisasjonsdata og fullmakter, eksempelvis organisasjonsheter, kostnadssteder m.m., fra Kundens Organisasjonsforvaltningssystemet.	M	

1.5.5 INTEGRASJON MED KLINISKE FAGSYSTEMER

Kunden fornyer og oppgraderer kontinuerlig sine fagsystemer, og har en pågående prosess for å oppgradere DIPS Classic til siste generasjon DIPS Arena. Det planlegges derfor å avvente med integrasjoner mellom sterilsystemet og EPJ-systemet inntil DIPS Arena er etablert.

Det er etablert et prosjekt i OUS som skal utarbeide kravspesifikasjon for operasjonsplanlegger, hvor krav om tett integrasjon mellom operasjonsplanleggeren og sterilsystem vil bli ivaretatt. Det er ikke endelig besluttet hvorvidt operasjonsplanlegger vil etableres som en funksjon i DIPS Arena, eller om operasjonsplanleggeren vil være et separat system integrert med DIPS Arena. Uavhengig av løsningsvalg, vil det kravstilles at operasjonsplanlegger har relevant funksjonalitet og tilgjengelige integrasjonsgrensesnitt for etablering av integrasjoner med sterilsystemet.

Inntil integrasjon med operasjonsplanlegger er etablert vil det være nødvendig at systemet innehar funksjonalitet for å manuelt opprette bestillinger og reserverasjoner av sterilt utstyr.

Det er nødvendig å etablere sporbarhet på hvilke brikker som er benyttet på hvilken operasjon og på hvilken pasient, samt kobling til steriliseringsprosessen for brikken benyttet på pasient (batch/lot).

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T5.33	Systemet skal støtte integrasjon med kundens EPJ-system.	O	
T5.34	Systemet skal støtte integrasjon med Kundens system for operasjonsplanlegging for bestilling og reserverasjon av sterile produkter til en operasjon. Merknad: Dette kan ved tidspunktet for etablering av integrasjonen være DIPS Arena, eller annet p.t. ukjent system.	O	
T5.35	Systemet bør støtte en integrasjon med operasjonsplanlegger, hvor systemet mottar en bestilling for reserverasjon av sterile produkter til en operasjon. Leverandøren bes utdype slik støtte, og gi anbefalinger vedr. integrasjon.	H	B
T5.36	Ved integrasjoner med operasjonsplanlegger, bør systemet støtte at operasjoner kan utføres på flere fysiske lokasjoner.	H	
T5.37	Systemet bør håndtere oppdatering av bestillinger fra operasjonsplanlegger. Systemet bør støtte oppdateringer inntil operasjonen er satt som ferdigstilt i operasjonsplanleggeren. Leverandøren bes utdype hvordan løsningen støtter løpende oppdateringer på en bestilling.	H	B
T5.38	Dersom utstyr planlagt benyttet til en operasjon skulle bli utilgjengelig av uforutsette grunner, bør systemet kunne sende en negativ kvittering til operasjonsplanlegger. Kvitteringen bør inneholde feilkode og forståelig beskrivelse av feilsituasjonen. Leverandøren bes utdype slik støtte.	H	B
T5.39	Leverandøren bes utdype hvordan sporingsinformasjon for sporing av sterile produkter for tilknytning mot pasient kan leveres strukturert til andre fagsystemer og hvilke dataformater systemet støtter.	H	B

1.5.6 INTEGRASJON MED ANDRE SYSTEMER

Kunden har i tillegg en pågående prosess for å vurdere fremtidig RTLS-system (Real-Time Locating System) for lokalisering, samt sporing eksempelvis gjennom bruk av et GS1 EPCIS-system.

I tillegg har kunden pågående prosesser for etablering av ytterligere systemer det i fremtiden kan tenkes å integrere systemet med, eksempelvis innen logistikk og automasjon.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T5.40	Systemet bør støtte automatisk oppdatering av status o.a. relevant informasjon basert på integrasjon med system for lokalisering. Leverandøren bes utdype muligheter for slik støtte i systemet. Merknad: Kunden har en pågående prosess for å etablere et RTLS (Real-Time Locating System) for utstyrslokalisering, samt en teknisk infrastruktur eksempelvis basert på RFID, WLAN, Bluetooth e.l., i ulike kombinasjoner. Det er p.t. ikke besluttet valg av system eller tekniske løsninger.	H	B
T5.41	Systemet bør ha støtte for automatisk oppdatering av status o.a. relevant informasjon basert på integrasjon med system for sporing, eksempelvis sporingssystem basert på GS1 EPCIS.	H	B
T5.42	Leverandøren bes utdype hvordan systemet kan tilrettelegge for integrasjon med et system for bestilling av transportoppdrag. Merknad: Kunden har i dag ikke tatt i bruk et sentralisert system for bestilling av transportoppdrag for håndtering av oppdrag utført ved bruk av interne eller eksterne aktører.	L	B
T5.43	Leverandøren bes utdype hvordan systemet kan tilrettelegge for bruk av automasjon og robotisering ifm. sterilproduksjon.	M	B
T5.44	Leverandøren bes utdype hvordan systemet kan tilrettelegge for økt bruk av automatiserte transportløsninger, eksempelvis AGV, autonome transportdroner eller autonome kjøretøy.	L	B
T5.45	Leverandøren bes utdype hvordan systemet kan tilrettelegge for økt bruk av automatiserte løsninger ved lagerstyring og plukk fra lager, f.eks. gjennom bruk av robotisering.	L	B

T5.46	Leverandøren bes utdype evt. andre integrasjoner leverandøren anbefaler, som kan tenkes å gi effekter og gevinster for Kunden.	M	B
-------	--	---	---

1.6 Informasjonssikkerhet

Kunden plikter å oppfylle norsk lovverk, og stiller strenge krav til oppfyllelse av relevant lovverk vedr. informasjonssikkerhet ved anskaffelse, etablering, drift og forvaltning av sine systemer.

Informasjonssikkerhet handler om å sikre at informasjonen systemet behandler:

- ikke blir kjent for uvedkomne (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkomne (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Det stilles krav til at tilbudt løsning skal tilfredsstille krav i Personvernforordningen (GDPR) artikkel 25 – Innebygd personvern, se:

- Datatilsynets veileder for innebygd personvern - <https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/>
- Datatilsynets informasjon om personvernforordningens krav til innebygd personvern til leverandører og utviklere i helse- og omsorgssektoren - <https://www.datatilsynet.no/personvern-pa-ulike-omrader/forskning-helse-og-velferd/leverandorer-og-utviklere-i-helse--og-omsorgssektoren/>
- GDPR – Article 25, Data protection by design and by default (på Engelsk) - <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>

Kunden er pålagt å etterleve Direktoratet for eHelse sin «Norm for informasjonssikkerhet» («Normen»), se:

- «Normen» - <https://ehelse.no/normen>
- «Normen» (på Engelsk) - <https://ehelse.no/normen/documents-in-english>

For å understøtte Kundens forpliktelser og lovkrav tilknyttet informasjonssikkerhet, har Helse Sør-Øst definert et sett krav til informasjonssikkerhet i *Regionalt ledelsessystem for Informasjonssikkerhet*. Kravsettet inneholder krav til infrastruktur, systemer og tjenester, samt til leverandører og ansvarlige for drift og forvaltning av infrastruktur, systemer og tjenester for Kunden, se forøvrig:

- <https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet> eller «SSA-T Bilag 1 - Vedlegg 5c - Sikkerhetsprinsipper og -krav for IKT-infrastruktur og applikasjoner».

Leverandøren forutsettes å ha satt seg inn i disse sikkerhetsprinsippene, og at disse kan etterleves. Sikkerhetskravene i dette kapittelet er spesielt trukket ut fra *Regionalt ledelsessystem for informasjonssikkerhet*, og vil tillegges vekt i anbudet.

Før systemet kan etableres, må det gjennomføres og foreligge en godkjent risikovurdering av systemets endelige løsningsdesign, med alle tilhørende komponenter, tjenester og konfigurasjon, slik systemet er planlagt etablert hos Kunden. Dette vil normalt utarbeides av Kundens tjenesteleverandør, i samarbeid med Kunde og Leverandør.

1.6.1 GENERELLE KRAV TIL AUTENTISERING OG AUTORISERING

På bakgrunn av interne krav og krav i lover og forskrifter, har Kunden høy fokus på identifisering av brukere og tilgangskontroll til applikasjoner.

Ønsket er sentralisert og eksternalisert tilgangsstyring med automatisert opprettelse, endring og sperring av brukere. Gevinsten er enklere administrasjon av tilganger og høyere sikkerhet gjennom rettidig styrt tilgang til ressurser. Målet er i siste ende å ha en «policy»-basert (Attribute Based Access Control, ABAC) styring av rettigheter som gir en finmasket og automatisert styring av tilganger som tilpasser seg brukerens arbeidssituasjon og derigjennom gir brukeren de tilganger som er nødvendige til det arbeidet bruker skal utføre i den gitte situasjon.

På veien til målet har kunden og kundens tjenesteleverandør flere komponenter som kan benyttes for autentisering og autorisering.

Deler av dette er beskrevet ytterligere i «SSA-T Bilag 3C – Kundens tekniske plattform – Identitet og tilgangsstyring».

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T6.1	Autentisering av brukere skal gjøres mot sentral autentiseringsløsning. Merknad: Med sentral autentiseringsløsning menes enten regional IAM-løsning etablert av Kundens tjenesteleverandør eller mot Kundens katalogtjeneste (Active Directory).	O	
T6.2	Systemet bør ha støtte for attributtbasert tilgangsstyring (ABAC). Merknad: Leverandøren bør utdype hvordan systemet er tilrettelagt eller kan tilrettelegges for attributtbasert tilgangsstyring, samt hvilke attributter som kan støttes for tilgangsstyring, eksempelvis organisasjon, ansattforhold, turnus, delegert ansvar og påloggingssted m.v.	H	B
T6.3	Dersom systemet ikke har støtte for attributtbasert tilgangsstyring, bør systemet ha støtte for rollebasert tilgangsstyring (RBAC). Merknad: Leverandøren bør utdype hvordan systemet er tilrettelagt for rollebasert tilgangsstyring, og hvorvidt roller og	H	B

	funksjonalitet/tilganger tilhørende rollen er forhåndsdefinert eller kan tilpasses i systemet.		
T6.4	Systemet bør etableres uten behov for en lokal brukerdatabase som manuelt må vedlikeholdes. Merknad: Dersom systemet har en brukerdatabase som manuelt må vedlikeholdes, bes leverandøren begrunne et slikt behov og beskrive formålet med denne.	H	B
T6.5	Varigheten av brukerens aktive sesjon i systemet skal være tidsavgrenset.	O	
T6.6	Systemet bør støtte konfigurert tidsavgrensning for brukerens aktive sesjon. Dersom systemet eller deler av systemet ikke har slik støtte, skal disse begrensningene beskrives og begrunnes.	H	B
T6.7	Systemet bør støtte at én og samme identifiserte bruker i systemet kan ha én eller flere roller, være tilknyttet én eller flere organisatoriske enheter, eller kunne opptre i samme eller forskjellige roller på tvers av organisatoriske enheter. Leverandøren bes utdype hvordan systemet evt. er tilrettelagt for å understøtte dette. Merknad: Dette kan eksempelvis være i forbindelse med: 1. at bruker på gitte tidspunkter kan være vakthavende på sin lokalisasjon, som krever eleverte rettigheter i en avgrenset tidsperiode 2. at bruker i noen sammenhenger kan ha en annen funksjon i arbeidsprosessene enn bruker normalt har 3. at bruker normalt arbeider ved én av lokalitetene, men i perioder bistår ved andre lokaliteter	H	B
T6.8	Applikasjonen bør støtte unik identifikator for entydig identifikasjon av organisasjonsenheter.	H	
T6.9	Systemet bør støtte at det er mer enn én autentisert bruker på systemet fra samme arbeidsflate. Utdyp evt. støtte, samt hvordan systemet håndterer pålogget bruker dersom ny bruker logger inn, f.eks. ved å avslutte foregående brukers	M	B

	sesjon eller holde sesjoner inaktive, men med mulighet for reaktivering ved raskt brukerskifte. Merknad: Det vil være aktuelt for enkelte bruksområder å konfigurere kundens arbeidsflate med «funksjonsbruker» (jmf. «SSA-T Bilag 3a – Kundens tekniske plattform»), som vil muliggjøre at flere brukere benytter samme innloggede arbeidsflate med hurtig brukerskifte i systemet. SSO vil ikke kunne benyttes på arbeidsflate med «funksjonsbruker».		
T6.10	Det skal kun benyttes personlige, identifiserte, brukere i systemet. Merknad: Fellesbrukere eller annen form for deling av brukerkontoer skal ikke forekomme i systemet.	O	
T6.11	Globale brukere, eksempelvis administrator, SA, root eller tilsvarende definert av Leverandør eller hardkodet i systemet bør unngås. Merknad: Kunden ønsker ikke pre-definerte eller hardkodede brukere som kan benyttes for ikke-sporbar tilgang til systemet, Dette gjelder også for 3. parts komponenter som benyttes i systemet. Eventuelle avvik fra dette bes utdypet og begrunnes, samt hvorvidt slike brukere kan deaktiveres eller slettes.	H	B
T6.12	Ved evt. støtte for integrasjon med Kundens katalogtjeneste, bør dette gjøres med sanntidsoppslag mot katalogtjenesten ved autentisering av brukere. Leverandøren bes utdype og begrunne evt. avvik fra dette. Merknad: Det er ikke ønskelig at integrasjon med Kundens katalogtjeneste benyttes for synkronisering av brukere til evt. lokal brukerdatabase i systemet.	M	B
T6.13	Passord bør overføres mellom systemets ulike komponenter i kryptert form. Ved evt. støtte for integrasjon med Kundens katalogtjeneste, bør dette skje via LDAP over SSL.	H	
T6.14	Passord som lagres i systemet, bør lagres kryptert eller som hash.	H	B

	Leverandøren bes utdype hvordan passord som evt. lagres i systemet er lagret, eksempelvis i form av klartekst, kryptert eller som hash.		
T6.15	Eventuelle lokale administratortilganger til administrasjonsmoduler bør håndheve Helse Sør-Østs krav til passordkompleksitet og lengde. Merknad: Kravene er p.t.: • Alle brukerkontoer skal ha passord • Passordet skal bestå av minst 8 tegn • Passordet skal ha minst 3 av 5 følgende egenskaper (jf. Microsoft complex password policy) ○ Store bokstaver (A-Z) ○ Små bokstaver (a-z) ○ Tall (0-9) ○ Spesialtegn (~!@#\$%^&* _-+=` \\(){}[];:'"<>,.?/) ○ Unicode Leverandøren bes utdype evt. støtte og avvik fra denne, samt hvorvidt passordkompleksitet er konfigurerbart i systemet. Helse Sør-Østs passordpolicy er nærmere beskrevet i «SSA-T Bilag 1 – Vedlegg 5b - Fellesregional passordpolicy for helseforetakene i Helse Sør-Øst».	H	B
T6.16	Systemet bør støtte Single Sign-On (SSO). Leverandøren bes utdype hvordan SSO støttes. Merknad: SSO vil ikke kunne benyttes på arbeidsflater hvor «funksjonsbruker» benyttes.	H	B
T6.17	Ved identifikasjon eller autentisering av bruker gjennom avlesing og dekoding av ansattkort, bør systemet autentisering skje via kundens sentrale autentiseringsmekanismer.	H	B
T6.18	Ved nektet tilgang til systemet bør applikasjonen presentere begrunnelsen på en forståelig måte til sluttbruker.	M	
T6.19	Ved rollebasert tilgangsstyring (RBAC) bør systemet støtte at rettigheter tildeles roller, og ikke tildeles individuelle brukere.	H	

1.6.2 KRAV TIL BRUK AV LØSNING FOR IDENTITY AND ACCESS MANAGEMENT

Kundens tjenesteleverandør har etablert en felles, regional løsning for Identity and Access Management (IAM) for bl.a. federering og provisjonering av brukere. Formålet er å sikre enhetlig og sentralisert tilgangsstyring for systemer etablert i Kundens tekniske plattform og på tvers av helseforetakene i Helse Sør-Øst. Det prefereres derfor systemer som kan integrere med IAM-løsningen gjennom federering og provisjonering av brukere, og at systemet støtter internasjonale standarder som eksempelvis SAML eller OpenID Connect for formålet.

Det er nødvendig at systemet støtter autentisering mot sentralisert løsning for tilgangsstyring, og støtte for attributtbasert tilgangsstyring (ABAC) vil prefereres. Dersom krav til ABAC ikke kan understøttes av systemet, vil rollebasert tilgangsstyring (RBAC) med provisjonerte roller være aktuelt alternativ. Det er ikke ønskelig med rollebasert tilgangsstyring som krever manuelt vedlikehold av brukere og tilganger i en lokal brukerdatabase i systemet.

Dersom systemet ikke kan integreres med Kundens IAM-løsning, er det nødvendig at systemet kan integreres med Kundens katalogtjeneste (Active Directory) via LDAP, fortrinnsvis LDAP over SSL (se kravpunkt T6.13).

Systemet bør ha tilgangsstyring som etterlever at medarbeideres rolle og oppgaver gir tilgang til funksjonalitet, og at den organisatoriske tilhørighet er styrende for hvilke data brukeren får adgang til.

IAM-løsningen etablert av Kundens tjenesteleverandør er nærmere beskrevet i «SSA-T Bilag 3c – Kundens tekniske plattform - Identitet og tilgangsstyring».

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T6.20	Systemet bør støtte federering som autentiseringsmekanisme.	H	
T6.21	Systemet bør støtte anerkjente standarder for federering som autentiseringsmekanisme, eksempelvis SAML 2.0 eller OpenID Connect.	H	
T6.22	Ved bruk av SAML, bør systemet støtte "Service Provider initiated" federeringsprosess.	H	
T6.23	Ved pålogging til systemet bør som minimum attributtene brukerid, organisasjonstilknytning og rolle tas imot fra sentral autentiseringsløsning for å gi bruker tilgang til informasjon og funksjonalitet i systemet ved etablering av brukers sesjon.	H	
T6.24	Systemet bør håndheve sikkerhetssesjonen. Merknad:	H	

	Dette inkluderer, men er ikke begrenset til inaktivitet, start- og sluttidspunkt på token.		
T6.25	Systemet bør bruke federeringsfunksjon dersom en bruker må autentiseres i en annen brukers sikkerhetssesjon. Merknad: Dersom systemet støtter kontroll og godkjenning (sidemannskontroll) med behov for autentisering av annen bruker enn den allerede innloggede, bør dette gjøres med sentralisert autentiseringsmekanisme. Leverandør bes beskrive sikkerhetsfunksjonalitet ved sidemannskontroll.	H	B
T6.26	Systemet bør ha mulighet til å falle tilbake til alternativ autentiseringsmekanisme dersom federeringsløsning er deaktivert eller utilgjengelig. Merknad: Dette innebærer at det ved bortfall av sentral federeringsløsning fortsatt må være mulig å logge på systemet for å sikre drift. Alternativ autentiseringsmekanisme kan i denne sammenhengen eksempelvis være bruk av automatisk provisjonerte, lokalt lagrede brukeridenter. Kravet bør sees i sammenheng med nødløsning, beskrevet i kravpunkt T3.18.	H	
T6.27	Ved vellykket <i>autentisering</i> av en bruker som <u>ikke</u> er <i>autorisert</i> til å benytte systemet, bør systemet ikke falle tilbake til alternativ autentiseringsmekanisme og bruker bør få beskjed om at tilgang er nektet.	H	
T6.28	Systemet bør spørre ekstern autoriseringstjeneste om det finnes en aktiv pasient-behandlerrelasjon, dersom intern tilgangskontrollmekanisme ikke kan avgjøre tilgang. Merknad: Dersom løsningen er behandlingsrettet helseregister er det krav om tilgang på pasientdata reguleres gjennom om det finnes en pasient-behandlerrelasjon. Det er p.t. ikke endelig avklart hvorvidt systemet vil kunne falle under kategorien behandlingsrettet helseregister.	L	

T6.29	Dersom ekstern autoriseringstjeneste benyttes bør kall mot denne gjøres iht internasjonale autoriseringsstandarder, eksempelvis XACML og OAuth.	H	
T6.30	Applikasjonen bør støtte én entydig regional bruker id per person (identitet). Merknad: Brukere bør identifiseres entydig på tvers av helseforetak i regionen.	L	
T6.31	Applikasjonen bør støtte provisjonering av brukere, dvs. oppretting, lesing, endring og sletting via et standardisert programmeringsgrensesnitt (API).	H	
T6.32	API for provisjonering bør støtte kryptert kommunikasjon. Merknad: Leverandøren bes utdype slik støtte, samt hvordan kommunikasjon er kryptert og iht. hvilke(n) standard(er).	H	B
T6.33	API for provisjonering bør støtte SCIM-standarden.	H	
T6.34	API for provisjonering bør være REST-basert, med kommunikasjon over HTTPS.	H	
T6.35	APIet bør gjøre det mulig å automatisere provisjonering av brukere i systemet, slik at rettigheter ikke må konfigureres manuelt.	H	
T6.36	APIet bør muliggjøre tildeling av individuelle rettigheter i tillegg til standardtilganger.	H	
T6.37	Systemet bør tilby et brukergrensesnitt for brukeradministrasjon, i tillegg til APIet for provisjonering.	H	
T6.38	APIet bør tilgjengeliggjøre data om brukerne i systemet slik at APIet kan benyttes ved revisjon av brukertilganger.	H	

1.6.3 LOGGING

Det stilles strenge krav til logging av bruk av systemet og sikkerhetshendelser i systemet.

Kundens tjenesteleverandør har etablert et sentralt loggmottak for håndtering av relevante system- og sikkerhetslogger fra Kundens systemer. Sentralt loggmottak er basert på Splunk.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
----------	------	-----------------------------	-------------

T6.39	Alle relevante handlinger bør logges. Relevante handlinger skal måles opp mot informasjonssystemet, men som et minimum skal følgende logges: • innlogginger • forsøk på innlogginger • oppretting, endring og sletting av data • oppretting, endring og sletting av brukere • innsyn eller endring i eventuelle helseopplysninger lagret i systemet • endringer, eller forsøk på endringer, i systemkonfigurasjonen Merknad: For ytterligere informasjon, henvises det til Normens faktaark 15 – «Logging og oppfølging av logger», se https://ehelse.no/normen/faktaark/faktaark-15-logging-og-oppfolging-av-logger	H	B
T6.40	Følgende informasjon skal minimum lagres ved tilgang og aktivitet i systemet: • Bruker, og hvilken av brukerens roller som var aktiv, som har forsøkt utført eller gjennomført tilgang/enhver form for aktivitet • Dataelementet som er opprettet, lest, endret eller slettet • Om dataelement endret er opprettet, lest, endret, skrevet ut, slettet eller annen aktivitet som det er mulig for autoriserte å gjennomføre • Dato og tidspunkt for gjennomføring/hendelsen • Angivelse av enhet hvor aktivitet/uautorisert tilgang er forsøkt utført og evt. gjennomført Merknad: For ytterligere informasjon, henvises det til Normens faktaark 15 – «Logging og oppfølging av logger», se https://ehelse.no/normen/faktaark/faktaark-15-logging-og-oppfolging-av-logger	H	B

1.6.4 NETTVERK OG KOMMUNIKASJON

Oppdragsgivers kablede og trådløse nettverk benytter NAC (802.1x) som stenger ned LAN-tilgang for ukjente eller inaktive enheter. Enheter som ikke kan autentiseres i nettverket vil plasseres i et karantenenett uten tilgang til andre komponenter og tjenester i infrastrukturen.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T6.41	Eventuelle leverandørleverte komponenter som skal tilkobles Kundens nettverk, eksempelvis strekkodelesere, etikettskrivere o.a. teknisk utstyr, bør være kompatibel med bruk av IEEE 802.1x (Network Access Control). Merknad: For alt utstyr som skal tilkobles og gis tilgang til Kundens nettverk, registreres utstyret som hovedregel med godkjent MAC-adresse for tilgangskontroll. Leverandør bes utdype evt. avvik i slik støtte.	H	B

1.6.5 INTEGRASJONGRENSESNIITT

Integrasjonsgrensesnitt må sikres, slik at integrasjonsgrensesnittene ikke kan muliggjøre en vei inn i systemet, muliggjøre endring av eller tilgjengeliggjøre informasjon systemet behandler for uvedkomne.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T6.42	Alle integrasjonsgrensesnitt (API) skal være sikret mot uautorisert bruk.	O	
T6.43	Alle tilgangsforespørsler til integrasjonsgrensesnitt (API) bør autentiseres vha. en internasjonal standard tilsvarende SAML. Leverandør bes utdype hvordan API er sikret.	H	B

1.6.6 KRYPTERING

Det er i Helse Sør-Øst etablert en felles regional kryptoinstruks, beskrevet i «SSA-T Bilag 1 - Vedlegg 5a – Fellesregional kryptopolicy».

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T6.44	All datatrafikk mellom endepunktene bør være kryptert på applikasjonslaget iht. Helse Sør-Øst kryptoinstruks.	H	

T6.45	Kryptering av evt. trafikk over https bør benytte TLS v1.2, eksempelvis ved bruk av webserver for webapplikasjon eller webservices for integrasjonsformål. Merknad: Kundens ønsker av sikkerhetsmessige grunner ikke å tillate bruk av eldre protokoller (SSL eller eldre versjoner av TLS). Leverandøren bes begrunne evt. avvik.	H	B
T6.46	Ved evt. bruk av sertifikater, bør disse utstedes av Kundens tjenesteleverandør	H	

1.6.7 ANTIVIRUS OG ANTIMALWARE

Kundens gjeldende standard software for anti-malware er i dag Trend på Windows servere og Microsoft System Center Endpoint Protection (SCEP) på Windows-basert arbeidsflate.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T6.47	Applikasjoner installert på Kundens arbeidsflate skal støtte Kundens standard programvare for antivirus/antimalware.	O	
T6.48	Antivirus-/antimalwarescanning på Kundens arbeidsflater bør skje uten behov for ekskludering av filer eller mapper. Leverandøren bes utdype evt. avvik.	H	B
T6.49	Serverapplikasjoner installert på Kundens servere bør støtte Kundens standard programvare for antivirus/antimalware. Leverandøren bes utdype evt. avvik.	H	B
T6.50	Antivirus-/antimalwarescanning på Kundens servere bør skje uten behov for ekskludering av filer eller mapper. Leverandøren bes utdype evt. avvik.	H	B

1.7 IKT-relatert drift og forvaltning

Kundens tjenesteleverandør er drift- og forvaltningsansvarlig for Kundens tekniske plattform. Kundens tjenesteleverandør vil også ha hovedansvaret for teknisk drift og forvaltning av systemet som skal etableres på plattformen, men vil utføre dette arbeidet i tett samarbeid med Kunden og Leverandøren. Kundens tjenesteleverandør vil normalt ha 1. og 2. linje brukerstøtte på systemet.

Det er derfor viktig at Leverandøren forholder seg til både tekniske løsninger og rutiner som inngår i tjenesteleverandørens drift- og forvaltning av systemet.

1.7.1 GENERELLE KRAV TIL IKT-RELATERT DRIFT OG FORVALTNING

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T7.1	Systemet bør kun benytte 3. parts komponenter som ikke allerede er End of Life/End of Support eller som blir det i løpet av innføringsperioden. Merknad: Eventuelle komponenter som allerede er utenfor End Of Life/End Of Support, eller som vil bli det i løpet av innføringsperioden, bør spesifiseres, begrunnes og planlagte oppgraderinger synliggjøres i systemets roadmap for videre utvikling.	H	B
T7.2	Leverandøren bes utdype hvilke muligheter og begrensninger som ligger i systemets administrative funksjoner og moduler som kan benyttes av Kunden og Kundens tjenesteleverandør ved drift- og forvaltning av systemet.	H	B
T7.3	Leverandøren bes utdype evt. medfølgende eller 3. parts verktøy og støttesystemer som må eller bør benyttes for å støtte opp om teknisk drift og applikasjonsforvaltning.	H	B
T7.4	For installasjon, feilsøk, feilretting, vedlikehold, oppdateringer, oppgraderinger og brukerstøtte som skjer gjennom bruk av fjernaksess, skal det inngås Databehandleravtale og signeres taushetserklæring mellom Leverandør og Kundens tjenesteleverandør.	O	
T7.5	All bruk av underleverandører som direkte eller indirekte gis tilgang til systemet installert i Kundens tekniske plattform skal opplyses om og godkjennes av Kunden og Kundens tjenesteleverandør. Merknad: Leverandøren bes utdype: • evt. bruk underleverandører • til hvilket formål underleverandører benyttes • underleverandørens navn og hvor de er lokalisert	O	B

T7.6	Leverandøren skal forholde seg til og etterleve Kundens og Kundens tjenesteleverandørs endringsregime¹ for produksjonssatte løsninger. Merknad: Leverandør kan ikke planlegge og/eller iverksette endringer som kolliderer med planlagte endringer i Kundens infrastruktur. Dette krever gjensidig varsling av planlagte endringer mellom aktørenes tjenesteanvarlige personell. Ved eventuell konflikt er det Kundens og Kundens tjenesteleverandørs endringsregime som har prioritet.	O	
------	--	---	--

1.7.2 FJERNAKSESS OG EKSTERNE TILGANGER

Helse Sør-Øst har etablert en standardisert portal for fjernaksess for leverandører gjennom bruk av løsninger fra F5 BigIP og Citrix, og tilbys i dag av Kundens tjenesteleverandør for alle eksterne leverandører. Den benevnes «Leverandør desktop» og skal benyttes for all leverandørspesifikk drift og forvaltning der det ikke forutsettes personlig oppmøte i Kundens lokaler.

For å kunne bruke denne løsningen må Leverandør kunne benytte F5 BigIP web-plugin for SSL VPN og Citrix Receiver web-klient på sine PC-er. Leverandøren får da tilgang til en aksesserver hos Kundens tjenesteleverandør, hvor nødvendig programvare og/eller fjernstyringsprogram mot server eller teknisk utstyr gjøres tilgjengelig. All bruk av fjernaksessløsningen skal knyttes til personlige, entydig identifiserte brukere hos Leverandøren.

Kunden har i tillegg etablert en standardisert énveis eller toveis «filsluse» for kontrollert og sikker overføring av godkjente data mellom Kunden og Leverandør.

Det er etablert en regional VPN-Gateway for terminering av VPN-forbindelser mellom Leverandører og Kunden. Dette er den foretrukne metoden for *utgående* datatransport over VPN fra Kunden sitt nettverk, dersom automatisk eller regelmessig teknisk overvåkingsdata kreves overført til Leverandøren. All planlagt bruk av *utgående* dataoverføring over VPN må først risikovurderes og godkjennes før dette kan etableres. Alle endringer i konfigurasjon og data som overføres skal godkjennes av Kunden og dokumenteres i Databehandleravtalen før endringer kan gjennomføres.

¹ Med endringsregime menes de reglene som gjelder for planlegging, varsling og utførelse av endringer på infrastruktur hos Kunden, inklusive sentrale datasentre i Helse Sør-Øst. Dette omfatter all fysisk infrastruktur som strøm/kjøling, fysisk kabling, nettverk, nettverkstjenester, serverplattformer (fysiske og virtuelle) som det tilbudte systemet er avhengig av for å kunne produsere de avtalte tjenestene. All endring som leverandør ønsker å utføre må være avtalt og omforent med Kundens tjenesteleverandør da dennes arbeid alltid har forrang ved kollisjon på tidsluker. Dette for å unngå at planlagt vedlikehold kan feile under utføring med tilhørende driftsforstyrrelser og fare for pasientsikkerheten.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T7.7	Leverandøren skal benytte Kundens standard fjernaksesløsning ved brukerstøtte, feilsøk, feilrettelse, vedlikehold og oppdateringer av systemet. Merknad: I dag gir Leverandør desktop tilgang til aksesserver med installerte forvaltnings-/driftsverktøy som UltraVNC, WinSCP, RDP og SSH. Bruk av egendefinert intern leverandøraksess med løsninger som 3G/4G/5G-eller ADSL-modem, samt programvare som TeamViewer, LogMeln etc. tillates ikke.	O	
T7.8	Leverandøren skal ved bruk av Kundens fjernaksesløsning benytte personlige, entydig identifiserte brukere. Merknad: Med entydig identifisert bruker menes: • For Norske borgere: ○ Fødselsnummer • For utenlandske borgere som oppholder seg i og arbeider hos leverandøren i Norge: ○ D-nummer • For utenlandske borgere som skal benytte fjernaksesløsningen, ett av følgende: ○ Nasjonal ID i eget hjemland for EU-borgere ○ Passnummer ○ Social security number ○ Tax identification number ○ Eller annen form for nasjonal identifikasjon som entydig identifiserer bruker	O	
T7.9	Dersom det er nødvendig med tilgang til programvare utover standard installerte forvaltnings-/driftsverktøy som UltraVNC, WinSCP, RDP og SSH, bør leverandøren utdype og begrunne slikt behov.	H	B
T7.10	Systemet bør ha et klart skille på innhold i tekniske logger og andre logger som kan inneholde personopplysninger, inkludert kodede.	H	B

	Leverandøren bese utdype hvorvidt leverandørtilgang til produksjonslogger kun omfatter tekniske data, og om det er risiko for innsyn i personopplysninger, inkludert kodede, ved slik tilgang.		
T7.11	Leverandør bør gjennomføre teknisk support uten behov for å få <i>automatisk</i> utlevert/overført tekniske logger og eksempelmateriale via overføring av logger til Leverandøren, eksempelvis via VPN. Leverandøren skal beskrive evt. behov og begrunne disse.	H	B
T7.12	Systemet bør støtte bruk av « <i>service tilgang</i> » eller « <i>service modus</i> », hvor evt. personopplysninger om pasient skjules/anonymiseres ifm. leverandørbistand.	L	B

1.7.3 OPPDATERING, OPPGRADERING OG VEDLIKEHOLD

Det er av sikkerhetsmessige og driftsmessige årsaker viktig for Kunden og Kundens tjenesteleverandør at systemet fortløpende kan vedlikeholdes og oppdateres, samt at systemet ikke legger begrensninger på hvordan vedlikehold av underliggende komponenter og tjenester i Kundens tekniske plattform kan foregå.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T7.13	Systemet bør ha mekanismer for å redusere nedetid ved oppdateringer, oppgraderinger og vedlikehold. Leverandøren bes utdype slike mekanismer, og beskrive hvilke former for endringer på systemet som typisk medfører nedetid, samt estimere normal nedetid for de enkelte endringene.	H	B
T7.14	Systemet bør ha støtte for å kunne ta ned og oppgradere enkeltvis noder i et «high availability»-design, uten at dette i nevneverdig grad påvirker systemets tilgjengelighet. Leverandøren bes utdype slik støtte, og evt. konsekvenser ved oppdatering av enkeltvis noder.	H	B
T7.15	Systemet bør håndtere automatisk utrulling av sikkerhetspatcher, servicepacks og andre oppdateringer fra leverandør av <i>operativsystem</i> på PC-klienter og servere. Leverandøren bes utdype evt. avvik fra dette, samt evt. begrensninger som skyldes sertifiseringer, produsentens egenpålagte begrensninger eller systemets tekniske begrensninger.	H	B

T7.16	Systemet bør håndtere automatisk utrulling av sikkerhetspatcher, servicepacks og andre oppdateringer fra leverandør av <i>databaseplattform og andre 3. parts komponenter</i> som benyttes i systemet.	H	B
T7.17	Korrigerings av korrupte verdier i databasen bør normalt kunne skje mens systemet er i bruk.	M	
T7.18	Leverandør bør utdype bistand som gis ved gjenoppbygging fra backup.	H	B

1.7.4 DRIFTSTEKNISK OVERVÅKING OG LOGGING

Kundens tjenesteleverandør har etablert sentraliserte løsninger for overvåking av underliggende komponenter og tjenester i Kundens tekniske plattform.

Det er sentralt og viktig for både Kunden og Kundens tjenesteleverandør at systemer etablert i Kundens tekniske plattform kan tilby drifts- og forvaltningsrelatert teknisk loggfunksjonalitet på flere nivåer.

Dette kan eksempelvis være ved feilsituasjoner eller varsler tilknyttet hardware, operativsystem, tjenester i systemet, feilhendelser og andre varsler som kan overvåkes og ageres på, for å bidra til at feilsituasjoner som påvirker brukere av systemet eller systemets funksjonalitet i størst mulig grad kan unngås. I tillegg er det nødvendig å ha god tilgang til teknisk loggdata for å i etterkant av feilsituasjoner kunne fremskaffe informasjon relevant for å avdekke feilårsak, slik at tiltak som forhindrer at feilen gjenoppstår kan implementeres.

Kundens tjenesteleverandør har etablert et sentralt loggmottak for håndtering av relevante system- og sikkerhetslogger fra Kundens systemer. Sentralt loggmottak er basert på Splunk. Det foretrekkes at systemspesifikke parametere som skal overvåkes av Kundens tjenesteleverandør lagres i operativsystemets hendelseslogg (eventlogg), hvor det kan fanges opp og overføres til Splunk.

Krav nr.	Krav	Kravets viktighet (O/H/M/L)	Beskriv (B)
T7.19	Systemet bør tilby mekanismer og/eller grensesnitt for driftsteknisk overvåking og feilrapportering. Leverandøren bes utdype eventuelle muligheter og begrensninger for integrasjon med eksisterende overvåkingssystem hos Kundens tjenesteleverandør. Merknad:	H	B

	Dette inkluderer eventuelle standarder og protokoller som kan benyttes, samt hvordan eventuell varsling til systemansvarlig kan gjennomføres, dersom dette skjer som en funksjon i systemet.		
T7.20	Leverandøren bør utdype hvilke komponenter og tjenester i systemet som kan og anbefales overvåkes. Merknad: Dette kan eksempelvis inkludere: • Prosesser • Servicer • Køer • Integrasjoner • Filområder • Logger • Porter	H	B
T7.21	Systemets logger bør på en tydelig måte skille <i>generell informasjon</i> fra <i>konkrete feil</i> som krever oppfølging og korrigering ved hendelser i systemet, slik at feilsituasjoner kan fanges opp. Leverandøren bes beskrive hvordan systemet skiller informasjon og feil i systemets logger, samt hvordan dette kategoriseres mht. type varsel/feil, alvorlighetsgrad o.l.	H	B
T7.22	Leverandøren bes utdype hva slags informasjon som logges ved hendelser i systemet, eksempelvis feilkode, feilårsak, hendelseskategori, komponent/modul som har forårsaket hendelse, dato/tidspunkt o.a. relevant informasjon som er nødvendig for å effektivt gjøre feilsøk og feilrettelser.	H	B
T7.23	Systemet bør ha funksjonalitet for å endre detaljnivået på logging. Leverandøren bes utdype evt. støtte for dette, og hvorvidt det er støtte for at dette kan gjøres av systemets drifts- og forvaltningsansvarlige, eksempelvis gjennom et brukergrensesnitt eller annen konfigurasjon.	H	B
T7.24	Alle systemfeil bør logges i operativsystemets standard hendelseslogg (eventlogg) med en forståelig feilkode og feilmelding.	H	