HELSE SØR-ØST

Prosjekt:

Nytt sykehus i Drammen

Tittel:

Bilag D17

IKT-teknisk rammeverk og informasjonssikkerhet

02	For implementering	02.03.20	CHN	ENE	ARH
01	For implementering	04.11.19	CHN	ENE	ARH
Rev.	Beskrivelse	Rev. Dato	Utarbeidet	Kontroll	Godkjent

Kontraktor/leverandørs logo:	Bygg nr:	Etasje nr.:	Systemgr.:	Antall sider:
				Side 1 av 7

Prosjekt:	Kontrakt nr:	Fag:	Dok.type:	Løpenr:	Rev.nr.:	Status:
NSD	**0000**	**Z**	**SP**	**0078**	**01**	**G**

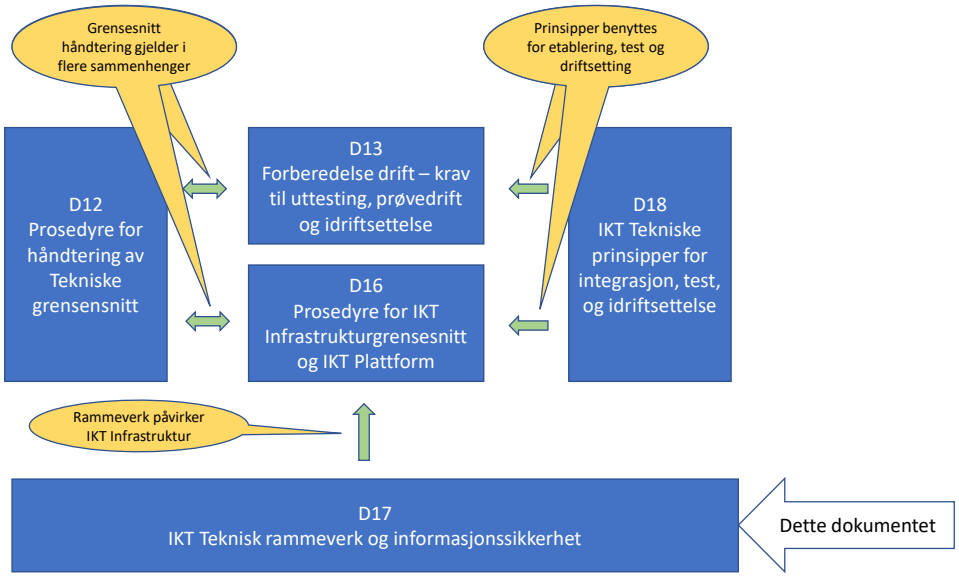
Innholdsfortegnelse

1 Innledning

Bilaget presenterer en sammenfatning av teknologistandarder og tilhørende krav og føringer som forutsettes benyttet ved leveranser til NSD.

1.1 Formål

Bilaget skal benyttes av Entreprenør/Leverandørene og valgt tilnærming skal avstemmes mellom Entreprenør/Leverandør og Byggherre for å sikre at teknologistandarder og tilhørende krav og føringer etableres slik at krav til forvaltning, drift, vedlikehold og informasjonssikkerhet ivaretas. Figuren nedenfor beskriver sammenhengen mellom omkringliggende bilag vha. gule merknader.



Figur 1 Sammenhengen mellom ulike bilag

Bilaget inngår i alle forespørsler som blir sendt ut for NSD. På grunn av at teknologien er preget av hurtige endringer vil det kunne bli revidert jevnlig (typisk 1 gang per år). Dokumentet vil derfor være et dynamisk dokument.

IKT Infrastruktur (Kablingssystemet og datanettet) ved NSD er bærer av alle tjenester over IP på lokasjonen.

Andre utstyr- og teknologistandarder enn de som er nevnt i dokumentet kan ikke tas i bruk uten at det på forhånd er avklart og avtalt, ref. «Bilag D16 Prosedyre for håndtering av IKT Infrastruktur grensesnitt og IKT Plattform».

Dokumentet er utarbeidet med bakgrunn i de IKT-teknologi-standardene som er i bruk i Helse Sør-Øst pr. august 2019, og som forventes å ville være gjeldende standarder ved oppstart av NSD 2025. Det er forventet en utvikling i disse standardene frem til 2024.

Føringene i dette dokumentet gjelder alle løsninger som benytter felles IKT infrastruktur og IKT Plattform slik som Medisinsk Teknisk Utstyr (MTU), ByggTeknisk Utstyr (BTU), Administrativt Teknisk Utstyr (ATU), og IKT infrastruktur.

Det er lagt ved fem vedlegg:

- Vedlegg A Kravspesifikasjon IKT Tjenester og Informasjonssikkerhet BTU (Byggteknisk og administrativt teknisk utstyr)
- Vedlegg B Kravspesifikasjon IKT Tjenester og Informasjonssikkerhet MTU (Medisinsk Teknisk Utstyr)
- Vedlegg C – Kundens tekniske plattform
- Vedlegg D – Kundens tekniske plattform – Integrasjon
- Vedlegg E – Kundens tekniske plattform – Identitet- og tilgangstyring

Som minimum skal det leveres en IKT System/løsningsskisse. Vedleggene skal for øvrig besvares iht. instruks i angitt i Bilag C. Vedleggene vil bli benyttet i forbindelse med kartleggingen av IKT Infrastruktur og IKT plattform kartlagt som en del av prosedyren beskrevet i Bilag D16 Prosedyre for IKT infrastrukturgrensesnitt og IKT-Plattform.

Vedlegg C, D og E er lagt ved som informasjon om det IKT tekniske rammeverket i Helse Sør-Øst.

1.2 Målgruppe

Dokumentet er rettet mot Byggherren, Entreprenørene/Leverandørens løsningsansvarlige, IKT Infrastrukturkoordinator (ref. Bilag D16), Helseforetakets tjenesteleverandør (Sykehuspartner HF) og Helseforetaket (VV).

1.3 Begrep

I dette bilaget benyttes Helseforetaket som betegnelse for VV. Innholdet i bilaget er utarbeidet av Helseforetaket sammen med Sykehuspartner som et generelt dokument som benyttes ved alle system og utstyrsanskaffelser.

Videre benyttes Leverandør som betegnelse på Totalentreprenør, Entreprenør eller Leverandør.

Forklaring til Forkortelser og øvrige begrep er gitt i kapittel **Error! Reference source not found.**

2 Føringer for Systemløsninger

Ved leveranser av systemløsninger skal Leverandøren fremlegge et overordnet løsningsdesign med systemdokumentasjon, som på en tydelig og oversiktlig måte viser de relevante hovedkomponenter, overordnet dataflyt og kommunikasjonsgrensesnitt internt og eksternt for løsningen. Dette gjelder uavhengig av om løsningen består av:

- For Medisinsk Teknisk Utstyr (MTU): Kun programvare, kun enkeltstående MTU eller sammensatte systemløsninger med server(e), MTU(er) og klient-PCer for MTU-styring/overvåking og datahøsting fra MTU.
- For byggnær IKT (BTU): Kun programvare, kun frittstående utstyrsenheter eller sammensatte tekniske anlegg/system med server(e) og klient-PCer for styring, regulering og overvåkning
- For administrativt teknisk utstyr (ATU): Kun programvare, frittstående utstyrsenheter eller sammensatte løsninger med server(e) og klient-PCer

Det er derfor meget viktig at dokumentasjonen gjenspeiler løsningen, uansett størrelse og omfang, eksempelvis med en tilhørende illustrasjon, slik den er tenkt etablert. Dokumentasjonen skal inkludere alle enkeltkomponenter i systemet (instrumenter, klient-PC, servere, lagring, nettverk, konvertere m.m.). Dette inkluderer også detaljert dataflyt mellom løsningens enkeltkomponenter, med eksisterende tjenesteelementer i Helseforetakets nettverk samt eventuelle behov for ekstern dataaksess.

Merknad: *Med «relevant» menes dataflyt som benytter eller traverserer datanettverk og derfor kan kreve at brannveggregler må tilrettelegges for at den tilbudte løsningen skal fungere i Helseforetakets IKT-infrastruktur.*

Hvis en løsning er basert på bruk av eksterne tjenester hos Entreprenør/Leverandør og/eller Produsent (skytjenester, web-portal eller tilsvarende), skal tilbudet også inneholde relevant løsningsdesign og Risiko og sårbarhetsanalyse (ROS) for leverandørens benyttede infrastruktur til produksjon av de nødvendige tjenestene som tilbudt løsning er avhengig av.

Det henvises til vedlegg A/B i dette bilaget – Kravspesifikasjon – IKT-tjenester og informasjonssikkerhet for MTU/BTU, hvor leverandøren skal som en del av tilbudet besvare relevante deler av vedlegget.

2.1 Overvåking og endrings-/oppdateringsregime

Sykehuspartner overvåker alle elementer som inngår i deres drifts- og forvaltningsregime. Leverandørløsninger og deres underliggende komponenter skal derfor tilby mekanismer og/eller grensesnitt for overvåking for å minimere forekomster av feil og nedetid.

For å sikre høyest mulig tjenestekvalitet er det en målsetning i Helseforetaket at det bare bør benyttes komponenter som har gyldige, produsentspesifikke vedlikeholdsavtaler gjennom hele kontraktsperioden. Helseforetaket har derfor preferanse for leverandører som i best mulig grad kan tilby en dokumentert og forpliktende roadmap for oppgradering og videreutvikling av sine løsninger.

I de tilfellene der en leverandør også skal ivareta drift- og forvaltningsoppgaver, så skal leverandøren både forholde seg til og etterleve det til enhver tids gjeldende endringsregime[1] for produksjonssatte løsninger.

[1] *Med endringsregime menes de reglene som gjelder for planlegging, varsling og utførelse av endringer på infrastruktur hos Helseforetaket og/eller Helseforetakets tjenesteleverandør, inklusive sentrale datasentre i Helse Sør-Øst. Dette omfatter all fysisk infrastruktur som strøm/kjøling, fysisk kabling, nettverk, nettverkstjenester,*

2.2 Redundans

Helseforetaket skal ha mulighet for å bestille tjenester med høyest mulig oppetid på sine lokasjoner. Dette stiller krav til redundans helt opp på systemnivå. Med dette menes også redundans på eksempelvis server- og nettverksløsninger som inngår i tjenesten eller som tjenesten er avhengig av for å levere med avtalt tjenestekvalitet og/eller oppetid. Viktige elementer for å ivareta nødvendig redundans på tjenester er:

- En systemløsning bør ha mulighet for intern lastbalansering
- En systemløsning bør ha mulighet for ekstern lastbalansert nettverkstilkobling
- En systemløsning bør ha mulighet for intern redundans (failover)
- En systemløsning bør ha mulighet for redundant ekstern nettverkstilkobling (failover)

Et kompenserende tiltak for manglende redundans er evne til lokal overlevelse for en tjeneste ved bortfall av andre tjenester som eksempelvis nettverksforbindelse. En tjeneste må da kunne mellomlagre resultater inntil nettverksforbindelse er operativ igjen og datasynkronisering kan gjennomføres.

3 Basis IKT Infrastruktur

3.1 Utstyrsmontasje

Entreprenørens utstyr skal plasseres i skap i ulike kommunikasjonsrom. Skapene vil være 80 x 100 x 240 cm i KR og 80 x 120 x 240 cm i HKR/SHKR Skapene vil bli utstyr med 19'' ramme. Utstyret kan enten rackmonteres eller plasseres på hyller. Skap vil bli utstyrt med 2 PDUer som er forsynt fra to ulike strømkurser (UPS).

For utstyr som skal plasseres utenfor kommunikasjonsrom må det særskilt angis behov for strøm (eventuelt UPS) og kjøling.

3.2 Kabling

Utstyr som inneholder intern kabling, skal grensesnitt mot både logisk og fysisk nettverk beskrives. Utstyr skal tilknyttes datanettet vha.:

- RJ45 Cat 6A/ea
- Fiber LC Single modus
- WLAN – 802.11a, g, n, ac el.

4 Vedlegg

Vedlegg A - Kravspesifikasjon IKT tjenester og informasjonssikkerhet for BTU

Vedlegg B - Kravspesifikasjon IKT tjenester og informasjonssikkerhet for MTU

---

serverplattformer (fysiske og virtuelle) som den tilbudte løsningen er avhengig av for å kunne produsere de avtalte tjenestene. All endring som leverandør ønsker å utføre må være avtalt og omforent med Helseforetakets 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.

Vedlegg C – Kundens tekniske plattform

Vedlegg D – Kundens tekniske plattform – Integrasjon

Vedlegg E – Kundens tekniske plattform – Identitet- og tilgangsstyring

Kravspesifikasjon

IKT- tjenester og Informasjonssikkerhet for BTU

Innholdsfortegnelse

VIKTIG INFORMASJON

Formål

Dette dokumentet skal brukes til evaluering/vurdering av Leverandørens tilbudte løsning innenfor områdene IKT og Informasjonssikkerhet. I tillegg skal den i størst mulig grad kartlegge løsningens grunnleggende funksjonalitet og egnethet i Oppdragsgivers IKT-infrastruktur i forkant av et endelig kundedesign. Dette minimerer risiko for **utilsiktede etableringskostnader, økt implementeringstid eller at ønsket og tilbudt funksjonalitet må reduseres** for å møte Oppdragsgivers pålagte krav til Informasjonssikkerhet og personvern. Dokumentet skal også medvirke til at Oppdragsgiver oppfyller lovreglene i personvernforordningen (GDPR).

Forklaring til skjema for kravspesifikasjon IKT-tjenester og Informasjonssikkerhet for BTU

Krav: (A/B/C/D)		
A	Obligatorisk	Obligatorisk krav som skal oppfylles. Manglende evne til å etterleve kravet medfører at tilbudt løsning skal avvises.
B	«Bør»-krav	Leverandørens oppfyllelse av kravet gis enten en egnethetsvurdering ved vurdering eller en score ved en faktisk tilbudsevaluering.
C	Dokumentasjon	Kan kombineres med A/B/D-angivelse av kravtype. Understreker da at Oppdragsgiver forventer et utdypende svar. Hvis C står alene er dette kun et informasjonspunkt som ikke krever besvarelse eller evalueres
D	Høy	Kombineres med B for å signalisere at kravet er svært viktig, men ikke obligatorisk. Leverandørens evne til å oppfylle kravet gis en score med en tilhørende **høy vekting** ved tilbudsevaluering.

Oppdragsgivers bestemmelser gjeldende Leverandørens besvarelse

Svar:
Alle angitte[1] krav uansett kravtype **skal** besvares av Leverandør. Svaret fastsetter i hvilken grad leverandøren kan tilfredsstille kravets ordlyd og innhold.

Kravene besvares med Ja (**J**), Nei (**N**) eller Utdyping (**U**). Svarkategori «**U**» dekker alle alternativer som ikke kan besvares med et entydig Ja/Nei. For krav som besvares med «**U**», skal det som ikke kan dekkes fra Leverandørens side særskilt utdypes. Dette for å sikre Oppdragsgivers forståelse av besvarelsen på kravene så man kan vurdere og/eller evaluere på korrekt grunnlag.

*Da denne kravspesifikasjonen er generisk og skal brukes til et stort spenn av BTU-anskaffelser, vil det være krav som ikke naturlig inngår i enhver anskaffelse. Kombinasjonen Nei som svar (**N**) og Ikke aktuelt (**I/A**) som utdyping kan benyttes av Oppdragsgiver for **å forhåndsmarkere** at krav ikke vurderes som aktuelle for en anskaffelse.*

***OBS:** Kombinasjonen Nei (**N**) og Ikke aktuelt (**I/A**) **kan også benyttes der leverandøren selv** anser kravet som uaktuelt ut fra innholdet i den tilbudte løsningen, med en skriftlig forklaring på hvorfor kravet ikke anses som aktuelt.*

Det **skal ikke** henvises til, eller benyttes, manualer, brosjyrer, reklamemateriell o.l. som ***rene besvarelser*** på kravpunkter. For å sikre korrekt sammenligningsgrunnlag når ulike leverandører skal evalueres/vurderes må en besvarelse på et krav derfor inneholde nødvendige kopier av den relevante teksten. Denne presiseringen er spesielt viktig for obligatoriske krav (A-krav) da disse kravene skal forplikte Leverandøren, og skape trygghet hos Oppdragsgiver på at det tilbys en løsning som er mulig å etablere i Oppdragiver sin infrastruktur.

[1] Med "angitte» menes kravpunkter som Oppdragsgiver ikke har markert som uaktuelle fra sin side med kombinasjonen: «N» og «I/A»

Dette sikrer at en påfølgende designprosess ikke medfører utilsiktede etableringskostnader og lang implementeringstid, samt at etterspurt og tilbudt funksjonalitet kan tas i bruk i henhold til Helse Sør-Øst sine krav til Informasjonssikkerhet og personvern.

Leverandøren er uansett ansvarlig for at deres designforslag og løsningselementer dokumenteres på en komplett og helhetlig måte for å dekke alle besvarelser og spesifikasjoner som inngår i denne kravspesifikasjonen. Dette betyr at Leverandøren også er ansvarlig for å beskrive alle nødvendige løsningselementer for å få en komplett og fungerende løsning, selv om slike elementer ikke er eksplisitt beskrevet av Oppdragsgiver i kravspesifikasjonen. Oppdragsgiver forventer derfor at Leverandøren gjør oppmerksom på eventuelle relevante aspekter ved løsningen som ikke er dekket av Oppdragsgivers kravspesifikasjon.

Utdyping av besvarelser:
Her **kan** Leverandør utfylle sin besvarelse av type «J» eller «N» der det oppleves som påkrevd for å sikre forståelsen. Det er imidlertid ikke anledning til å omskrive et «J» til «N», eller omvendt, gjennom en slik utdyping. Entydig besvarelse av typen «**J/N»** uten nevneverdig utdyping forventes kun på enkle krav. Ved besvarelsen «**J/N»** på enkle krav anser Oppdragsgiver at Leverandøren har **akseptert/benektet** alle vilkår i kravet 100%, og evaluerer ut fra dette. Ved besvarelse «**U**» **skal** Leverandøren beskrive hva som ikke kan tilfredsstilles i Oppdragsgivers krav. Leverandøren skal beskrive i hvilken grad et avvik er permanent, eller om dette kan løses med en designendring/alternativt løsningsforslag. Dersom innfrielse av kravet krever endring i Leverandørens tilbudte løsning, skal Leverandøren angi tidsperspektiv for når kravet vil være innfridd. Hvis alternative løsningsforslag endrer prisbildet har skal det utdypes med priskonsekvens som behandles i henhold til beskrivelsen i avsnitt under for **«Pris:»**. Leverandøren skal her dokumentere den faktiske priskonsekvens for Oppdragsgiver.

Pris:
Svares ut med «**J**» eller «**N**». Leverandør angir her om det eksisterer et eget, dedikert, priselement for at leverandøren skal kunne oppfylles sine forpliktelser i henhold til svar på kravet. Det forventes da at tilhørende priselement er angitt i Prisbilaget – med henvisning til korresponderende kravelement. Hvis svaret er «N» forutsetter Oppdragsgiver at kravet er oppfylt ved kontraktsinngåelse, eller innen et avtalefestet tidspunkt i kontraktsperioden, uten at det utløser noen ekstra kostnad for Oppdragsgiver.

Vurdering av kvalitet på dokumentasjon

Oppdragsgiver ønsker at alle besvarelser på mer enn ca. 100 ord, eller som inneholder figurer, flyttes ut i Leverandørens svarbilag med henvisning for å gi økt lesbarhet og sikre en helhetlig forståelse og korrekt vurdering/evaluering. Slike besvarelser skal referere til kravnummer og utarbeides spesifikt for det kravet det gjelder.

Oppdragsgiver vil vurdere kvaliteten på den tilsendte dokumentasjon og besvarelsene i kravspesifikasjonen samlet sett. Dette kan gis en samlet poengsum ved en evaluering.

1 OVERORDNET SYSTEMBESKRIVELSE

Denne seksjonen omhandler krav til Leverandørens overordnede beskrivelse av den samlede leveransen.

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Kravtekst:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Overordnede dokumentasjonskrav				
1.1	Leverandøren skal fremlegge et overordnet løsningsdesign og systemdokumentasjon som på en tydelig og oversiktlig måte viser de relevante hovedkomponenter, overordnet dataflyt og kommunikasjonsgrensesnitt internt og eksternt for løsningen. Dette kravet gjelder uavhengig av om løsningen består av kun programvare, kun enkeltstående BTU eller sammensatte systemløsninger med server(e), skytjenester, BTU(er) og klient-PCer for BTU-styring/overvåking og datahøsting fra BTU. **Merknad**: Det er meget viktig at dokumentasjonen gjenspeiler løsningen, uansett størrelse og omfang, eksempelvis med en tilhørende illustrasjon, slik den er tenkt etablert hos Oppdragsgiver. Dokumentasjonen skal inkludere alle enkeltkomponenter i systemet (Feltkomponenter, undersentraler, klient-PC, servere, lagring, nettverk, konvertere m.m.).	**AC**			
1.2	Leverandøren skal fremlegge en detaljert oversikt, basert på utarbeidet dokumentasjon fra kravpunkt 1.1, over all relevant nettverksmessig dataflyt slik den er planlagt etablert hos Oppdragsgiver. Dette inkluderer detaljert dataflyt mellom løsningens enkeltkomponenter, med eksisterende tjenesteelementer i Oppdragsgivers nettverk, samt eventuell datautveksling med skytjenester eller andre eksterne tjenester. **Merknad:** Med «relevant» menes dataflyt som benytter eller traverserer Oppdragsgivers datanettverk og derfor kan kreve at brannveggregler må tilrettelegges for at den tilbudte løsningen skal fungere i Oppdragsgivers IKT-infrastruktur.	**AC**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Kravtekst:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
1.3	Hvis den tilbudte løsningen er basert på bruk av eksterne tjenester hos Leverandør og/eller Produsent (skytjenester, web-portal eller tilsvarende), bør tilbudet også inneholde relevant løsningsdesign og ROS for leverandørens benyttede infrastruktur til produksjon av de nødvendige tjenestene som tilbudt løsning er avhengig av. **Merknad**: Hvis det ikke benyttes eksterne tjenester, så besvares punktet med «N» og «I/A»	**BD**			
1.4	Det IKT-relaterte bistandsomfanget i Leverandørens tilbud skal inkludere all leverandørbistand som tilbys for ferdigstillelse av endelig løsningsdesign i Oppdragsgivers infrastruktur, installasjon, konfigurasjon, testing og produksjonssetting, samt utarbeidelse av nødvendig system- og driftsdokumentasjon.	**A**			
	Overvåking og endrings-/oppdateringsregime				
1.5	Den tilbudte løsningen eller komponenter i løsningen bør tilby mekanismer og/eller grensesnitt for overvåking for å minimere forekomster av feil og nedetid. **Merknad:** Eventuelle føringer og begrensninger rundt mulighet for integrasjon med eksisterende overvåkingssystem hos Oppdragsgiver, samt hvordan eventuell varsling til systemansvarlig kan gjennomføres, utdypes i Leverandørens besvarelse.	**BC**			
1.6	Leverandøren skal forholde seg til, og etterleve, Oppdragsgivers og Oppdragsgivers driftsleverandørs endringsregime[2] for produksjonssatte løsninger. **Merknad:** Leverandør kan ikke planlegge og/eller iverksette endringer som kolliderer med planlagte endringer i Oppdragsgivers infrastruktur. Dette krever gjensidig varsling av planlagte endringer mellom aktørenes tjenesteansvarlige personell. Ved eventuell konflikt er det Oppdragsgivers og Oppdragsgivers driftsleverandørs endringsregime som har prioritet.	**A**			

[2] Med endringsregime menes de reglene som gjelder for planlegging, varsling og utførelse av endringer på infrastruktur hos Oppdragsgiver, inklusive sentrale datasentre i Helse Sør-Øst. Dette omfatter all fysisk infrastruktur som strøm/kjøling, fysisk kabling, nettverk, nettverkstjenester, serverplattformer (fysiske og virtuelle) som den tilbudte løsningen er avhengig av for å kunne produsere de avtalte tjenestene. All endring som leverandør ønsker å utføre må være avtalt og omforent med Oppdragsgivers

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Kravtekst:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
1.7	Den tilbudte løsningen bør bare benytte komponenter som har gyldige, produsentspesifikke vedlikeholdsavtaler gjennom hele kontraktsperioden. **Merknad:** Eventuelle komponenter som allerede er utenfor produsentspesifikk vedlikeholdsavtale (End Of Life/End Of Support) eller som vil bli det i løpet av avtaletiden skal spesifiseres.	**BCD**			
1.8	Leverandøren bør tilby en dokumentert og forpliktende roadmap for oppgradering og videreutvikling av den tilbudte løsningen.	**BC**			
1.9	Leverandøren bør sikre at produsentens anbefalinger følges ved oppdatering av programvare, konfigurasjon, kodeverk, eller andre registre for å ivareta den tilhørende endringsprosessen på tilbudt løsning. **Merknad:** Det er viktig at det utdypes hvordan løsningen skal vedlikeholdes (gjennom integrasjon, brukergrensesnitt, oppdatering av database, eller lignende), samt overordnede kommunikasjonstekniske krav for å gjennomføre slik oppdatering på den tilbudte løsningen.	**BCD**			
	Redundanskrav				
	Med redundanskrav menes krav knyttet til redundans på eksempelvis server- og nettverksløsninger som den tilbudte løsningen inkluderer eller er avhengig av for å levere med avtalt tjenestekvalitet og/eller oppetid. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».	**C**			
1.11	En tilbudt systemløsning bør ha mulighet for intern lastbalansering	**B**			
1.12	En tilbudt systemløsning bør ha mulighet for ekstern lastbalansert nettverkstilkobling	**B**			

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.

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Kravtekst:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
1.13	En tilbudt systemløsning bør ha mulighet for intern redundans (failover)	**B**			
1.14	Den tilbudte løsningen bør ha mulighet for redundant ekstern nettverkstilkobling (failover)	**B**			

2 LISENSHÅNDTERING

Denne seksjonen skal beskrive hvilke lisensieringsmekanismer den tilbudte løsningen eventuelt benytter. For Oppdragsgiver og Oppdragsgivers 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.

OUS Kravspesifikasjon			**Leverandørens besvarelse**		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	De etterfølgende kravpunktene besvares kun hvis det tilbudte systemet inneholder lisensieringsmekanismer. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».				
2.1	Eventuelle lisensieringsmekanismer bør være basert på sentral lisens og sentralisert lisensforvaltning.	**BD**			
2.2	Leverandøren bør beskrive systemets 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 • bruk av lisensservere utenfor Oppdragsgivers infrastruktur, inklusiv teknisk løsning og eventuelle konsekvenser for bruk av løsningen dersom slik kommunikasjon ikke kan etableres av Oppdragsgiver	**BCD**			
2.3	Leverandøren bør på en oversiktlig måte utdype eventuelle begrensninger i bruk av systemet som er en konsekvens av lisensieringsmekanismen. Eksempler på viktige utdypingsområder er begrensninger av teknisk eller funksjonell art: • i antall brukere • i antall tilkoblede enheter	**BCD**			

OUS Kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	• lagringsvolumer • ved overskridelser av lisensgrenser				
2.4	Systemet bør ha tydelige og veldokumenterte rutiner for forvaltning og vedlikehold av lisens/sertifikat. Eksempler på viktige utdypingsområder er: • Hvordan fornyes evt. tidsavgrenset lisens/sertifikat • Hvordan aktiveres/deaktiveres tidsbegrenset lisens/sertifikat • Hvordan utføres versjonering av lisens/sertifikat	**BCD**			
2.5	Systemet bør ved midlertidig bortfall av lisensieringsmekanisme fungere uten at dette påvirker bruken av systemet. Leverandøren bes beskrive evt. konsekvenser for bruk av systemet ved bortfall av lisensieringsmekanisme.	**BC**			

3 NETTVERK

Sykehuspartner er i dag Oppdragsgiver sin leverandør av nettverksinfrastruktur med tilhørende nettverkskomponenter som svitsjer, rutere, brannmurer o.l. BTU-tjenester vil normalt etableres logisk adskilt fra andre tjenester og Oppdragsgivers administrative nett forøvrig. Ved behov åpnes det for tilgang mot annet BTU og integrasjoner mot andre tjenester i Oppdragsgivers nettverk, som f.eks. fagsystemer.

Ved bruk av konvertering mellom Ethernet og andre interfaceteknologier, må dette dokumenteres detaljert for å sikre at de tilbudte løsningene er teknologikompatible og kan benyttes i et kundespesifikt design. Oppdragsgiver sitt nettverk er klargjort for IPv6, men dette er ikke tatt i bruk ennå. Gjeldende protokoll er IPv4. Oppdragsgivers nettverk kan benytte NAC (802.1x) som stenger ned LAN-tilgang for ukjente eller inaktive enheter. Oppdragsgiver har også standardisert brannmursregulering mellom nettverkssoner hvor inaktive TCP-sesjoner termineres av sikkerhetsgrunner etter 60 minutter. Dette legger krav på det utstyret som skal kobles opp i Oppdragsgiver sitt nettverk, og Leverandør må ta hensyn til dette i utarbeidelsen av tilbudt løsning.

Oppdragsgiver tillater heller ikke at Klient-PC-er eller servere som inngår i den tilbudte løsningen kan settes opp som mulige gateway-maskiner (dvs. skal ikke ha to eller flere nettverkskort) mellom ***et internt BTU-nett og Oppdragsgiver sitt datanettverk***. I slike tilfeller skal leveransen inkludere en godkjent ruter/brannmur som **separerer** den tilbudte løsningen fra Oppdragsgiver sitt datanettverk.

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
3.1	Den tilbudte løsningen bør benytte standard teknologier/protokoller for kablet ekstern datatrafikk, for eksempel RJ45/Ethernet, USB, Firewire. **Merknad:** Utdyp hvilke standard teknologier/protokoller som benyttes, samt eventuelle avvik i form av leverandørspesifikke begrensninger eller tekniske krav.	**BC**			
3.2	Den tilbudte løsningen bør benytte IPv4 dersom den tilbudte løsningen har ekstern datautveksling over Ethernet med Oppdragsgivers systemer.	**BD**			
3.3	Den tilbudte løsningen bør støtte fremtidig bruk av IPv6 dersom den tilbudte løsningen har ekstern datautveksling over Ethernet med Oppdragsgivers systemer.	**B**			
3.4	Den tilbudte løsningen bør konfigureres med Oppdragsgivers egne IP-adresseserier dersom den tilbudte løsningen har ekstern datautveksling over Ethernet/IP med Oppdragsgivers systemer. **Merknad:** Dersom den tilbudte løsningen ikke støtter bruk av Oppdragsgiver sine IP-adresseserier kan leveransen inkludere en dokumentert og leverandørdriftet ruter/gateway/brannmur som utfører "NAT/PAT" adresseoversetting mellom Oppdragsgivers adresseserie og Leverandørens adresseserie. Dokumentasjonen skal inneholde nødvendige IP-adresser og TCP-/UDP-portnumre for tjenester som tilgjengeliggjøres. Denne ruter/gateway/brannmur-løsningen skal alltid risikovurderes og godkjennes før en tilkobling til Oppdragsgivers nettverk kan utføres.	**BC**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
3.5	Den tilbudte løsningen bør benytte oppdragsgivers nettverk uten å stille leverandørspesifikke begrensninger eller tekniske krav. **Merknad:** Utdyp eventuelle begrensninger/krav i forhold til CE eller andre sertifiseringer, eksempelvis føringer på: • må den samlede, tilbudte løsningen stå i ett og samme VLAN, eller kan den segmenteres i flere VLAN? • Tilgjengelig nettverkskapasitet (båndbredde), latency, pakkestørrelse eller pakketap i nettverket, bruk av brannvegg etc.	**BCD**			
3.6	Den tilbudte løsningen bør håndtere brudd i nettverkskommunikasjon mellom de ulike delene av løsningen, slik at den medisinske funksjonaliteten opprettholdes mens systemet gjenoppretter sin nettverkskommunikasjon uten behov for manuelle brukeroperasjoner. **Merknad:** Se avsnitt 2 i ledetekst for kapittel 3. Sikkerhetsmekanismer i Oppdragsgivers nettverk lukker inaktive nettforbindelser på lag2 & lag3 (MAC&IP). Leverandørens eventuelle krav og konsekvenser gitt av disse mekanismene må dokumenteres med tanke på design og tilhørende sikkerhetsgodkjenning.	**BC**			
3.7	Hvis den tilbudte løsningen implementerer dataoverføring basert på trådløs kommunikasjon bør det benyttes standard teknologier/protokoller, eksempelvis WLAN, Bluetooth, GSM/LTE, annen RF. **Merknad:** Utdyp eventuelle avvik gitt av leverandørspesifikke begrensninger eller tekniske krav, eksempelvis manglende support for sikkerhetsmekanismer, forholdsregler knyttet opp mot frekvenser, signalstyrker, mulighet for interferens etc.	**BC**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
3.8	Leverandørens tilbudte løsningsdesign bør unngå bruk av komponenter med to eller flere nettverkskort som skal kobles opp mot Oppdragsgiver sitt datanettverk. **Merknad:** Ved bruk av flere nettverkskort *kan* etablerte sikkerhetsfunksjoner i Oppdragsgiver sitt datanettverk brytes eller omgås. Dette er en uønsket situasjon for Oppdragsgiver. Unntak kan gis for påkrevde og dokumenterte funksjonelle behov, eksempelvis for instrumenter direktekoblet til klient-PC med krysset kabel.	**BD**			
3.9	Leverandørens eventuelle lokale instrumentnett og Oppdragsgiver sitt datanettverk bør kun sammenkobles med en, for Oppdragsgiver/Tjenesteleverandør, godkjent ruter/brannmur som separerer den tilbudte løsningen fra Oppdragsgiver sitt datanettverk ref. punkt 3.8.	**BD**			
3.10	Datatrafikk fra den tilbudte løsningen bør benytte IP-Unicast ved traversering av Oppdragsgivers brannvegger. **Merknad**: Oppdragsgivers nettverk støtter i dag *ikke* bruk av IP-Multicast gjennom ruter/VRF.	**BD**			
3.11	Leverandørens tilbudte løsning bør være kompatibel med bruk av IEEE 802.1x (Network Access Control). **Merknad**: For alt utstyr som skal tilkobles og gis tilgang til Oppdragsgivers nettverk, registreres utstyret som hovedregel med godkjent MAC-adresse for tilgangskontroll.	**BD**			
3.12	Leverandørens tilbudte løsning bør fungere uavhengig av WINS eller Windows hosts-fil.	**BC**			
3.13	Leverandørens tilbudte løsning bør benytte DNS navneoppslag fremfor IP-adresser.	**B**			
3.14	Leverandørens tilbudte løsning bør fungere uten krav til jording via nettverk (STP).	**B**			

4 MASKINVARE

Sykehuspartner er i dag Oppdragsgiver sin foretrukne leverandør av maskinvare som klient-PCer, servere (fysiske og virtuelle), lagringsløsninger, skrivere, skannere og strekkodelesere.

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
4.1	Leverandørens tilbudte serverløsning bør implementeres på virtuell serverplattform som kan leveres av Oppdragsgivers tjenesteleverandør. **Merknad**: Utdyp eventuelle leverandørspesifikke krav til virtuelle servere, for eksempel: RAM, CPU, OS (HOST/GUEST), disk, RAID, tilkoblingskort o.l.	**BC**			
4.2	Leverandørens tilbudte løsning bør implementeres på klient-PCer som kan leveres av Oppdragsgivers tjenesteleverandør. **Merknad**: Utdyp eventuelle leverandørspesifikke krav til klient-PCer, for eksempel: RAM, CPU, OS, disk, RAID, tilkoblingskort o.l.	**BC**			
4.3	Dersom påkrevet som en del av løsningen, bør Leverandørens tilbudte løsning implementeres på bærbare enheter (eks. bærbar PC, mobiltelefon, nettbrett, personsøker eller lignende) som kan leveres av Oppdragsgivers tjenesteleverandør, forutsatt at utstyret oppfyller Leverandørens eventuelle krav til medisinsk godkjenning av slikt utstyr. **Merknad**: Utdyp også eventuelle andre leverandørspesifikke krav til slike bærbare enheter (bærbar PC, mobiltelefon, nettbrett, personsøker eller lignende), for eksempel: RAM, CPU, OS, disk, o.l.	**BC**			
4.4	Leverandørens tilbudte løsning bør benytte lagringsløsninger som kan leveres av Oppdragsgivers tjenesteleverandør. **Merknad**: Utdyp eventuelle leverandørspesifikke krav til benyttet lagringsløsning dokumenteres, for eksempel: lagringsprinsipper, filsystem, diskvolum, lese/skrivehastighet, o.l.	**BC**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
4.5	Foretrukket løsning for utskrift i Oppdragsgiver er basert på sentraliserte nettverksskrivere med «Pull Print» (sikker print). Leverandørens tilbudte løsning bør benytte sentraliserte nettverksskrivere som kan leveres av Oppdragsgivers tjenesteleverandør for utskriftsløsninger. **Merknad**: Utdyp eventuelle leverandørspesifikke krav til lokale skrivere (lokalprinter eller egne nettverksskrivere), for eksempel: RAM, CPU, disk, utskriftshastighet, tilkoblingskort o.l. Bruk av «Pull Print» **forutsetter** at Leverandørens tilbudte løsning kan integreres i tilstrekkelig grad mot, alternativt innmeldes i, Oppdragsgivers AD for nødvendig brukerhåndtering.	**BC**			
4.6	Leverandørens tilbudte løsning bør benytte periferiutstyr som skanner, strekkodeleser o.l. som kan leveres av Oppdragsgivers tjenesteleverandør, forutsatt at utstyret oppfyller nødvendige krav til medisinsk godkjenning **Merknad**: Utdyp eventuelle andre leverandørspesifikke krav til slikt periferiutstyr (supporterte merker, modeller, strekkodeformater, utskriftsformat etc.).	**BC**			

5 OPERATIVSYSTEM OG PROGRAMVARE

Dette kapittelet omhandler operativsystem, samt tilhørende programvare og komponenter i den tilbudte løsningen. For øyeblikket er standard operativsystem Windows 7 64/32-bit på klient-PCer og Windows Server 2019 på servere. Det er pågående aktivitet for å oppdatere standard operativsystem for klient-PCer til Windows 10. I tillegg supporterer Tjenesteleverandør nyere versjoner av RedHat Linux. Gjennom Tjenesteleverandørens avtaleverk er målsetningen at alle løsninger skal støtte en såkalt «N/(N-1)»-livssyklus for alle de systemkomponenter som inngår i en løsning. Dette betyr at det benyttes siste, eller nest siste, versjon av alle HW/SW-komponenter.

Gjeldene standard software hos Oppdragsgiver for anti-malware er i dag Trend på Windows servere og Microsoft System Center Endpoint Protection (SCEP) på Windows-klienter. For databaser er gjeldende standard Microsoft SQL Server 2019 og Oracle Enterprise R12.

Enkelte av helseforetakene i HSØ benytter RES One Suite fra RES (res.com) for styring og sikring av klientarbeidsflater på Windows 7-plattformen, inkludert tilgjengeliggjøring av klientapplikasjoner med alle tilhørende plugins/3.partskomponenter. Distribusjon av applikasjoner gjøres hovedsakelig via APP-V, alternativt via SCCM. RES One Suite har i ettertid byttet navn til Ivanti Workspace Control (ivanti.com), og vil fremover benyttes på Windows 10 klient-PCer.

Kravene i dette kapitlet omhandler også nødvendige systemkomponenter som Oppdragsgiver må tilgjengeliggjøre for at den tilbudte løsningen skal fungere som avtalt. Slike systemkomponenter bør kunne hentes fra gjeldende produkt- og tjenestekatalog fra Tjenesteleverandør. Eksempelvis kan Tjenesteleverandør utstede nødvendige sertifikater til bruk for HTTPS/SSL i serversammenheng etter nærmere avtale.

OUS kravspesifikasjon			**Leverandørens besvarelse**		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
5.1	Leverandørspesifikk *klient-PC* som inngår i den tilbudte løsningen bør benytte OS i henhold til Tjenesteleverandør sitt regime for livssyklus. **Merknad:** Med *klient-PC* menes PC som benyttes enten til styring/overvåking av et direktetilkoblet BTU eller PC med installert programvare for prosessering av BTU-genererte data.	**B**			
5.2	Leverandørspesifikk *server* med Windows- eller Linux-OS som inngår i den tilbudte løsningen bør benytte OS i henhold til Tjenesteleverandør sitt regime for livssyklus.	**B**			
5.3	Leverandør bør utdype alle relevante krav for påkrevde komponenter (OS, klientapplikasjoner, serverprogramvare o.l.) som ikke leveres som en del av den tilbudte løsningen, eller avviker fra Tjenesteleverandørens standarder. Eksempelvis: Nettleser, webserver, databaser, Java, Flash, Silverlight, MS Office, .NET Framework, C++ Redistributable, MDAC o.l. og eventuelle spesifikke versjoner av disse.	**BCD**			
5.4	Hvis tilbudt løsning benytter lokal webserver bør det være implementert mekanismer som sikrer server og innhold mot uautorisert tilgang. **Merknad**: Utdyp hvilke sikkerhetsmekanismer som er aktivert, samt hvilke mekanismer som kan aktiveres i tillegg.	**BC**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
5.5	Funksjonaliteten i den tilbudte løsningen bør ikke til enhver tid være avhengig av kommunikasjon med webtjenester utenfor Oppdragsgivers nettverk, eksempelvis hos Leverandør/Produsent eller direkte mot internett. **Merknad:** Oppdragsgiver krever kontroll og sporbarhet på all ekstern kommunikasjon. Dokumentasjon på hvorfor slik kommunikasjon er påkrevd, og i hvilken grad løsningen ivaretar Oppdragsgiver sine sikkerhetskrav til ekstern kommunikasjon må fremlegges ved tidspunkt for tilbud. Endelig bruk av slik kommunikasjon krever en gjennomført risikovurdering som gir en godkjenning.	**BD**			
5.6	Leverandør bør gjennomføre relevant «herding» av OS og benyttede applikasjoner på Leverandørspesifikt utstyr som inngår i den tilbudte løsningen.	**B**			
5.7	Den tilbudte løsningen bør benytte kryptering på applikasjonsnivå ved datautveksling med andre systemer.	**B**			
5.8	Leverandørspesifikke *klient-PCer* bør benytte Oppdragsgiver sin standard-programvare for anti-malware. **Merknad:** Leverandør må utdype eventuelle behov for avvik fra Oppdragsgivers standard pga sertifiseringer som, CE etc.	**B**			
5.9	Oppdatering av definisjonsfiler for kjent malware på *klient-PCer* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell oppdatering av definisjonsfiler.	**BC**			
5.10	Malwarescanning på Leverandørspesifikke *klient-PCer* bør skje uten behov for ekskludering av mapper.	**B**			
5.11	Malwarescanning på *klient-PCer* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell malwarescanning.	**BC**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
5.12	Leverandørspesifikke *servere* bør benytte Oppdragsgiver sin standard-programvare for anti-malware. **Merknad:** Leverandør må utdype eventuelle behov for avvik fra Oppdragsgivers standard pga sertifiseringer som, CE etc.	**B**			
5.13	Oppdatering av malwaresignaturer på *servere* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell oppdatering av malwaresignaturer, inklusiv eventuelle eksterne tilganger nødvendig.	**BC**			
5.14	Malwarescanning på Leverandørspesifikke *servere* bør skje uten behov for ekskludering av mapper.	**B**			
5.15	Malwarescanning på *servere* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell malwarescanning.	**BC**			
5.16	Utrulling av sikkerhetspatcher og servicepacks fra OS-leverandør bør utføres uten produsentspesifikke krav eller begrensninger. **Merknad:** Begrensninger som skyldes sertifiseringer eller produsentens egenpålagte begrensninger må dokumenteres. Det er også viktig for Oppdragsgiver at det utdypes hvorvidt nødvendige sikkerhetspatcher og servicepacks kan installeres automatisk, eller om det kreves at automatisk oppdatering må forsinkes eller settes opp til å installeres først ved neste omstart av klient-PCer eller server.	**BCD**			
5.17	Leverandørspesifikke *klient-PCer* som inngår i den tilbudte løsningen bør ha mulighet for å meldes inn i Oppdragsgiver sitt AD	**B**			
5.18	AD-innmeldte *klient-PCer* som skal benyttes i den tilbudte løsningen bør benytte diskkryptering (eks. MS Bitlocker). **Merknad**: Utdyp eventuelle begrensninger knyttet til bruk av diskkryptering.	**B**			
5.19	Leverandørspesifikke *servere* som inngår i den tilbudte løsningen bør ha mulighet for å meldes inn i Oppdragsgiver sitt AD	**B**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
5.20	Den tilbudte løsningens tilhørende klientapplikasjon(er) bør være kompatibel med Oppdragsgivers bruk av RES One/Ivanti Workspace Control og App-V samt SCCM. **Merknad**: Utdyp eventuelle forutsetninger og begrensninger i den tilbudte løsningen.	**BD**			
5.21	Bruk og/eller vedlikehold av installert programvare på den tilbudte løsningen (utover selve OS-installasjonen) på *klient -PC* bør skje uten bruk av lokal administratorrettighet på operativsystemet.	**B**			
5.22	Bruk og/eller vedlikehold av installert programvare på den tilbudte løsningen (utover selve OS-installasjonen) på s*erver* bør skje uten bruk av lokal administratorrettighet på operativsystemet.	**B**			

6 INFORMASJONSSIKKERHET OG TILGANGSSTYRING

Oppdragsgiver stiller strenge krav til sikkerhet i forbindelse med etablering og drift av BTU. BTU skal beskyttes mot eksterne trusler, sykehusnettet og annet BTU. Sykehusnettet skal på sin side beskyttes mot BTU. Helseforetakene i Helse Sør-Øst har i fellesskap vedtatt et regionalt ledelsessystem for informasjonssikkerhet basert på ISO 27001. Ledelsessystemet er gjeldene for samtlige helseforetak i regionen. Kravene i dette kapitellet er utledet av krav fra ledelsessystemet.

- Regionalt ledelsessystem for informasjonssikkerhet - https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet

Oppdragsgiver plikter å oppfylle lovreglene i personvernforordningen (GDPR). Det stilles derfor krav til at tilbudt løsning skal tilfredsstille krav i Personvernforordningen 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

Oppdragsgiver 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

Eksempler på føringer gitt av personvernforordningens krav til innebygd personvern og «Normen» er:

- Oppdragsgiver prefererer BTU-løsninger der det benyttes individuell brukeridenter med sikret rollebasert tilgangsstyring
- Oppdragsgiver har som målsetning å standardisere på å bruke Oppdragsgiver sin Integrasjonstjeneste basert på Helse Sør-Øst sin Regionale Integrasjonsplattform for alle former for integrasjon mellom nettverks- og sikkerhetssoner. Dette gjelder både socket-basert kommunikasjon og filflytt.
- For løsninger som krever bruk av eksternt lagringsmedium for manuell overføring av datafiler retter Oppdragsgiver seg etter retningslinjene fra regionalt styringssystem for informasjonssikkerhet, ref. regional kryptopolicy punkt 4.3: «Kryptering under lagring av data». I dag benyttes krypterte lagringsenheter fra IronKey hos Oppdragsgiver.

OUS kravspesifikasjon			**Leverandørens besvarelse**		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
6.1	Den tilbudte løsningen bør ikke ha vesentlige avvik i forhold til lover og regler for informasjons- og pasientsikkerhet. **Merknad:** Leverandøren skal utdype alle relevante avvik. Dette for å sikre at alle risikomomenter kan vurderes og ivareta Oppdragsgiver sitt pålegg om å etterleve Direktoratet for eHelse sin «Norm for informasjonssikkerhet» («Normen»).	**BCD**			
6.2	Leverandøren bør, så snart produsenten har implementert funksjonalitet og forbedringer som støtter GDPR og teknisk IT-sikkerhet, tilby Oppdragsgiver programvareoppdatering, programvarelisens og installasjon uten ekstra kostnad for Oppdragsgiver.	**B**			
6.3	Den tilbudte løsningen bør benytte sentralisert fillagring og/eller database. **Merknad**: Utdyp evt. hvilken databaseplattform som støttes, samt hvorvidt løsningen baseres på lokale tjenester og om de i så fall kan erstattes med sentraliserte serverbaserte tjenester.	**BC**			
6.4	Den tilbudte løsningen bør benytte individuelle brukeridenter både på OS- og applikasjonsnivå.	**B**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
6.5	Individuell brukerautentisering bør gjøres mot grupper definert i Active Directory via LDAP, fortrinnsvis LDAP over SSL (LDAPS). **Merknad**: Utdyp hvorvidt både LDAP eller LDAPS støttes. Leverandøren bør også utdype hvorvidt en LDAP/LDAPS integrasjon kun gjør en synk av brukere fra AD til lokal brukerdatabase, eller om autentisering skjer direkte mot AD.	**BC**			
6.6	Alle former for lokale brukerprofiler (brukernavn/passord) lagret i lokale brukerdatabaser, konfigurasjonsfiler e.l. som benyttes til klient-, database- eller applikasjonspålogging bør sikres med standardiserte mekanismer for tilgangskontroll og kryptering. Se regional kryptopolicy. **Merknad**: Utdyp hvordan krav til tilgangskontroll og kryptering er tenkt ivaretatt i den tilbudte løsningen.	**BCD**			
6.7	Den tilbudte løsningen bør støtte attributtbasert tilgangsstyring (ABAC) og regelbasert tilgangsstyring (PBAC). Sentrale utdypingselementer er: • hvilke rolletyper som eksisterer – eksempelvis adminbruker, superbruker, Lese&Skrive-bruker, Lese-bruker e.l.? • er roller endelig fastsatt eller kan roller (om)konfigureres i løsningen? • Hvilke sikringsmekanismer som er etablert for å unngå endring i rollebasert tilgangsstyring er bygget inn i den tilbudte løsningen?	**BCD**			
6.8	Den tilbudte løsningen bør ha funksjonalitet for begrensning av tilgang til personopplysninger for enkeltbrukere og grupper av brukere.	**BCD**			
6.9	Hvis den tilbudte løsningen inneholder standard- eller systembrukere, så bør det bare benyttes unike passord før tilkobling til Oppdragsgivers IKT-infrastruktur. **Merknad:** Det skal ikke benyttes hardkodede passord, passord som kan hentes direkte fra brukermanualer eller annen form for tilgjengelig dokumentasjon.	**BD**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
6.10	Ved eventuelt behov for ekstern transport, eller ved lagring av personopplysninger på minnepinne, ekstern harddisk, filsystem eller i database, bør den tilbudte løsningen støtte kryptering av data. **Merknad:** Beskrive evt. støtte og krypteringsstandard/-styrke som benyttes.	**BC**			
6.11	Hvis den tilbudte løsningen benytter eksterne webløsninger/-portaler for analyse, rapportering eller drift og forvaltning bør løsningen oppnå en «Overall Rating» på rapport generert hos Qualys SSL[3] Labs på minst «A». **Merknad**: Hvis det ikke benyttes eksterne webløsninger/portaler besvares spørsmålet med «N» og «I/A»	**B**			
6.12	Ved eventuelt behov for ekstern transport, eller ved lagring av personopplysninger på minnepinne, ekstern harddisk, filsystem eller i database, bør den tilbudte løsningen støtte kryptering av data. Merknad: Beskrive evt. støtte og krypteringsstandard/-styrke som benyttes	**BCD**			

7 BACKUP

Oppdragsgiver ønsker å etterleve prinsippene om Data Lifecycle Management hvor Backup/Restore er en sentral komponent for å ivareta datasikkerhet og integritet. Målsetningen er å benytte sentralisert Backup/Restore i størst mulig grad.

[3] Qualys SSL Server Test er en åpen verifisering av kryptering. https://www.ssllabs.com/

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Kravpunktene under fylles ut hvis den tilbudte løsningen skal benytte egenprodusert eller sentrale backuptjenester over Oppdragsgivers nettverk eller hvis dette er funksjonalitet som kan tas i bruk i løpet av kontraktsperioden. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».				
7.1	Backup av disk, inklusive programvare, konfigurasjon, kalibrering o.l., på server og klient-PC bør kjøres mot eksisterende sentraliserte og automatiserte backuptjenester hos Oppdragsgiver. **Merknad:** Det forutsettes da at backupklient kan installeres på den tilbudte løsningen og eventuelle leverandørspesifikke brannmurer åpnes for tilgang fra Oppdragsgiver sin backupløsning.	**B**			
7.2	Backup av databaser bør kjøres mot eksisterende sentraliserte og automatiserte backuptjenester hos Oppdragsgiver. **Merknad:** Det forutsettes da at backupklient kan installeres på den tilbudte løsningen og eventuelle leverandørspesifikke brannmurer åpnes for tilgang fra Oppdragsgiver sin backupløsning.	**B**			
7.3	Databaser som inngår i den tilbudte løsningen bør ha støtte for både full og inkrementell backup (gjennom f.eks. loggbackup/loggshipping) av databaser	**B**			
7.4	Leverandørbistand ifm. gjenoppretting fra backup bør enten være inkludert, eller spesifisert i prisbilaget for serviceavtale	**B**			

8 INTEGRASJONER

Hvis den tilbudte løsningen benytter datautveksling med sentrale kundesystemer, bør dette skje med bruk av åpne/de Facto standarder for slik datautveksling.

Helse Sør-Øst har en Regional Integrasjonsplattform for informasjonsdeling. Denne plattformen inneholder standardiserte integrasjonsløsninger for utsendelser og kvitteringer av for eksempel alarmer via sms og epost.

Hensikten med de etterfølgende kravene er å identifisere om produktet støtter den Regional Integrasjonsplattformen som er etablert i Helse Sør-Øst. Dette gjelder viktige elementer som loggfunksjonalitet, sikkerhetsmekanismer, benyttede kommunikasjonsprotokoller, meldingsformater og semantikk. Alle disse faktorene vil påvirke tidsforbruk og kostnad ved en etablering av integrasjon.

OUS kravspesifikasjon			**Leverandørens besvarelse**		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Kravpunktene under fylles ut hvis den tilbudte løsningen skal utveksle data med andre sentrale servertjenester i Oppdragsgivers nettverk eller dette er funksjonalitet som kan tas i bruk i løpet av kontraktsperioden. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».	**C**			
8.1	Den tilbudte løsningen bør inkludere API eller tekniske løsninger for å tilpasses en Integrasjonsløsning, eksempelvis: Webservice, fileksport/import, WCF, BacNet, Modbus, KNX,OPC DA, OPC UA mm	**B**			
8.2	Den tilbudte løsningen bør benytte API på en sikker måte for integrasjon og informasjonsutveksling. Utdyp hvilke sikkerhetsmekanismer den tilbudte løsningen kan supportere ved bruk av API.	**BC**			
8.3	All utveksling av informasjon bør etableres med internasjonale standarder. **Merknad:** Eksempler på slike standdarder er BacNet, Modbus, KNX, mm	**BC**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
8.4	Utveksling av informasjon bør gjøres uten å være underlagt leverandørspesifikke krav eller begrensninger i forhold til hvilke protokoller som kan benyttes. Eksempler på protokoller som kan benyttes hos Oppdragsgiver er: TCP/UDP, FTP/FTPS/SFTP, SMB, SMTP, SOAP (HTTP/HTTPS), REST (HTTP/HTTPS), MSMQ, OPC DA, OPC UA	**BC**			
8.5	Den tilbudte løsningen bør benytte Oppdragsgivers standardiserte integrasjonstjeneste uten at det stilles leverandørspesifikke krav eller begrensninger for semantikk i de benyttede standardiserte meldingsformater, inkludert hvilke formatversjoner, som kan benyttes.. **Merknad**: Utdyp slike eventuelle krav/begrensninger, inkludert eventuelle implementeringsavvik i benyttet standard.	**BC**			
8.6	Den tilbudte løsningen bør ha mulighet for logging av meldingsflyt og meldingskvitteringer som gjør det mulig å oppdage meldinger som ikke kommer frem eller blir kvittert med negativ kvittering, men også vite hvilke meldinger som har kommet korrekt fram til mottakeren **Merknad**: Utdyp hvilken loggfunksjonalitet den tilbudte løsningen eventuelt har og hvordan dette kan understøtte behov for meldingsdokumentasjon, eventuell feilsøking og analysering av avvik på sendte og mottatte data i grensesnittet mellom BTU og andre aktører.	**BCD**			
8.7	Den tilbudte løsningen bør leveres med dokumentasjon som beskriver leverandørens grensesnitt for integrasjoner; herunder hvilke tags som benyttes og hvilket format tag har.	**BCD**			

9 IKT-RELATERT DRIFT OG FORVALTNING

Helse Sør-Øst tilbyr i dag en standard fjernaksessløsning for alle eksterne utstyrsleverandører. Den benevnes «Leverandøraksess» og skal benyttes for all leverandørspesifikk drift og forvaltning som ikke skjer med fysisk oppmøte i Oppdragsgivers 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. Bruk av egendefinert intern leverandøraksess med løsninger som 4G-modem, samt programvare som TeamViewer, LogMeIn og liknende tillates ikke i Helse Sør-Øst.

Leverandøren får tilgang til en aksesserver hos Oppdragsgiver, hvor nødvendig programvare og/eller fjernstyringsprogram mot BTU klient/-server gjøres tilgjengelig. Alle brukere av fjernaksessløsningen skal knyttes opp mot personlige, identifiserte brukere hos Leverandøren.

Enkelte helseforetak har i tillegg standardisert «filsluse» for kontrollert og sikker overføring av godkjente data mellom Oppdragsgiver og Leverandør.

Det er etablert en regional VPN-Gateway for terminering av VPN-forbindelser mellom Leverandører og Oppdragsgiver. Dette er den foretrukne metoden for utgående datatransport over VPN fra Oppdragsgiver sitt nettverk. All planlagt bruk av dataoverføring over VPN må først risikovurderes og godkjennes før dette kan etableres. Leverandøren skal gi en forpliktende forsikring/dokumentasjon på benyttede dataformater, at VPN-bruken kun omfatter tekniske data, og at det ikke er risiko for overføring av personopplysninger, inkludert krypterte. Alle ønskede endringer i formatoppsett og bruk av VPN skal godkjennes av Oppdragsgiver i forkant før endringer kan gjennomføres.

Det er sentralt og viktig for både Oppdragsgiver og Oppdragsgivers Tjenesteleverandør at utstyr i Oppdragsgiver sitt nettverk kan tilby loggingsfunksjonalitet på flere nivåer (hardware/OS/sikkerhet/brukeraktivitet m.m.). Alle logger som den tilbudte løsningen genererer der innholdet må klassifiseres som virksomhets- eller personsensitivt, må sikres i henhold krav om informasjonssikkerhet (ref. «Normen»). Dette må gjøres for å sikre at essensiell logginformasjon ikke kan leses, endres eller slettes av uautorisert personell.

Hvis Oppdragsgiver er omforent med Leverandør om at drift og forvaltning krever bruk av Leverandøraksess, så må det som hovedregel inngås Databehandleravtale med Oppdragsgivers tjenesteleverandør.

OUS kravspesifikasjon			**Leverandørens besvarelse**		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Kravpunktene under er relatert til bruk av Oppdragsgivers fjernaksessløsning og fylles kun ut hvis denne planlegges benyttet ved produksjonssetting eller dette er funksjonalitet som kan tas i bruk i løpet av kontraktsperioden.	**C**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
9.1	Leverandøren bør benytte Oppdragsgiver sin tilbudte fjernaksessløsning for drift og forvaltning av den tilbudte løsningen. **Merknad**: Utdyp hvilket behov Leverandør har for tilgjengeliggjort programvare i Oppdragsgiver sin standard fjernaksessløsning for å supportere den tilbudte løsningen via fjerntilgang. I dag gir Leverandøraksess tilgang til aksesserver med installerte forvaltnings-/driftsverktøy som *UltraVNC, WinSCP, RDP og SSH*.	**BCD**			
9.2	Logger som leverandør har tilgang til for drift og forvaltning bør kun inneholde teknisk informasjon, og ikke personopplysninger. **Merknad**: Utdyp hvorvidt leverandørtilgang til produksjonslogger kun omfatter tekniske data, og om det er risiko for innsyn i personopplysninger, inkludert kodede.	**BCD**			
9.3	Leverandør bør gjennomføre teknisk support uten behov for å få utlevert/overført tekniske logger og eksempelmateriale via VPN.	**BCD**			
9.4	Noen løsninger har støtte for at personopplysninger skjules/anonymiseres når leverandør har tilgang til systemet ifm. vedlikehold, såkalt «service tilgang» eller «service user modus». Leverandøren bes beskrive evt. støtte for dette i den tilbudte løsningen.	**BD**			
9.5	Den tilbudte løsningen bør logge og lagre tekniske hendelser eller feil. **Merknad**: Utdyp hvorvidt det benyttes logging til Windows EventLog, loggfiler, databaser, SNMP traps etc.	**BD**			
9.6	Den tilbudte løsningen bør logge og lagre brukeroperasjoner (brukeraktivitet inklusiv uautorisert, eller forsøk på uautorisert, bruk). **Merknad**: Utdyp hvorvidt det benyttes logging til Windows EventLog, loggfiler, databaser, SNMP traps etc.	**BD**			
9.7	Den tilbudte løsningen bør gi autoriserte brukere hos oppdragsgiver tilgang til logger gjennom et standardisert brukergrensesnitt. **Merknad**: Utdyp hvordan logger tilgjengeliggjøres.	**BC**			

OUS kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
9.8	For de ulike typene loggdata som lagres i den tilbudte løsningen, inkludert lesing, endring og sletting av logger, bør gjeldende offentlige informasjonssikkerhetskrav ivaretas. **Merknad**: Utdyp hvordan sikkerhetskrav knyttet til konfidensialitet, integritet og tilgjengelighet ivaretas for de ulike typene loggdata som lagres i den tilbudte løsningen.	**BCD**			

Forkortelser og begreper

Begreper	Beskrivelse
4G-modem	USB-modem benyttet til 4G GSM-kommunikasjon
ABAC	Attribute Based Access Control – også benevnt policy based access control (PBAC), definerer et tilgangskontrollregime hvor rettigheter tildeles brukeren gjennom bruk av regelsett ved å kombinere ulike attributer.
AD	Active Directory – Microsofts katalogtjeneste for autentisering og autorisering av brukere innenfor et Windows domene
API	Application Programming Interface, grensesnitt for integrasjon
BAS	Bygningsautomatikksystem (se SD)
BTU	Byggteknisk utstyr
BacNet	Datakommunikasjonsprotokoll benyttet i BAS
Bluetooth	Teknologi for trådløs kommunikasjon
CPU	Central Processing Unit - prosessor i f.eks. klient-PC/server
CSV	CSV - Comma Separated Values - tekstfil inneholdende data separert med komma eller annet tegn for separasjon av felt
Dali	BAS protokoll typrisk benyttet for lysstyring
DNS	Domain Name System - Systemtjeneste for å oversette mellom maskinnavn og IP-adresse
Ekstern datautveksling	Med ekstern datautveksling menes all datatrafikk som benytter Oppdragsgivers infrastruktur. Dette kan eksempelvis være kommunikasjon med sentraliserte tjenester for autentisering og autorisering av brukere, fillagring, database, eller integrasjon med andre tjenester.
Endringsregime	Med endringsregime menes de reglene som gjelder for planlegging, varsling og utførelse av endringer på Oppdragsgivers infrastruktur, inklusive sentrale datasentre i Helse Sør-Øst. Dette omfatter all fysisk infrastruktur som strøm/kjøling, fysisk kabling, nettverk, nettverkstjenester, serverplattformer (fysiske og virtuelle) som den tilbudte løsningen er avhengig av for å kunne produsere de avtalte tjenestene. All endring som leverandør ønsker å utføre må være avtalt og omforent med Oppdragsgivers 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.
Fagsystem	Et større, overbyggende IT-system som ivaretar bred funksjonell støtte innenfor et avgrenset funksjonsområde, eller på tvers av flere funksjonsområder. Eksempelvis LIMS, EPJ eller elektronisk kurve.
F5 BigIP VPN	Standard leverandøraksess via VPN leveres gjennom produktet BigIP fra F5
Firewire	IEEE1394, teknologi for kablet høyhastighets dataoverføring
FTP/FTPS	File Transfer Protocol/File Transfer Protocol m/SSL-kryptering, protokoller for filoverføring
GDPR	General Data Protection Regulation (EU) 2016/679, EUs personvernforordning
GSM	Global System for Mobile Communications - standard for telekommunikasjon for mobiler
Herding	Herding av klient PC, server o.a. IKT-komponenter er en metode som benyttes for å øke komponentens sikkerhet ved å fjerne og begrense mulige sikkerhetsmessige sårbarheter som kan utnyttes av en angriper. Dette kan eksempelvis gjøres gjennom å sikre at operativsystem, programvare og 3.programvarekomponenter er sikkerhetspatchet eller oppdatert til siste versjon, bruk av antivirus/anti-malware, bruk av lokal brannmur, samt stoppe/sperre tjenester som ikke benyttes.
HOST	Windows hosts fil, statisk tekstfil med oversikt over maskinnavn og korresponderende IP-adresse
HTTP/ HTTPS	HyperText Transfer Protocol/HyperText Transfer Protocol Secure - standarder for kommunikasjon for World Wide Web
IEEE 802.1x	Standard for autentisering av maskinvare tilkoblet nettverk. Må ikke forveksles med standarder for trådløst nett (WLAN).
Integrasjon	En integrasjon er en knytning mellom to eller flere systemer ved hjelp av definerte grensesnitt.
IP-multicast	IP-kommunikasjon hvor data sendes samtidig til en spesifisert gruppe lyttende mottakere i nettverket
IPv4	Standard adresseringsprotokoll for forbindelsesfri kommunikasjon i nettverk
IPv6	Siste versjon av IP-kommunikasjonsprotokoll som på sikt vil erstatte IPv4
Ironkey	Godkjent USB-lagringsenhet med krypteringsteknologi (www.ironkey.com)
KNX	OSI-basert nettverks protocol for BAS
Lagrings-løsning	Samlebegrep for ulike nettverkstilkoblede løsninger der data kan lagres eksternt. Eksempler er filserver (fysisk/virtuell), NAS/SAN
LAN	Local Area Network, kablet nettverk
LDAP	Lightweight Directory Access Protocol – Standard protokoll for tilkobling/integrasjon mot Active Directory

Begreper	Beskrivelse
Leverandør	I dette dokumentet benyttes dette som begrep for den som leverer tilbud på bakgrunn av en anbudsforespørsel fra Oppdragsgiver
MAC-adresse	Unik ID tildelt nettverksgrensesnitt på lag2 i OSI-modellen
ModBus	Kommunikasjonsprotokoll benyttet mellom automasjon og feltenheter
MS SCEP	Microsoft System Center Endpoint Protection – standard antivirusløsning for klient-PCer i HSØ
MSMQ	Microsoft Message Queuing – Microsofts løsning for meldingskø, støttet i de fleste versjoner av Windows
NAC	Network Access Control – Se IEEE 802.1x
NAS	Network Attached Storage
NAT/PAT	Network Address Translation/Port Address Translation – en metode for å mappe en IP-addresse/Port-range til en annen
Oppdragsgiver	I dette dokumentet benyttes dette som begrep for de(t) aktuelle helsefortak(ene)
OS	Operativsystem
PBAC	Policy Based Access Control – Se ABAC
Personopplysning	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar, fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet
RAM	Internminne
RDP	Remote Desktop Protocol – Microsoft protokoll for fjernstyring av Windows PC/server
RF	Radiofrekvens
RJ45	Modulærkontakt benyttet for termingering av nettverkskabel (Ethernet)
Risikovurdering	Risikovurdering utføres ved nyetablering av, samt endringer på, eksisterende BTU-løsninger i HSØ. Risikovurderingen skal identifisere risiko og sårbarhet i løsningen, samt evt. risikoreduserende tiltak med ansvarlig for utførelse.
RS232	Seriellport – grensesnitt for seriell dataoverføring
SAN	Storage Area Network
SD anlegg	Anlegg for sentral driftskontroll
Sensitive personopplysninger	Se Særlige kategorier av personopplysninger
SFTP	FTP over SSH
Skytjeneste	Skytjenester (cloud computing) er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.
SMB	Server Message Block – kommunikasjonsprotokoll for filer og skrivere.
SNMP trap	Simple Network Management Protocol, Trap – en metode for en klient å informere en overvåkningstjeneste om hendelser, som feil, i nettverk eller programvare.
SOAP	Simple Object Access Protocol - Protokoll for utveksling av strukturert informasjon over web-servicer vha. XML
SSH	Secure Shell - Applikasjonsprotokoll med kryptert kommunikasjon for tilgang til pålogging og kommandolinje på fjernstyrt klient/server
SSL	Secure Sockets Layer – Sertifikatbasert krypteringsprotokoll typisk benyttet for web
STP	Shielded Twister Pair, nettverkskabel med skjerming og mulighet for jording
Særlige kategorier av personopplysninger	Med særlige kategorier av personopplysninger (tidligere benevt sensitive personopplysninger) menes i denne sammenheng: • Opplysninger regulert av Personvernforordningen artikkel 9 • Helseopplysninger som inneholder navn, fødselsnummer eller andre personentydige kjennetegn slik at opplysningene kan spores tilbake til en enkeltperson • Helseopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet og erstattet med et løpenummer, en kode, fiktive navn eller lignende, som viser til en atskilt liste med de direkte personopplysningene, eksempelvis et rekvisisjonsnummer, prøve-ID e.l.
TCP	Transmission Control Protocol – Sikker kommunikasjonsprotokoll for applikasjoner som kommuniserer over et IP-nettverk
Tjeneste-leverandør	Det til enhver tid gjeldende selskap/organisasjon som har ansvar for drift- og forvaltningsansvar for Oppdragsgiver sin samlede IKT-infrastruktur og IKT-tjenestekatalog
UDP	User Datagram Protocol – Usikker kommunikasjonsprotokoll for applikasjoner som kommuniserer over et IP-nettverk
UltraVNC	Applikasjon for fjernstyring av klient/server gjennom fjernaksessløsning
USB	Universal Serial Bus – grensesnitt for tilkobling av periferiutstyr
VLAN	Virtual LAN - en måte for logisk inndeling av nettverk i separate broadcastdomener

Begreper	Beskrivelse
VRF	Virtual Routing and Forwarding. En virtualiseringsteknologi som gjør det mulig å ha flere uavhengige rutingstabeller i en og ruter. Dette gjør det mulig å ha overlappende, eller identisk adresserom i rutingstabellene uten at det gir adressekonflikter. Man slipper da å etablere separate nettverk med flere fysiske rutere, alt kan etableres og segmenteres på en og samme ruter.
WCF	Windows Communications Foundation – Microsoft API for integrasjonstjenester
WINS	Windows Internet Name Service. Tjeneste definert av Microsoft for å mappe maskinnavn opp mot IP-adresse og tjenestetype maskinen kan tilby
WLAN	Wireless Local Area Network, trådløst nettverk
XML	eXtensible Markup Language - Standard for strukturerte data i tekstformat

Kravspesifikasjon

IKT- tjenester og Informasjonssikkerhet for MTU

Innholdsfortegnelse

VIKTIG INFORMASJON

Formål

Dette dokumentet skal brukes til evaluering/vurdering av Leverandørens tilbudte løsning innenfor områdene IKT og Informasjonssikkerhet. I tillegg skal den i størst mulig grad kartlegge løsningens grunnleggende funksjonalitet og egnethet i Oppdragsgivers IKT-infrastruktur i forkant av et endelig kundedesign. Dette minimerer risiko for **utilsiktede etableringskostnader, økt implementeringstid eller at ønsket og tilbudt funksjonalitet må reduseres** for å møte Oppdragsgivers pålagte krav til Informasjonssikkerhet og personvern. Dokumentet skal også medvirke til at Oppdragsgiver oppfyller lovreglene i personvernforordningen (GDPR).

Forklaring til skjema for kravspesifikasjon IKT-tjenester og Informasjonssikkerhet for MTU

Krav: (A/B/C/D)		
A	Obligatorisk	Obligatorisk krav som skal oppfylles. Manglende evne til å etterleve kravet medfører at tilbudt løsning skal avvises.
B	«Bør»-krav	Leverandørens oppfyllelse av kravet gis enten en egnethetsvurdering ved vurdering eller en score ved en faktisk tilbudsevaluering.
C	Dokumentasjon	Kan kombineres med A/B/D-angivelse av kravtype. Understreker da at Oppdragsgiver forventer et utdypende svar. Hvis C står alene er dette kun et informasjonspunkt som ikke krever besvarelse eller evalueres
D	Høy	Kombineres med B for å signalisere at kravet er svært viktig, men ikke obligatorisk. Leverandørens evne til å oppfylle kravet gis en score med en tilhørende **høy vekting** ved tilbudsevaluering.

Oppdragsgivers bestemmelser gjeldende Leverandørens besvarelse

Svar:
Alle angitte[1] krav uansett kravtype **skal** besvares av Leverandør. Svaret fastsetter i hvilken grad leverandøren kan tilfredsstille kravets ordlyd og innhold.

Kravene besvares med Ja (**J**), Nei (**N**) eller Utdyping (**U**). Svarkategori «**U**» dekker alle alternativer som ikke kan besvares med et entydig Ja/Nei. For krav som besvares med «**U**», skal det som ikke kan dekkes fra Leverandørens side særskilt utdypes. Dette for å sikre Oppdragsgivers forståelse av besvarelsen på kravene så man kan vurdere og/eller evaluere på korrekt grunnlag.

*Da denne kravspesifikasjonen er generisk og skal brukes til et stort spenn av MTU-anskaffelser, vil det være krav som ikke naturlig inngår i enhver anskaffelse. Kombinasjonen Nei som svar (**N**) og Ikke aktuelt (**I/A**) som utdyping kan benyttes av Oppdragsgiver for **å forhåndsmarkere** at krav ikke vurderes som aktuelle for en anskaffelse.*

***OBS:** Kombinasjonen Nei (**N**) og Ikke aktuelt (**I/A**) **kan også benyttes der leverandøren selv** anser kravet som uaktuelt ut fra innholdet i den tilbudte løsningen, med en skriftlig forklaring på hvorfor kravet ikke anses som aktuelt.*

Det **skal ikke** henvises til, eller benyttes, manualer, brosjyrer, reklamemateriell o.l. som ***rene besvarelser*** på kravpunkter. For å sikre korrekt sammenligningsgrunnlag når ulike leverandører skal evalueres/vurderes må en besvarelse på et krav derfor inneholde nødvendige kopier av den relevante teksten. Denne presiseringen er spesielt viktig for obligatoriske krav (A-krav) da disse kravene skal forplikte Leverandøren, og skape trygghet hos Oppdragsgiver på at det tilbys en løsning som er mulig å etablere i Oppdragiver sin infrastruktur.

[1] Med "angitte» menes kravpunkter som Oppdragsgiver ikke har markert som uaktuelle fra sin side med kombinasjonen: «N» og «I/A»

Dette sikrer at en påfølgende designprosess ikke medfører utilsiktede etableringskostnader og lang implementeringstid, samt at etterspurt og tilbudt funksjonalitet kan tas i bruk i henhold til Helse Sør-Øst sine krav til Informasjonssikkerhet og personvern.

Leverandøren er uansett ansvarlig for at deres designforslag og løsningselementer dokumenteres på en komplett og helhetlig måte for å dekke alle besvarelser og spesifikasjoner som inngår i denne kravspesifikasjonen. Dette betyr at Leverandøren også er ansvarlig for å beskrive alle nødvendige løsningselementer for å få en komplett og fungerende løsning, selv om slike elementer ikke er eksplisitt beskrevet av Oppdragsgiver i kravspesifikasjonen. Oppdragsgiver forventer derfor at Leverandøren gjør oppmerksom på eventuelle relevante aspekter ved løsningen som ikke er dekket av Oppdragsgivers kravspesifikasjon.

Utdyping av besvarelser:
Her **kan** Leverandør utfylle sin besvarelse av type «J» eller «N» der det oppleves som påkrevd for å sikre forståelsen. Det er imidlertid ikke anledning til å omskrive et «J» til «N», eller omvendt, gjennom en slik utdyping. Entydig besvarelse av typen «**J/N»** uten nevneverdig utdyping forventes kun på enkle krav. Ved besvarelsen «**J/N»** på enkle krav anser Oppdragsgiver at Leverandøren har **akseptert/benektet** alle vilkår i kravet 100%, og evaluerer ut fra dette. Ved besvarelse «**U**» **skal** Leverandøren beskrive hva som ikke kan tilfredsstilles i Oppdragsgivers krav. Leverandøren skal beskrive i hvilken grad et avvik er permanent, eller om dette kan løses med en designendring/alternativt løsningsforslag. Dersom innfrielse av kravet krever endring i Leverandørens tilbudte løsning, skal Leverandøren angi tidsperspektiv for når kravet vil være innfridd. Hvis alternative løsningsforslag endrer prisbildet har skal det utdypes med priskonsekvens som behandles i henhold til beskrivelsen i avsnitt under for **«Pris:»**. Leverandøren skal her dokumentere den faktiske priskonsekvens for Oppdragsgiver.

Pris:
Svares ut med «**J**» eller «**N**». Leverandør angir her om det eksisterer et eget, dedikert, priselement for at leverandøren skal kunne oppfylles sine forpliktelser i henhold til svar på kravet. Det forventes da at tilhørende priselement er angitt i Prisbilaget – med henvisning til korresponderende kravelement. Hvis svaret er «N» forutsetter Oppdragsgiver at kravet er oppfylt ved kontraktsinngåelse, eller innen et avtalefestet tidspunkt i kontraktsperioden, uten at det utløser noen ekstra kostnad for Oppdragsgiver.

Vurdering av kvalitet på dokumentasjon

Oppdragsgiver ønsker at alle besvarelser på mer enn ca. 100 ord, eller som inneholder figurer, flyttes ut i Leverandørens svarbilag med henvisning for å gi økt lesbarhet og sikre en helhetlig forståelse og korrekt vurdering/evaluering. Slike besvarelser skal referere til kravnummer og utarbeides spesifikt for det kravet det gjelder.

Oppdragsgiver vil vurdere kvaliteten på den tilsendte dokumentasjon og besvarelsene i kravspesifikasjonen samlet sett. Dette kan gis en samlet poengsum ved en evaluering.

1 OVERORDNET SYSTEMBESKRIVELSE

Denne seksjonen omhandler krav til Leverandørens overordnede beskrivelse av den samlede leveransen.

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Kravtekst:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Overordnede dokumentasjonskrav				
1.1	Leverandøren skal fremlegge et overordnet løsningsdesign og systemdokumentasjon som på en tydelig og oversiktlig måte viser de relevante hovedkomponenter, overordnet dataflyt og kommunikasjonsgrensesnitt internt og eksternt for løsningen. Dette kravet gjelder uavhengig av om løsningen består av kun programvare, kun enkeltstående MTU eller sammensatte systemløsninger med server(e), skytjenester, MTU(er) og klient-PCer for MTU-styring/overvåking og datahøsting fra MTU. **Merknad**: Det er meget viktig at dokumentasjonen gjenspeiler løsningen, uansett størrelse og omfang, eksempelvis med en tilhørende illustrasjon, slik den er tenkt etablert hos Oppdragsgiver. Dokumentasjonen skal inkludere alle enkeltkomponenter i systemet (instrumenter, klient-PC, servere, lagring, nettverk, konvertere m.m.).	**AC**			
1.2	Leverandøren skal fremlegge en detaljert oversikt, basert på utarbeidet dokumentasjon fra kravpunkt 1.1, over all relevant nettverksmessig dataflyt slik den er planlagt etablert hos Oppdragsgiver. Dette inkluderer detaljert dataflyt mellom løsningens enkeltkomponenter, med eksisterende tjenesteelementer i Oppdragsgivers nettverk, samt eventuell datautveksling med skytjenester eller andre eksterne tjenester. **Merknad:** Med «relevant» menes dataflyt som benytter eller traverserer Oppdragsgivers datanettverk og derfor kan kreve at brannveggregler må tilrettelegges for at den tilbudte løsningen skal fungere i Oppdragsgivers IKT-infrastruktur.	**AC**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Kravtekst:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
1.3	Hvis den tilbudte løsningen er basert på bruk av eksterne tjenester hos Leverandør og/eller Produsent (skytjenester, web-portal eller tilsvarende), bør tilbudet også inneholde relevant løsningsdesign og ROS for leverandørens benyttede infrastruktur til produksjon av de nødvendige tjenestene som tilbudt løsning er avhengig av. **Merknad**: Hvis det ikke benyttes eksterne tjenester, så besvares punktet med «N» og «I/A»	**BD**			
1.4	Det IKT-relaterte bistandsomfanget i Leverandørens tilbud skal inkludere all leverandørbistand som tilbys for ferdigstillelse av endelig løsningsdesign i Oppdragsgivers infrastruktur, installasjon, konfigurasjon, testing og produksjonssetting, samt utarbeidelse av nødvendig system- og driftsdokumentasjon.	**A**			
	Overvåking og endrings-/oppdateringsregime				
1.5	Den tilbudte løsningen eller komponenter i løsningen bør tilby mekanismer og/eller grensesnitt for overvåking for å minimere forekomster av feil og nedetid. **Merknad:** Eventuelle føringer og begrensninger rundt mulighet for integrasjon med eksisterende overvåkingssystem hos Oppdragsgiver, samt hvordan eventuell varsling til systemansvarlig kan gjennomføres, utdypes i Leverandørens besvarelse.	**BC**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Kravtekst:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
1.6	Leverandøren skal forholde seg til, og etterleve, Oppdragsgivers og Oppdragsgivers driftsleverandørs endringsregime[2] for produksjonssatte løsninger. **Merknad:** Leverandør kan ikke planlegge og/eller iverksette endringer som kolliderer med planlagte endringer i Oppdragsgivers infrastruktur. Dette krever gjensidig varsling av planlagte endringer mellom aktørenes tjenesteansvarlige personell. Ved eventuell konflikt er det Oppdragsgivers og Oppdragsgivers driftsleverandørs endringsregime som har prioritet.	**A**			
1.7	Den tilbudte løsningen bør bare benytte komponenter som har gyldige, produsentspesifikke vedlikeholdsavtaler gjennom hele kontraktsperioden. **Merknad:** Eventuelle komponenter som allerede er utenfor produsentspesifikk vedlikeholdsavtale (End Of Life/End Of Support) eller som vil bli det i løpet av avtaletiden skal spesifiseres.	**BCD**			
1.8	Leverandøren bør tilby en dokumentert og forpliktende roadmap for oppgradering og videreutvikling av den tilbudte løsningen.	**BC**			
1.9	Leverandøren bør sikre at produsentens anbefalinger følges ved oppdatering av programvare, konfigurasjon, kodeverk, nomenklatur eller andre registre for å ivareta den tilhørende endringsprosessen på tilbudt løsning. **Merknad:** Det er viktig at det utdypes hvordan løsningen skal vedlikeholdes (gjennom integrasjon, brukergrensesnitt, oppdatering av database, eller lignende), samt overordnede kommunikasjonstekniske krav for å gjennomføre slik oppdatering på den tilbudte løsningen.	**BCD**			
	Redundanskrav				

[2] Med endringsregime menes de reglene som gjelder for planlegging, varsling og utførelse av endringer på infrastruktur hos Oppdragsgiver, inklusive sentrale datasentre i Helse Sør-Øst. Dette omfatter all fysisk infrastruktur som strøm/kjøling, fysisk kabling, nettverk, nettverkstjenester, serverplattformer (fysiske og virtuelle) som den tilbudte løsningen er avhengig av for å kunne produsere de avtalte tjenestene. All endring som leverandør ønsker å utføre må være avtalt og omforent med Oppdragsgivers 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.

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Kravtekst:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Med redundanskrav menes krav knyttet til redundans på eksempelvis server- og nettverksløsninger som den tilbudte løsningen inkluderer eller er avhengig av for å levere med avtalt tjenestekvalitet og/eller oppetid. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».	**C**			
1.10	Den tilbudte løsningen bør mellomlagre data lokalt på benyttet klient-PC eller instrument for å opprettholde medisinsk funksjonalitet ved brudd i datakommunikasjon med andre systemer. **Merknad:** For Oppdragsgiver er det viktig å få utdypet hvor stor den eventuelle lokale lagrings-/bufferkapasiteten er (eksempelvis maksimal tidsperiode, antall kjøringer e.l.), samt hvilke overførings- og sletterutiner som eventuelt finner sted når datakommunikasjonen er gjenopprettet.	**B**			
1.11	En tilbudt systemløsning bør ha mulighet for intern lastbalansering	**B**			
1.12	En tilbudt systemløsning bør ha mulighet for ekstern lastbalansert nettverkstilkobling	**B**			
1.13	En tilbudt systemløsning bør ha mulighet for intern redundans (failover)	**B**			
1.14	Den tilbudte løsningen bør ha mulighet for redundant ekstern nettverkstilkobling (failover)	**B**			

2 LISENSHÅNDTERING

Denne seksjonen skal beskrive hvilke lisensieringsmekanismer den tilbudte løsningen eventuelt benytter. For Oppdragsgiver og Oppdragsgivers 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.

Kravspesifikasjon			**Leverandørens besvarelse**		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	De etterfølgende kravpunktene besvares kun hvis det tilbudte systemet inneholder lisensieringsmekanismer. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».				
2.1	Eventuelle lisensieringsmekanismer bør være basert på sentral lisens og sentralisert lisensforvaltning.	**BD**			
2.2	Leverandøren bør beskrive systemets 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 • bruk av lisensservere utenfor Oppdragsgivers infrastruktur, inklusiv teknisk løsning og eventuelle konsekvenser for bruk av løsningen dersom slik kommunikasjon ikke kan etableres av Oppdragsgiver	**BCD**			
2.3	Leverandøren bør på en oversiktlig måte utdype eventuelle begrensninger i bruk av systemet som er en konsekvens av lisensieringsmekanismen. Eksempler på viktige utdypingsområder er begrensninger av teknisk eller funksjonell art: • i antall brukere • i antall tilkoblede enheter	**BCD**			

Kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	• lagringsvolumer • ved overskridelser av lisensgrenser				
2.4	Systemet bør ha tydelige og veldokumenterte rutiner for forvaltning og vedlikehold av lisens/sertifikat. Eksempler på viktige utdypingsområder er: • Hvordan fornyes evt. tidsavgrenset lisens/sertifikat • Hvordan aktiveres/deaktiveres tidsbegrenset lisens/sertifikat • Hvordan utføres versjonering av lisens/sertifikat	**BCD**			
2.5	Systemet bør ved midlertidig bortfall av lisensieringsmekanisme fungere uten at dette påvirker bruken av systemet. Leverandøren bes beskrive evt. konsekvenser for bruk av systemet ved bortfall av lisensieringsmekanisme.	**BC**			

3 NETTVERK

Sykehuspartner er i dag Oppdragsgiver sin leverandør av nettverksinfrastruktur med tilhørende nettverkskomponenter som svitsjer, rutere, brannmurer o.l. MTU-tjenester vil normalt etableres logisk adskilt fra andre tjenester og Oppdragsgivers administrative nett forøvrig. Ved behov åpnes det for tilgang mot annet MTU og integrasjoner mot andre tjenester i Oppdragsgivers nettverk, som f.eks. fagsystemer.

Ved bruk av konvertering mellom Ethernet og andre interfaceteknologier, må dette dokumenteres detaljert for å sikre at de tilbudte løsningene er teknologikompatible og kan benyttes i et kundespesifikt design. Oppdragsgiver sitt nettverk er klargjort for IPv6, men dette er ikke tatt i bruk ennå. Gjeldende protokoll er IPv4. Oppdragsgivers nettverk kan benytte NAC (802.1x) som stenger ned LAN-tilgang for ukjente eller inaktive enheter. Oppdragsgiver har også standardisert brannmursregulering mellom nettverkssoner hvor inaktive TCP-sesjoner termineres av sikkerhetsgrunner etter 60 minutter. Dette legger krav på det utstyret som skal kobles opp i Oppdragsgiver sitt nettverk, og Leverandør må ta hensyn til dette i utarbeidelsen av tilbudt løsning.

Oppdragsgiver tillater heller ikke at Klient-PC-er eller servere som inngår i den tilbudte løsningen kan settes opp som mulige gateway-maskiner (dvs. skal ikke ha to eller flere nettverkskort) mellom ***et internt MTU-nett og Oppdragsgiver sitt datanettverk***. I slike tilfeller skal leveransen inkludere en godkjent ruter/brannmur som **separerer** den tilbudte løsningen fra Oppdragsgiver sitt datanettverk.

HSØ kravspesifikasjon	Leverandørens besvarelse

Nr:	Beskrivelse:	Krav: (A/B/C/D)	Svar: (J/N/U)	Utdyping: (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	Pris: (J/N)
3.1	Den tilbudte løsningen bør benytte standard teknologier/protokoller for kablet ekstern datatrafikk, for eksempel RJ45/Ethernet, USB, Firewire. **Merknad:** Utdyp hvilke standard teknologier/protokoller som benyttes, samt eventuelle avvik i form av leverandørspesifikke begrensninger eller tekniske krav.	**BC**			
3.2	Den tilbudte løsningen bør benytte IPv4 dersom den tilbudte løsningen har ekstern datautveksling over Ethernet med Oppdragsgivers systemer.	**BD**			
3.3	Den tilbudte løsningen bør støtte fremtidig bruk av IPv6 dersom den tilbudte løsningen har ekstern datautveksling over Ethernet med Oppdragsgivers systemer.	**B**			
3.4	Den tilbudte løsningen bør konfigureres med Oppdragsgivers egne IP-adresseserier dersom den tilbudte løsningen har ekstern datautveksling over Ethernet/IP med Oppdragsgivers systemer. **Merknad:** Dersom den tilbudte løsningen ikke støtter bruk av Oppdragsgiver sine IP-adresseserier kan leveransen inkludere en dokumentert og leverandørdriftet ruter/gateway/brannmur som utfører "NAT/PAT" adresseoversetting mellom Oppdragsgivers adresseserie og Leverandørens adresseserie. Dokumentasjonen skal inneholde nødvendige IP-adresser og TCP-/UDP-portnumre for tjenester som tilgjengeliggjøres. Denne ruter/gateway/brannmur-løsningen skal alltid risikovurderes og godkjennes før en tilkobling til Oppdragsgivers nettverk kan utføres.	**BC**			
3.5	Den tilbudte løsningen bør benytte oppdragsgivers nettverk uten å stille leverandørspesifikke begrensninger eller tekniske krav. **Merknad:** Utdyp eventuelle begrensninger/krav i forhold til MDR eller andre sertifiseringer, eksempelvis føringer på: • må den samlede, tilbudte løsningen stå i ett og samme VLAN, eller kan den segmenteres i flere VLAN? • vil en løsning segmentert over flere VLAN, gi konsekvenser for eksisterende sertifiseringer – eks: MDR og/eller CE? • Tilgjengelig nettverkskapasitet (båndbredde), latency, pakkestørrelse eller pakketap i nettverket, bruk av brannvegg etc.	**BCD**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
3.6	Den tilbudte løsningen bør håndtere brudd i nettverkskommunikasjon mellom de ulike delene av løsningen, slik at den medisinske funksjonaliteten opprettholdes mens systemet gjenoppretter sin nettverkskommunikasjon uten behov for manuelle brukeroperasjoner. **Merknad:** Se avsnitt 2 i ledetekst for kapittel 3. Sikkerhetsmekanismer i Oppdragsgivers nettverk lukker inaktive nettforbindelser på lag2 & lag3 (MAC&IP). Leverandørens eventuelle krav og konsekvenser gitt av disse mekanismene må dokumenteres med tanke på design og tilhørende sikkerhetsgodkjenning.	**BC**			
3.7	Hvis den tilbudte løsningen implementerer dataoverføring basert på trådløs kommunikasjon bør det benyttes standard teknologier/protokoller, eksempelvis WLAN, Bluetooth, GSM/LTE, annen RF. **Merknad:** Utdyp eventuelle avvik gitt av leverandørspesifikke begrensninger eller tekniske krav, eksempelvis manglende support for sikkerhetsmekanismer, forholdsregler knyttet opp mot frekvenser, signalstyrker, mulighet for interferens etc.	**BC**			
3.8	Leverandørens tilbudte løsningsdesign bør unngå bruk av komponenter med to eller flere nettverkskort som skal kobles opp mot Oppdragsgiver sitt datanettverk. **Merknad:** Ved bruk av flere nettverkskort *kan* etablerte sikkerhetsfunksjoner i Oppdragsgiver sitt datanettverk brytes eller omgås. Dette er en uønsket situasjon for Oppdragsgiver. Unntak kan gis for påkrevde og dokumenterte funksjonelle behov, eksempelvis for instrumenter direktekoblet til klient-PC med krysset kabel.	**BD**			
3.9	Leverandørens eventuelle lokale instrumentnett og Oppdragsgiver sitt datanettverk bør kun sammenkobles med en, for Oppdragsgiver/Tjenesteleverandør, godkjent ruter/brannmur som separerer den tilbudte løsningen fra Oppdragsgiver sitt datanettverk ref. punkt 3.8.	**BD**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
3.10	Datatrafikk fra den tilbudte løsningen bør benytte IP-Unicast ved traversering av Oppdragsgivers brannvegger. **Merknad**: Oppdragsgivers nettverk støtter i dag *ikke* bruk av IP-Multicast gjennom ruter/VRF.	**BD**			
3.11	Leverandørens tilbudte løsning bør være kompatibel med bruk av IEEE 802.1x (Network Access Control). **Merknad**: For alt utstyr som skal tilkobles og gis tilgang til Oppdragsgivers nettverk, registreres utstyret som hovedregel med godkjent MAC-adresse for tilgangskontroll.	**BD**			
3.12	Leverandørens tilbudte løsning bør fungere uavhengig av WINS eller Windows hosts-fil.	**BC**			
3.13	Leverandørens tilbudte løsning bør benytte DNS navneoppslag fremfor IP-adresser.	**B**			
3.14	Leverandørens tilbudte løsning bør fungere uten krav til jording via nettverk (STP).	**B**			

4 MASKINVARE

Sykehuspartner er i dag Oppdragsgiver sin foretrukne leverandør av maskinvare som klient-PCer, servere (fysiske og virtuelle), lagringsløsninger, skrivere, skannere og strekkodelesere.

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
4.1	Leverandørens tilbudte serverløsning bør implementeres på virtuell serverplattform som kan leveres av Oppdragsgivers tjenesteleverandør. **Merknad**: Utdyp eventuelle leverandørspesifikke krav til virtuelle servere, for eksempel: RAM, CPU, OS (HOST/GUEST), disk, RAID, tilkoblingskort o.l.	**BC**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
4.2	Leverandørens tilbudte løsning bør implementeres på klient-PCer som kan leveres av Oppdragsgivers tjenesteleverandør. **Merknad**: Utdyp eventuelle leverandørspesifikke krav til klient-PCer, for eksempel: RAM, CPU, OS, disk, RAID, tilkoblingskort o.l.	**BC**			
4.3	Dersom påkrevet som en del av løsningen, bør Leverandørens tilbudte løsning implementeres på bærbare enheter (eks. bærbar PC, mobiltelefon, nettbrett, personsøker eller lignende) som kan leveres av Oppdragsgivers tjenesteleverandør, forutsatt at utstyret oppfyller Leverandørens eventuelle krav til medisinsk godkjenning av slikt utstyr. **Merknad**: Utdyp også eventuelle andre leverandørspesifikke krav til slike bærbare enheter (bærbar PC, mobiltelefon, nettbrett, personsøker eller lignende), for eksempel: RAM, CPU, OS, disk, o.l.	**BC**			
4.4	Leverandørens tilbudte løsning bør benytte lagringsløsninger som kan leveres av Oppdragsgivers tjenesteleverandør. **Merknad**: Utdyp eventuelle leverandørspesifikke krav til benyttet lagringsløsning dokumenteres, for eksempel: lagringsprinsipper, filsystem, diskvolum, lese/skrivehastighet, o.l.	**BC**			
4.5	Foretrukket løsning for utskrift i Oppdragsgiver er basert på sentraliserte nettverksskrivere med «Pull Print» (sikker print). Leverandørens tilbudte løsning bør benytte sentraliserte nettverksskrivere som kan leveres av Oppdragsgivers tjenesteleverandør for utskriftsløsninger. **Merknad**: Utdyp eventuelle leverandørspesifikke krav til lokale skrivere (lokalprinter eller egne nettverksskrivere), for eksempel: RAM, CPU, disk, utskriftshastighet, tilkoblingskort o.l. Bruk av «Pull Print» **forutsetter** at Leverandørens tilbudte løsning kan integreres i tilstrekkelig grad mot, alternativt innmeldes i, Oppdragsgivers AD for nødvendig brukerhåndtering.	**BC**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
4.6	Leverandørens tilbudte løsning bør benytte periferiutstyr som skanner, strekkodeleser o.l. som kan leveres av Oppdragsgivers tjenesteleverandør, forutsatt at utstyret oppfyller nødvendige krav til medisinsk godkjenning **Merknad**: Utdyp eventuelle andre leverandørspesifikke krav til slikt periferiutstyr (supporterte merker, modeller, strekkodeformater, utskriftsformat etc.).	**BC**			

5 OPERATIVSYSTEM OG PROGRAMVARE

Dette kapittelet omhandler operativsystem, samt tilhørende programvare og komponenter i den tilbudte løsningen. For øyeblikket er standard operativsystem Windows 7 64/32-bit på klient-PCer og Windows Server 2019 på servere. Det er pågående aktivitet for å oppdatere standard operativsystem for klient-PCer til Windows 10. I tillegg supporterer Tjenesteleverandør nyere versjoner av RedHat Linux. Gjennom Tjenesteleverandørens avtaleverk er målsetningen at alle løsninger skal støtte en såkalt «N/(N-1)»-livssyklus for alle de systemkomponenter som inngår i en løsning. Dette betyr at det benyttes siste, eller nest siste, versjon av alle HW/SW-komponenter.

Gjeldene standard software hos Oppdragsgiver for anti-malware er i dag Trend på Windows servere og Microsoft System Center Endpoint Protection (SCEP) på Windows-klienter. For databaser er gjeldende standard Microsoft SQL Server 2019 og Oracle Enterprise R12.

Enkelte av helseforetakene i HSØ benytter RES One Suite fra RES (res.com) for styring og sikring av klientarbeidsflater på Windows 7-plattformen, inkludert tilgjengeliggjøring av klientapplikasjoner med alle tilhørende plugins/3.partskomponenter. Distribusjon av applikasjoner gjøres hovedsakelig via APP-V, alternativt via SCCM. RES One Suite har i ettertid byttet navn til Ivanti Workspace Control (ivanti.com), og vil fremover benyttes på Windows 10 klient-PCer.

Kravene i dette kapitlet omhandler også nødvendige systemkomponenter som Oppdragsgiver må tilgjengeliggjøre for at den tilbudte løsningen skal fungere som avtalt. Slike systemkomponenter bør kunne hentes fra gjeldende produkt- og tjenestekatalog fra Tjenesteleverandør. Eksempelvis kan Tjenesteleverandør utstede nødvendige sertifikater til bruk for HTTPS/SSL i serversammenheng etter nærmere avtale.

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
5.1	Leverandørspesifikk *klient-PC* som inngår i den tilbudte løsningen bør benytte OS i henhold til Tjenesteleverandør sitt regime for livssyklus. **Merknad:** Med *klient-PC* menes PC som benyttes enten til styring/overvåking av et direktetilkoblet MTU eller PC med installert programvare for prosessering av MTU-genererte data.	**B**			
5.2	Leverandørspesifikk *server* med Windows- eller Linux-OS som inngår i den tilbudte løsningen bør benytte OS i henhold til Tjenesteleverandør sitt regime for livssyklus.	**B**			
5.3	Leverandør bør utdype alle relevante krav for påkrevde komponenter (OS, klientapplikasjoner, serverprogramvare o.l.) som ikke leveres som en del av den tilbudte løsningen, eller avviker fra Tjenesteleverandørens standarder. Eksempelvis: Nettleser, webserver, databaser, Java, Flash, Silverlight, MS Office, .NET Framework, C++ Redistributable, MDAC o.l. og eventuelle spesifikke versjoner av disse.	**BCD**			
5.4	Hvis tilbudt løsning benytter lokal webserver bør det være implementert mekanismer som sikrer server og innhold mot uautorisert tilgang. **Merknad**: Utdyp hvilke sikkerhetsmekanismer som er aktivert, samt hvilke mekanismer som kan aktiveres i tillegg.	**BC**			
5.5	Funksjonaliteten i den tilbudte løsningen bør ikke til enhver tid være avhengig av kommunikasjon med webtjenester utenfor Oppdragsgivers nettverk, eksempelvis hos Leverandør/Produsent eller direkte mot internett. **Merknad:** Oppdragsgiver krever kontroll og sporbarhet på all ekstern kommunikasjon. Dokumentasjon på hvorfor slik kommunikasjon er påkrevd, og i hvilken grad løsningen ivaretar Oppdragsgiver sine sikkerhetskrav til ekstern kommunikasjon må fremlegges ved tidspunkt for tilbud. Endelig bruk av slik kommunikasjon krever en gjennomført risikovurdering som gir en godkjenning.	**BD**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
5.6	Leverandør bør gjennomføre relevant «herding» av OS og benyttede applikasjoner på Leverandørspesifikt utstyr som inngår i den tilbudte løsningen.	**B**			
5.7	Den tilbudte løsningen bør benytte kryptering på applikasjonsnivå ved datautveksling med andre systemer.	**B**			
5.8	Leverandørspesifikke *klient-PCer* bør benytte Oppdragsgiver sin standard-programvare for anti-malware. **Merknad:** Leverandør må utdype eventuelle behov for avvik fra Oppdragsgivers standard pga sertifiseringer som MDR, CE etc.	**B**			
5.9	Oppdatering av definisjonsfiler for kjent malware på *klient-PCer* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell oppdatering av definisjonsfiler.	**BC**			
5.10	Malwarescanning på Leverandørspesifikke *klient-PCer* bør skje uten behov for ekskludering av mapper.	**B**			
5.11	Malwarescanning på *klient-PCer* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell malwarescanning.	**BC**			
5.12	Leverandørspesifikke *servere* bør benytte Oppdragsgiver sin standard-programvare for anti-malware. **Merknad:** Leverandør må utdype eventuelle behov for avvik fra Oppdragsgivers standard pga sertifiseringer som MDR, CE etc.	**B**			
5.13	Oppdatering av malwaresignaturer på *servere* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell oppdatering av malwaresignaturer, inklusiv eventuelle eksterne tilganger nødvendig.	**BC**			
5.14	Malwarescanning på Leverandørspesifikke *servere* bør skje uten behov for ekskludering av mapper.	**B**			
5.15	Malwarescanning på *servere* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell malwarescanning.	**BC**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
5.16	Utrulling av sikkerhetspatcher og servicepacks fra OS-leverandør bør utføres uten produsentspesifikke krav eller begrensninger. **Merknad:** Begrensninger som skyldes sertifiseringer eller produsentens egenpålagte begrensninger må dokumenteres. Det er også viktig for Oppdragsgiver at det utdypes hvorvidt nødvendige sikkerhetspatcher og servicepacks kan installeres automatisk, eller om det kreves at automatisk oppdatering må forsinkes eller settes opp til å installeres først ved neste omstart av klient-PCer eller server.	**BCD**			
5.17	Leverandørspesifikke *klient-PCer* som inngår i den tilbudte løsningen bør ha mulighet for å meldes inn i Oppdragsgiver sitt AD	**B**			
5.18	AD-innmeldte *klient-PCer* som skal benyttes i den tilbudte løsningen bør benytte diskkryptering (eks. MS Bitlocker). **Merknad**: Utdyp eventuelle begrensninger knyttet til bruk av diskkryptering.	**B**			
5.19	Leverandørspesifikke *servere* som inngår i den tilbudte løsningen bør ha mulighet for å meldes inn i Oppdragsgiver sitt AD	**B**			
5.20	Den tilbudte løsningens tilhørende klientapplikasjon(er) bør være kompatibel med Oppdragsgivers bruk av RES One/Ivanti Workspace Control og App-V samt SCCM. **Merknad**: Utdyp eventuelle forutsetninger og begrensninger i den tilbudte løsningen.	**BD**			
5.21	Bruk og/eller vedlikehold av installert programvare på den tilbudte løsningen (utover selve OS-installasjonen) på *klient -PC* bør skje uten bruk av lokal administratorrettighet på operativsystemet.	**B**			
5.22	Bruk og/eller vedlikehold av installert programvare på den tilbudte løsningen (utover selve OS-installasjonen) på *server* bør skje uten bruk av lokal administratorrettighet på operativsystemet.	**B**			

6 INFORMASJONSSIKKERHET OG TILGANGSSTYRING

Oppdragsgiver stiller strenge krav til sikkerhet i forbindelse med etablering og drift av MTU. MTU skal beskyttes mot eksterne trusler, sykehusnettet og annet MTU. Sykehusnettet skal på sin side beskyttes mot MTU. Helseforetakene i Helse Sør-Øst har i fellesskap vedtatt et regionalt ledelsessystem for informasjonssikkerhet basert på ISO 27001. Ledelsessystemet er gjeldene for samtlige helseforetak i regionen. Kravene i dette kapitellet er utledet av krav fra ledelsessystemet.

- Regionalt ledelsessystem for informasjonssikkerhet - https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet

Oppdragsgiver plikter å oppfylle lovreglene i personvernforordningen (GDPR). Det stilles derfor krav til at tilbudt løsning skal tilfredsstille krav i Personvernforordningen 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

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

- «Normen» - https://ehelse.no/normen
- Veileder i personvern og informasjonssikkerhet - medisinsk utstyr - https://ehelse.no/normen/veiledere/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr
- «Normen» (på Engelsk) - https://ehelse.no/normen/documents-in-english

Eksempler på føringer gitt av personvernforordningens krav til innebygd personvern og «Normen» er:

- Oppdragsgiver prefererer MTU-løsninger der det benyttes individuell brukeridenter med sikret rollebasert tilgangsstyring
- MTU-løsninger skal ikke lagre personopplysninger hvor navn, fødselsnummer eller rekvisisjonsnummer sammen med diagnose, prøveresultat og lignende lagres uten at krav til Informasjonssikkerhet er ivaretatt
- Oppdragsgiver har som målsetning å standardisere på å bruke Oppdragsgiver sin Integrasjonstjeneste basert på Helse Sør-Øst sin Regionale Integrasjonsplattform for alle former for integrasjon mellom nettverks- og sikkerhetssoner. Dette gjelder både socket-basert kommunikasjon og filflytt.
- For løsninger som krever bruk av eksternt lagringsmedium for manuell overføring av datafiler retter Oppdragsgiver seg etter retningslinjene fra regionalt styringssystem for informasjonssikkerhet, ref. regional kryptopolicy punkt 4.3: «Kryptering under lagring av data». I dag benyttes krypterte lagringsenheter fra IronKey hos Oppdragsgiver.

HSØ kravspesifikasjon	Leverandørens besvarelse

Nr:	Beskrivelse:	Krav: (A/B/C/D)	Svar: (J/N/U)	Utdyping: (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	Pris: (J/N)
6.1	Den tilbudte løsningen bør ikke ha vesentlige avvik i forhold til lover og regler for informasjons- og pasientsikkerhet. **Merknad:** Leverandøren skal utdype alle relevante avvik. Dette for å sikre at alle risikomomenter kan vurderes og ivareta Oppdragsgiver sitt pålegg og å etterleve Direktoratet for eHelse sin «Norm for informasjonssikkerhet» («Normen»).	**BCD**			
6.2	Leverandøren bør, så snart produsenten har implementert funksjonalitet og forbedringer som støtter GDPR og teknisk IT-sikkerhet, tilby Oppdragsgiver programvareoppdatering, programvarelisens og installasjon uten ekstra kostnad for Oppdragsgiver.	**B**			
6.3	Den tilbudte løsningen bør benytte sentralisert fillagring og/eller database. **Merknad**: Utdyp evt. hvilken databaseplattform som støttes, samt hvorvidt løsningen baseres på lokale tjenester og om de i så fall kan erstattes med sentraliserte serverbaserte tjenester.	**BC**			
6.4	Den tilbudte løsningen bør benytte individuelle brukeridenter både på OS- og applikasjonsnivå.	**B**			
6.5	Individuell brukerautentisering bør gjøres mot grupper definert i Active Directory via LDAP, fortrinnsvis LDAP over SSL (LDAPS). **Merknad**: Utdyp hvorvidt både LDAP eller LDAPS støttes. Leverandøren bør også utdype hvorvidt en LDAP/LDAPS integrasjon kun gjør en synk av brukere fra AD til lokal brukerdatabase, eller om autentisering skjer direkte mot AD.	**BC**			
6.6	Alle former for lokale brukerprofiler (brukernavn/passord) lagret i lokale brukerdatabaser, konfigurasjonsfiler e.l. som benyttes til klient-, database- eller applikasjonspålogging bør sikres med standardiserte mekanismer for tilgangskontroll og kryptering. Se regional kryptopolicy. **Merknad**: Utdyp hvordan krav til tilgangskontroll og kryptering er tenkt ivaretatt i den tilbudte løsningen.	**BCD**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
6.7	Den tilbudte løsningen bør støtte attributtbasert tilgangsstyring (ABAC) og regelbasert tilgangsstyring (PBAC). Sentrale utdypingselementer er: • hvilke rolletyper som eksisterer – eksempelvis adminbruker, superbruker, Lese&Skrive-bruker, Lese-bruker e.l.? • er roller endelig fastsatt eller kan roller (om)konfigureres i løsningen? • Hvilke sikringsmekanismer som er etablert for å unngå endring i rollebasert tilgangsstyring er bygget inn i den tilbudte løsningen?	**BCD**			
6.8	Den tilbudte løsningen bør ha funksjonalitet for begrensning av tilgang til personopplysninger for enkeltbrukere og grupper av brukere.	**BCD**			
6.9	Hvis den tilbudte løsningen inneholder standard- eller systembrukere, så bør det bare benyttes unike passord før tilkobling til Oppdragsgivers IKT-infrastruktur. **Merknad:** Det skal ikke benyttes hardkodede passord, passord som kan hentes direkte fra brukermanualer eller annen form for tilgjengelig dokumentasjon.	**BD**			
6.10	Ved eventuelt behov for ekstern transport, eller ved lagring av personopplysninger på minnepinne, ekstern harddisk, filsystem eller i database, bør den tilbudte løsningen støtte kryptering av data. **Merknad:** Beskrive evt. støtte og krypteringsstandard/-styrke som benyttes.	**BC**			
6.11	Hvis den tilbudte løsningen benytter eksterne webløsninger/-portaler for analyse, rapportering eller drift og forvaltning bør løsningen oppnå en «Overall Rating» på rapport generert hos Qualys SSL[3] Labs på minst «A». **Merknad**: Hvis det ikke benyttes eksterne webløsninger/portaler besvares spørsmålet med «N» og «I/A»	**B**			

[3] Qualys SSL Server Test er en åpen verifisering av kryptering. https://www.ssllabs.com/

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
6.12	Løsningen bør ha funksjonalitet for automatisert sletting av personopplysninger, når disse er prossesert eller bekreftet overført til fagsystem.	**BCD**			

7 BACKUP

Oppdragsgiver ønsker å etterleve prinsippene om Data Lifecycle Management hvor Backup/Restore er en sentral komponent for å ivareta datasikkerhet og integritet. Målsetningen er å benytte sentralisert Backup/Restore i størst mulig grad.

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Kravpunktene under fylles ut hvis den tilbudte løsningen skal benytte egenprodusert eller sentrale backuptjenester over Oppdragsgivers nettverk eller hvis dette er funksjonalitet som kan tas i bruk i løpet av kontraktsperioden. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».				
7.1	Backup av disk, inklusive programvare, konfigurasjon, kalibrering o.l., på server og klient-PC bør kjøres mot eksisterende sentraliserte og automatiserte backuptjenester hos Oppdragsgiver. **Merknad:** Det forutsettes da at backupklient kan installeres på den tilbudte løsningen og eventuelle leverandørspesifikke brannmurer åpnes for tilgang fra Oppdragsgiver sin backupløsning.	**B**			
7.2	Backup av databaser bør kjøres mot eksisterende sentraliserte og automatiserte backuptjenester hos Oppdragsgiver. **Merknad:** Det forutsettes da at backupklient kan installeres på den tilbudte løsningen og eventuelle leverandørspesifikke brannmurer åpnes for tilgang fra Oppdragsgiver sin backupløsning.	**B**			
7.3	Databaser som inngår i den tilbudte løsningen bør ha støtte for både full og inkrementell backup (gjennom f.eks. loggbackup/loggshipping) av databaser	**B**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
7.4	Leverandørbistand ifm. gjenoppretting fra backup bør enten være inkludert, eller spesifisert i prisbilaget for serviceavtale	**B**			

8 INTEGRASJONER

Hvis den tilbudte løsningen benytter datautveksling med sentrale kundesystemer, bør dette skje med bruk av åpne/de Facto standarder for slik datautveksling.

Helse Sør-Øst har en Regional Integrasjonsplattform for informasjonsdeling og informasjonsutveksling internt i helseforetaket, mellom helseforetak og med eksterne aktører. Denne plattformen inneholder standardiserte integrasjonsløsninger, basert på internasjonale og nasjonale standarder. Eksempler på slike standarder er HL7/HL7 FHIR . Eksempler på kjente og benyttede kommunikasjonsprotokoller er HTTP(S), FTP, SFTP/FTPS, SMB.

Hensikten med de etterfølgende kravene er å identifisere om produktet støtter den Regional Integrasjonsplattformen som er etablert i Helse Sør-Øst. Dette gjelder viktige elementer som loggfunksjonalitet, sikkerhetsmekanismer, benyttede kommunikasjonsprotokoller, meldingsformater og semantikk. Alle disse faktorene vil påvirke tidsforbruk og kostnad ved en etablering av integrasjon.

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Kravpunktene under fylles ut hvis den tilbudte løsningen skal utveksle data med andre sentrale servertjenester i Oppdragsgivers nettverk eller dette er funksjonalitet som kan tas i bruk i løpet av kontraktsperioden. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».	**C**			
8.1	Den tilbudte løsningen bør inkludere API eller tekniske løsninger for å tilpasses en Integrasjonsløsning, eksempelvis: Webservice, fileksport/import, WCF, DICOM.	**B**			
8.2	Den tilbudte løsningen bør benytte API på en sikker måte for integrasjon og informasjonsutveksling. Utdyp hvilke sikkerhetsmekanismer den tilbudte løsningen kan supportere ved bruk av API.	**BC**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
8.3	All utveksling av informasjon bør etableres med internasjonale standarder. **Merknad:** Eksempler på slike standdarder er HL7 og DICOM	**BC**			
8.4	Utveksling av informasjon bør gjøres uten å være underlagt leverandørspesifikke krav eller begrensninger i forhold til hvilke protokoller som kan benyttes. Eksempler på protokoller som kan benyttes hos Oppdragsgiver er: TCP/UDP, FTP/FTPS/SFTP, SMB, SMTP, SOAP (HTTP/HTTPS), REST (HTTP/HTTPS), MSMQ, DICOM.	**BC**			
8.5	Personopplysninger bør ikke overføres i parametere, metadata, header eller på annet vis i integrasjoner slik at de blir synlige i transportlogger underveis til mottakeren **Merknad:** F.eks ved bruk av HL7 FHIR GET vil parameterne legges i webserver loggen på transportserverne	**BD**			
8.6	Den tilbudte løsningen bør benytte Oppdragsgivers standardiserte integrasjonstjeneste uten at det stilles leverandørspesifikke krav eller begrensninger for semantikk i de benyttede standardiserte meldingsformater, inkludert hvilke formatversjoner, som kan benyttes.. **Merknad**: Utdyp slike eventuelle krav/begrensninger, inkludert eventuelle implementeringsavvik i benyttet standard. Eksempler på slik semantikk er: ASTM, HL7, ebXML.	**BC**			
8.7	Den tilbudte løsningen bør ha mulighet for logging av meldingsflyt og meldingskvitteringer som gjør det mulig å oppdage meldinger som ikke kommer frem eller blir kvittert med negativ kvittering, men også vite hvilke meldinger som har kommet korrekt fram til mottakeren **Merknad**: Utdyp hvilken loggfunksjonalitet den tilbudte løsningen eventuelt har og hvordan dette kan understøtte behov for meldingsdokumentasjon, eventuell feilsøking og analysering av avvik på sendte og mottatte data i grensesnittet mellom MTU og andre aktører.	**BCD**			
8.8	Den tilbudte løsningen bør leveres med dokumentasjon som beskriver leverandørens grensesnitt for integrasjoner.	**BCD**			

9 IKT-RELATERT DRIFT OG FORVALTNING

Helse Sør-Øst tilbyr i dag en standard fjernaksessløsning for alle eksterne utstyrsleverandører. Den benevnes «Leverandøraksess» og skal benyttes for all leverandørspesifikk drift og forvaltning som ikke skjer med fysisk oppmøte i Oppdragsgivers 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. Bruk av egendefinert intern leverandøraksess med løsninger som 4G-modem, samt programvare som TeamViewer, LogMeIn og liknende tillates ikke i Helse Sør-Øst.

Leverandøren får tilgang til en aksesserver hos Oppdragsgiver, hvor nødvendig programvare og/eller fjernstyringsprogram mot MTU-klient/-server gjøres tilgjengelig. Alle brukere av fjernaksessløsningen skal knyttes opp mot personlige, identifiserte brukere hos Leverandøren.

Enkelte helseforetak har i tillegg standardisert «filsluse» for kontrollert og sikker overføring av godkjente data mellom Oppdragsgiver og Leverandør.

Det er etablert en regional VPN-Gateway for terminering av VPN-forbindelser mellom Leverandører og Oppdragsgiver. Dette er den foretrukne metoden for utgående datatransport over VPN fra Oppdragsgiver sitt nettverk. All planlagt bruk av dataoverføring over VPN må først risikovurderes og godkjennes før dette kan etableres. Leverandøren skal gi en forpliktende forsikring/dokumentasjon på benyttede dataformater, at VPN-bruken kun omfatter tekniske data, og at det ikke er risiko for overføring av personopplysninger, inkludert krypterte. Alle ønskede endringer i formatoppsett og bruk av VPN skal godkjennes av Oppdragsgiver i forkant før endringer kan gjennomføres.

Det er sentralt og viktig for både Oppdragsgiver og Oppdragsgivers Tjenesteleverandør at utstyr i Oppdragsgiver sitt nettverk kan tilby loggingsfunksjonalitet på flere nivåer (hardware/OS/sikkerhet/brukeraktivitet m.m.). Alle logger som den tilbudte løsningen genererer der innholdet må klassifiseres som virksomhets- eller personsensitivt, må sikres i henhold krav om informasjonssikkerhet (ref. «Normen»). Dette må gjøres for å sikre at essensiell logginformasjon ikke kan leses, endres eller slettes av uautorisert personell.

Hvis Oppdragsgiver er omforent med Leverandør om at drift og forvaltning krever bruk av Leverandøraksess, så må det som hovedregel inngås Databehandleravtale med Oppdragsgivers tjenesteleverandør.

HSØ kravspesifikasjon			**Leverandørens besvarelse**		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
	Kravpunktene under er relatert til bruk av Oppdragsgivers fjernaksessløsning og fylles kun ut hvis denne planlegges benyttet ved produksjonssetting eller dette er funksjonalitet som kan tas i bruk i løpet av kontraktsperioden.	**C**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
9.1	Leverandøren bør benytte Oppdragsgiver sin tilbudte fjernaksessløsning for drift og forvaltning av den tilbudte løsningen. **Merknad**: Utdyp hvilket behov Leverandør har for tilgjengeliggjort programvare i Oppdragsgiver sin standard fjernaksessløsning for å supportere den tilbudte løsningen via fjerntilgang. I dag gir Leverandøraksess tilgang til aksesserver med installerte forvaltnings-/driftsverktøy som *UltraVNC, WinSCP, RDP og SSH*.	**BCD**			
9.2	Logger som leverandør har tilgang til for drift og forvaltning bør kun inneholde teknisk informasjon, og ikke personopplysninger. **Merknad**: Utdyp hvorvidt leverandørtilgang til produksjonslogger kun omfatter tekniske data, og om det er risiko for innsyn i personopplysninger, inkludert kodede.	**BCD**			
9.3	Leverandør bør gjennomføre teknisk support uten behov for å få utlevert/overført tekniske logger og eksempelmateriale via VPN.	**BCD**			
9.4	Noen løsninger har støtte for at personopplysninger skjules/anonymiseres når leverandør har tilgang til systemet ifm. vedlikehold, såkalt *«service tilgang» eller «service user modus»*. Leverandøren bes beskrive evt. støtte for dette i den tilbudte løsningen.	**BD**			
9.5	Den tilbudte løsningen bør logge og lagre tekniske hendelser eller feil. **Merknad**: Utdyp hvorvidt det benyttes logging til Windows EventLog, loggfiler, databaser, SNMP traps etc.	**BD**			
9.6	Den tilbudte løsningen bør logge og lagre brukeroperasjoner (brukeraktivitet inklusiv uautorisert, eller forsøk på uautorisert, bruk). **Merknad**: Utdyp hvorvidt det benyttes logging til Windows EventLog, loggfiler, databaser, SNMP traps etc.	**BD**			
9.7	Den tilbudte løsningen bør gi autoriserte brukere hos oppdragsgiver tilgang til logger gjennom et standardisert brukergrensesnitt. **Merknad**: Utdyp hvordan logger tilgjengeliggjøres.	**BC**			

HSØ kravspesifikasjon			Leverandørens besvarelse		
Nr:	**Beskrivelse:**	**Krav:** (A/B/C/D)	**Svar:** (J/N/U)	**Utdyping:** (Maks. 100 ord, eller henvisning til kravet i Leverandørens svarbilag)	**Pris:** (J/N)
9.8	For de ulike typene loggdata som lagres i den tilbudte løsningen, inkludert lesing, endring og sletting av logger, bør gjeldende offentlige informasjonssikkerhetskrav ivaretas. **Merknad**: Utdyp hvordan sikkerhetskrav knyttet til konfidensialitet, integritet og tilgjengelighet ivaretas for de ulike typene loggdata som lagres i den tilbudte løsningen.	**BCD**			

Forkortelser og begreper

Begreper	Beskrivelse
4G-modem	USB-modem benyttet til 4G GSM-kommunikasjon
ABAC	Attribute Based Access Control – også benevnt policy based access control (PBAC), definerer et tilgangskontrollregime hvor rettigheter tildeles brukeren gjennom bruk av regelsett ved å kombinere ulike attributer.
AD	Active Directory – Microsofts katalogtjeneste for autentisering og autorisering av brukere innenfor et Windows domene
API	Application Programming Interface, grensesnitt for integrasjon
ASTM	Standardiseringsorgan for internasjonale standarder, bl.a. innenfor labkommunikasjon.
Bluetooth	Teknologi for trådløs kommunikasjon
CPU	Central Processing Unit - prosessor i f.eks. klient-PC/server
CSV	CSV - Comma Separated Values - tekstfil inneholdende data separert med komma eller annet tegn for separasjon av felt
DICOM	Digital Imaging and Communications in Medicine – standard for utveksling av bildefiler
DNS	Domain Name System - Systemtjeneste for å oversette mellom maskinnavn og IP-adresse
ebXML	Electronic Business using eXtensible Markup Language - XML standarder for bruk ved elektronisk overføring av forretningsinformasjon
Ekstern datautveksling	Med ekstern datautveksling menes all datatrafikk som benytter Oppdragsgivers infrastruktur. Dette kan eksempelvis være kommunikasjon med sentraliserte tjenester for autentisering og autorisering av brukere, fillagring, database, eller integrasjon med andre tjenester.
Endringsregime	Med endringsregime menes de reglene som gjelder for planlegging, varsling og utførelse av endringer på Oppdragsgivers infrastruktur, inklusive sentrale datasentre i Helse Sør-Øst. Dette omfatter all fysisk infrastruktur som strøm/kjøling, fysisk kabling, nettverk, nettverkstjenester, serverplattformer (fysiske og virtuelle) som den tilbudte løsningen er avhengig av for å kunne produsere de avtalte tjenestene. All endring som leverandør ønsker å utføre må være avtalt og omforent med Oppdragsgivers 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.
EPJ	Elektronisk pasientjournal
Fagsystem	Et større, overbyggende IT-system som ivaretar bred funksjonell støtte innenfor et avgrenset funksjonsområde, eller på tvers av flere funksjonsområder. Eksempelvis LIMS, EPJ eller elektronisk kurve.
F5 BigIP VPN	Standard leverandøraksess via VPN leveres gjennom produktet BigIP fra F5
Firewire	IEEE1394, teknologi for kablet høyhastighets dataoverføring
FTP/FTPS	File Transfer Protocol/File Transfer Protocol m/SSL-kryptering, protokoller for filoverføring
GDPR	General Data Protection Regulation (EU) 2016/679, EUs personvernforordning
GSM	Global System for Mobile Communications - standard for telekommunikasjon for mobiler
Herding	Herding av klient PC, server o.a. IKT-komponenter er en metode som benyttes for å øke komponentens sikkerhet ved å fjerne og begrense mulige sikkerhetsmessige sårbarheter som kan utnyttes av en angriper. Dette kan eksempelvis gjøres gjennom å sikre at operativsystem, programvare og 3.programvarekomponenter er sikkerhetspatchet eller oppdatert til siste versjon, bruk av antivirus/anti-malware, bruk av lokal brannmur, samt stoppe/sperre tjenester som ikke benyttes.
HL7	Health Level 7 – standard for meldingsutveksling av klinisk og administrativ informasjon mellom helserelaterte informasjonssystemer
HOST	Windows hosts fil, statisk tekstfil med oversikt over maskinnavn og korresponderende IP-adresse
HTTP/ HTTPS	HyperText Transfer Protocol/HyperText Transfer Protocol Secure - standarder for kommunikasjon for World Wide Web
IEEE 802.1x	Standard for autentisering av maskinvare tilkoblet nettverk. Må ikke forveksles med standarder for trådløst nett (WLAN).
Integrasjon	En integrasjon er en knytning mellom to eller flere systemer ved hjelp av definerte grensesnitt.
IP-multicast	IP-kommunikasjon hvor data sendes samtidig til en spesifisert gruppe lyttende mottakere i nettverket
IPv4	Standard adresseringsprotokoll for forbindelsesfri kommunikasjon i nettverk
IPv6	Siste versjon av IP-kommunikasjonsprotokoll som på sikt vil erstatte IPv4
Ironkey	Godkjent USB-lagringsenhet med krypteringsteknologi (www.ironkey.com)
Lagrings-løsning	Samlebegrep for ulike nettverkstilkoblede løsninger der data kan lagres eksternt. Eksempler er filserver (fysisk/virtuell), NAS/SAN
LAN	Local Area Network, kablet nettverk

Begreper	Beskrivelse
LDAP	Lightweight Directory Access Protocol – Standard protokoll for tilkobling/integrasjon mot Active Directory
Leverandør	I dette dokumentet benyttes dette som begrep for den som leverer tilbud på bakgrunn av en anbudsforespørsel fra Oppdragsgiver
LIMS	Laboratory Information Management System, laboratoriesystem
MAC-adresse	Unik ID tildelt nettverksgrensesnitt på lag2 i OSI-modellen
MDD	Medical Device Directive
MS SCEP	Microsoft System Center Endpoint Protection – standard antivirusløsning for klient-PCer i HSØ
MSMQ	Microsoft Message Queuing – Microsofts løsning for meldingskø, støttet i de fleste versjoner av Windows
MTU	Medisinskteknisk utstyr
NAC	Network Access Control – Se IEEE 802.1x
NAS	Network Attached Storage
NAT/PAT	Network Address Translation/Port Address Translation – en metode for å mappe en IP-addresse/Port-range til en annen
Oppdragsgiver	I dette dokumentet benyttes dette som begrep for de(t) aktuelle helsefortak(ene)
OS	Operativsystem
PACS	Picture Archiving and Communication System
PBAC	Policy Based Access Control – Se ABAC
Personopplysning	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar, fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet
RAM	Internminne
RDP	Remote Desktop Protocol – Microsoft protokoll for fjernstyring av Windows PC/server
RF	Radiofrekvens
RJ45	Modulærkontakt benyttet for termingering av nettverkskabel (Ethernet)
Risikovurdering	Risikovurdering utføres ved nyetablering av, samt endringer på, eksisterende MTU-løsninger i HSØ. Risikovurderingen skal identifisere risiko og sårbarhet i løsningen, samt evt. risikoreduserende tiltak med ansvarlig for utførelse.
RS232	Seriellport – grensesnitt for seriell dataoverføring
SAN	Storage Area Network
Sensitive personopplysninger	Se Særlige kategorier av personopplysninger
SFTP	FTP over SSH
Skytjeneste	Skytjenester (cloud computing) er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.
SMB	Server Message Block – kommunikasjonsprotokoll for filer og skrivere.
SNMP trap	Simple Network Management Protocol, Trap – en metode for en klient å informere en overvåkningstjeneste om hendelser, som feil, i nettverk eller programvare.
SOAP	Simple Object Access Protocol - Protokoll for utveksling av strukturert informasjon over web-servicer vha. XML
SSH	Secure Shell - Applikasjonsprotokoll med kryptert kommunikasjon for tilgang til pålogging og kommandolinje på fjernstyrt klient/server
SSL	Secure Sockets Layer – Sertifikatbasert krypteringsprotokoll typisk benyttet for web
STP	Shielded Twister Pair, nettverkskabel med skjerming og mulighet for jording
Særlige kategorier av personopplysninger	Med særlige kategorier av personopplysninger (tidligere benevt sensitive personopplysninger) menes i denne sammenheng: • Opplysninger regulert av Personvernforordningen artikkel 9 • Helseopplysninger som inneholder navn, fødselsnummer eller andre personentydige kjennetegn slik at opplysningene kan spores tilbake til en enkeltperson • Helseopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet og erstattet med et løpenummer, en kode, fiktive navn eller lignende, som viser til en atskilt liste med de direkte personopplysningene, eksempelvis et rekvisisjonsnummer, prøve-ID e.l.
TCP	Transmission Control Protocol – Sikker kommunikasjonsprotokoll for applikasjoner som kommuniserer over et IP-nettverk
Tjeneste-leverandør	Det til enhver tid gjeldende selskap/organisasjon som har ansvar for drift- og forvaltningsansvar for Oppdragsgiver sin samlede IKT-infrastruktur og IKT-tjenestekatalog

Begreper	Beskrivelse
UDP	User Datagram Protocol – Usikker kommunikasjonsprotokoll for applikasjoner som kommuniserer over et IP-nettverk
UltraVNC	Applikasjon for fjernstyring av klient/server gjennom fjernaksessløsning
USB	Universal Serial Bus – grensesnitt for tilkobling av periferiutstyr
VLAN	Virtual LAN - en måte for logisk inndeling av nettverk i separate broadcastdomener
VRF	Virtual Routing and Forwarding. En virtualiseringsteknologi som gjør det mulig å ha flere uavhengige rutingstabeller i en og ruter. Dette gjør det mulig å ha overlappende, eller identisk adresserom i rutingstabellene uten at det gir adressekonflikter. Man slipper da å etablere separate nettverk med flere fysiske rutere, alt kan etableres og segmenteres på en og samme ruter.
WCF	Windows Communications Foundation – Microsoft API for integrasjonstjenester
WINS	Windows Internet Name Service. Tjeneste definert av Microsoft for å mappe maskinnavn opp mot IP-adresse og tjenestetype maskinen kan tilby
WLAN	Wireless Local Area Network, trådløst nettverk
XML	eXtensible Markup Language - Standard for strukturerte data i tekstformat

Bilag D17 - Vedlegg C

Kundens tekniske plattform

Innhold

1 Innledning

Det finnes i hovedsak tre IKT-plattformer i Helse Sør-Øst.

AHUS:
Betjener Akershus Universitetssykehus. Det finnes et begrenset antall tjenester fra SIKT til AHUS hvor det brukes AD trust for autentisering.

OUS:
Betjener Oslo Universitetssykehus.

SIKT:
Betjener alle øvrige helseforetak i Helse Sør-Øst, samt et mindre antall private virksomheter.

Dette dokumentet beskriver på et overordnet nivå SIKT IKT-plattformen.

Sykehuspartner HF er Kundens tjenesteleverandør, og er ansvarlig for etablering, drift og forvaltning av IKT-plattformen, samt mange av Kundens løsninger etablert i plattformen. Tjenesteleverandørens driftsansvar inkluderer datasentre etablert hos Kunden og fellesregionale datasentre etablert for helseforetakene i Helse Sør-Øst. Kunden har i tillegg enkelte lokale drifts og forvaltningsenheter med ansvar for IKT-systemer, bl.a. tilknyttet medisinskteknisk utstyr (MTU), laboratorievirksomhet og stråleterapi.

Leverandører gjøres oppmerksom på at IKT-plattformen er i kontinuerlig videreutvikling. Den overordnede strategiske målsetningen i regionen er å samle alt inn i en ny fellesregional plattform. Det må derfor forventes kontinuerlige aktiviteter i overskuelig framtid med migrering, konsolidering og sanering som kan påvirke nye anskaffelser både med tanke på målarkitekturer og prosjektgjennomføring. Endringer og oppgraderinger av infrastrukturen vil kunne forekomme i løpet av avtaleperioden.

1.1 Grønn IT

Helse Sør-Øst ønsker å fremme bærekraftig bruk av IT og forholder seg til føringer fra Grønn IT (https://www.ikt-norge.no/bransjenormer-guider/gronn-it/) ved anskaffelse, etablering, drift og forvaltning av IKT-plattformen og løsninger etablert i IKT-plattformen.

1.2 Livssyklus

Helse Sør-Øst er opptatt av at løsninger skal kunne vedlikeholdes og videreutvikles løpende, såkalt «Lifecycle Management». Operativsystem og programvare vil normalt støttes i gjeldende hovedversjon, samt forrige hovedversjon (n, n-1). Dette gjelder eksempelvis komponenter og tjenester:

- levert av Kundens tjenesteleverandør, og ikke inngår i leveransen av løsningen
- levert som en del av løsningen

- levert av 3.part

Løsningen må derfor kontinuerlig oppdateres og vedlikeholdes for å imøtekomme dette prinsippet. Merk at dette også medfører at løsningen må støtte løpende patching og oppgraderinger i Kundens tekniske plattform.

2 Arkitekturprinsipper

Helse Sør-Øst anser visse egenskaper som viktige for alle løsninger som skal innføres. Disse egenskapene er nedfelt som arkitekturprinsipper, og er nærmere beskrevet i følgende dokumenter:

- DIFIs «Overordnede IT arkitekturprinsipper for offentlig sektor»
- DIFIs «Arkitekturprinsipper for samhandling»
- Nasjonal IKT «Arkitekturprinsipper i spesialisthelsetjenesten»

3 Datasenter

Helseforetakene på SIKT-plattformen har normalt to separate datasentre (Sentralt hovedkommunikasjonsrom - SHKR). Her produseres tjenester som konsumeres lokalt på helseforetaket, og kritiske tjenester som er nødvendig for lokal overlevelse ved nettverksbrudd..

Det er etablert to fellesregionale datasentre (SDS) i Helse Sør-Øst:

- SDS1 lokalisert hos Digiplex
- SDS3 lokalisert hos Basefarm

Det er i tillegg etablert et eksternt datasenter for katastrofebackup (kald backup), SDS2 på Ahus.

Kundens lokale datasentre er knyttet sammen med fellesregionale datasentre via egne samband.

4 Nettverksinfrastruktur

4.1 Overordnet

Kundens nettverk er bygd opp med nettelementer primært fra Cisco og noe fra Juniper og HP både for kablet og trådløst nettverk.

De fellesregionale datasentrene (SDS) benytter nettelementer fra Cisco og Palo Alto.. Kommunikasjonen mellom Kundens nettverk og HSØ forøvrig er basert på IPv4 og ikke lag-2.

Det er etablert et felles redundant høyhastighets transportnett (HSØ Kjernenett) som kobler alle foretakene sammen. Dette er basert på en tradisjonell topologi med P og PE noder med MPLS som transportprotokoll.

4.2 Brannmurer

Det er standardisert på Cisco brannmurer internt, mens det benyttes brannmurer fra Palo Alto ut mot Internett. Cisco brannmurene er konfigurert med TCP «idle timeout» på to timer i Kundens nettverk, og Idle timeout på 1 time i de fellesregionale datasentrene.

4.3 Aksesskontroll

Det benyttes IEEE 802.1X EAP-TLS på alle kablede og trådløse nett hos Kunden. For utstyr som ikke støtter IEEE 802.1x benyttes MAC autentisering for å tildele riktig VLAN

802.1x med EAP-TLS autentiserer maskinsertifikater mot en RADIUS-tjeneste. Denne gir tilgang til spesifikke VLAN, eller nekter tilgang basert på sikkerhetsregler og attributter fra Active Directory (AD). Dersom endeutstyr som tilhører et HF nektes tilgang, skal porten plasseres i et karantene-VLAN der klienten får mulighet til å fikse opp i problemet som gjorde at den ble nektet tilgang.

4.4 Lastbalansering

Det benyttes lastbalanserer i Kundens lokale datasentre (SHKR), samt lastbalanserere i fellesregionale datasentre (SDS). Det benyttes lastbalanserere fra F5.

4.5 Trådløst nettverk

Kundens trådløse nettverk er etablert med utstyr fra Cisco Networks. De samme sikkerhetsprinsipper og sikkerhetsmekanismer som er innført for kablet nettverk er også etablert for trådløse nett.

Følgende SSID og tilhørende nettverk er standard:

SSID	Bånd (GHz)	Autentisering	Bruk
SIKTv2	2.4+5	WPA2 med 802.1x	Bærbare SIKT-laptops
SIV-util	2.4+5	WPA2 med 802.1x	MTU og bygg teknisk
Sykehusgjest	2.4+5	Portal/MACfilter	Pasienter og pårørende. Gjestenett

TABELL 1: TRÅDLØST NETTVERK – SSID OVERSIKT

SSID «SIKTv2» er standard SSID i HSØ for SIKT-klienter (PC'r). SSID «SykehusGjest» er standard SSID i HSØ for gjester.

4.6 Regionalt WAN mottak

Alle eksterne nettverksforbindelser, inklusive VPN-basert fjernaksess for ansatte og leverandører, termineres på regionalt WAN mottak. Regionalt WAN mottak er en del av kjerneinfrastrukturen som er levert av Kundens tjenesteleverandør.

Det er kun IPv4 trafikk som er mulig mellom WAN mottak og Kundens nettverk.

5 PC-klienter

5.1 Standard PC-klienter

Windows 7 64-bit benyttes i dag som operativsystem på standard PC-klienter, men det pågår en prosess for å oppgradere standard PC-klienter til Windows 10, planlagt ferdigstilt 2020. Brukere tillates ikke å være lokale administratorer, og det er kun godkjent programvare som tillates på klientene.

Standard PC-klient benytter lokal Windows brannmur, samt System Center Endpoint Protection (SCEP) for antivirus/antimalware. Det tillates ikke klient-til-klient trafikk.

Det er sperret for tilkoblet periferiutstyr som identifiseres som lagringsenheter, eksempelvis optiske drev eller USB-tilkoblet lagring. Krypterte USB lagringsenheter fra IronKey tillates, forutsatt at dette er bestilt gjennom og administrert av Kundens tjenesteleverandør. Alle bærbare PC-klienter er krypterte med BitLocker Drive Encryption.

5.2 MTU Klient

En MTU-klient defineres som en klient som i utgangspunktet er “single-purpose”, og benyttes til dedikerte oppgaver i tilknytning til MTU, eksempelvis for:

- overvåking eller styring av et MTU
- kjøring av MTU-relaterte klientapplikasjoner for etterbehandling av data hvor MTU er datakilde
- pre-prosessering av data som skal benyttes av MTU.

Det benyttes Windows 7 som standard (Engelsk Windows 7 Enterprise med SP 1 og 64 bit-utgave, med mulighet for norsk språkpakke). Bruk av Windows 10 er under planlegging. MTU-klienter kan ikke primært benyttes til kontor-administrative oppgaver, men det kan tilgjengeliggjøres en Citrix-arbeidsflate som gir brukeren tilgang til administrative og kliniske fagsystemer.

MTU-klienter etableres i egne MTU-klientsoner iht. sonemodellen etablert i Kundens nettverk, og kan ha redusert eller endret funksjonalitet fra SIKT Standard klient mht.:

- Antivirus
- Sikkerhetspatching

- Lokal lagring – inkl. lagring av sensitiv informasjon
- Backup
- Klientoppsett som skyldes softwaremessige krav fra leverandør, som f.eks. manglende støtte for RES og SCCM
- Utvidede eller tilpassede tilganger og rettigheter
- Funksjonsbrukerkonseptet (fellesbruker, typisk påloginger som går over flere skift eller tilrettelagt etter arbeidsprosesser)
- Skjermsparer og automatisk låsing
- Forvaltning:
    - fjernaksess for Kundens ansatte med MTU drifts- og forvaltningsansvar
    - fjernaksess for leverandører av MTU
- Internettilgang

Det benyttes i hovedsak en eller flere av følgende varianter av Windows 7 MTU-klient (blandet praksis i de forskjellige Helseforetakene):

- MTU-Standard – er basert på Kundens standard Windows 7 PC-klient, men har mulighet for enkelte tilpasninger i konfigurasjon mht. sikkerhet, drift og forvaltning. Dette er foretrukken MTU-klienttype.
- MTU-GPO - Denne klienttypen brukes hvis en eller flere av tjenestene SCCM, RES og SCEP ikke kan/bør benyttes. Klienten blir i stedet herdet med et sett GPO-er og er så langt det er mulig fjernadministrert.
- MTU-Ren - Dette er en frittstående klientvariant, som ikke kan være medlem av domenet og benytter ikke GPO.

For å beskytte MTU klienter med funksjonsbruker (konstant pålogget PC med upersonlig bruker) mot utilsiktet innsyn, samt logge brukeraktivitet, er det under utvikling en AD-styrt skjermlås, som kan låses opp av alle identifiserte brukere som tilhører riktig AD gruppe.

5.3 Funksjonsbruker

Kunden har etablert et standardisert konsept for håndtering av fellesbrukere på operativsystem, også kalt «funksjonsbruker».

Det ønskes fortrinnsvis å unngås bruk av funksjonsbrukere på operativsystemet, og benytte individuelle brukere for å bedre sikre tilgang, kontroll og sporbarhet. For enkelte bruksområder vil det derimot være hensiktsmessig å benytte funksjonsbruker, eksempelvis i sammenheng med PC-klienter som benyttes til aktiviteter som pågår over flere arbeidsskift.

Det er for funksjonsbruker etablert en rekke begrensninger:

- Funksjonsbruker er knyttet til én spesifikk PC-klient, og PC-klienten er satt opp med auto-pålogging. PC-klienten kan ikke benyttes for individuell pålogging når satt opp med funksjonsbruker

- Det er ikke tilgang til internett
- Det er ikke tilgang til filområder
- Det er ikke tilgang til epost
- Det stilles som krav at applikasjoner som gir tilgang til personopplysninger skal være sikret med individuell pålogging mot sentral autentiseringsløsning (IAM eller AD)
- Tilgang til filområder, epost o.a. applikasjoner kan skje gjennom en Citrix arbeidsflate, med krav om individuell pålogging av bruker

5.4 Distribusjon og patching av programvare

Til administrasjon, distribusjon og patching av *lokalt installert* programvare benyttes Microsoft System Center Configuration Manager i MSI-format. Microsoft App-V benyttes for sentralt *strømmede* applikasjoner. Programmene pakkes i MSI/App-V format ved hjelp av AdminStudio. App-V er preferert metode for applikasjonsdistribusjon.

Applikasjoner som skal distribueres til flere standard PC-klienter, skal normalt pakkes av Kundens tjenesteleverandør og distribueres gjennom godkjente distribusjonsmetoder. Alle applikasjoner som skal benyttes må «whitelistes» i RES One Suite.

5.5 Dynamisk arbeidsflate

RES One Suite fra Ivanti, i senere versjoner endret navn til Ivanti Workspace Control (ivanti.com), benyttes for å tilpasse og levere arbeidsflaten ut fra funksjonelle behov og brukerens organisatoriske tilhørighet. Herunder ligger tilgjengeliggjøring og «whitelisting» av applikasjoner.

5.6 Internettaksess

Internett aksess tillates fra PC-klienter på port 80 og 443 (http/https), og det benyttes URL filtrering på ytre brannmur (Palo Alto). Internet Exporer 11 er standard nettleser, og det er ikke tillatt med lokalt installert Java runtime.

Ved innføring av Windows 10 vil standard nettleser bli Microsoft Edge.

Google Chrome er innført som sekundærnettleser for Windows 7, og vil videreføres som sekundærnettleser for Windows 10.

5.7 Utskrift

Sentralisert utskriftsløsning er basert på Canon Uniflow Pull print/follow-me print, og det benyttes primært multifunksjonsskrivere etablert i sentrale områder.

For behov som ikke dekkes av sentralisert utskriftsløsning, som etikettskrivere og spesialskrivere, kan disse etableres lokalt. Dette forutsetter gjennomført risikovurdering.

5.8 AD struktur

Det benyttes ett felles domene for alle nye tjenester: sikt.sykehuspartner.no

Det finnes fortsatt andre domener i bruk, men disse er under avvikling og skal ikke benyttes ved etablering av nye tjenester.

5.9 Central Driver Store

Det tillates ikke at standard PC-klienter kan laste ned drivere fra Internett for installasjon. Alle godkjente og oppdaterte drivere skal gjøres tilgjengelig i lokalt etablert Central Driver Store i forbindelse med utrulling av Windows 10. Fjernaksess for ansatte (Always-on VPN)

I fjernaksessløsningen for ansatte hos Kunden benyttes Big-IP Access Policy Manager sammen med Big-IP Edge Client. Tilgang autentiseres med ID-Porten på sikkerhetsnivå 4, og gir tilgang til Kundens nettverk fra bærbare PC-klienter. I tillegg kan bruker logge seg på virtuelle arbeidsflater basert på Citrix-terminalaksess.

Prinsippet for VPN-tilgang er at en PC-klient automatisk tilkobles Kundens nettverk via VPN (såkalt «Always-on») og alltid er underlagt de samme sikkerhetsbestemmelsene for nettverkstilganger uansett hvor i verden man befinner seg. Dette innebærer også at internettaksess alltid reguleres gjennom ytre brannmur (Palo Alto).

Det tillates ikke bruk av BYOD-enheter i Kundens nettverk, bortsett fra i Gjestenett.

6 Server

Servere kjøres i hovedsak som virtuelle maskiner under VMware. Operativsystem på nye servere skal være:

- Windows Server 2019 og Windows Server 2016
- Redhat Enterprise Linux (RHEL) 7.5

Andre versjoner av operativsystemene finnes fremdeles i drift, men vil gradvis migreres til siste støttede versjon eller utfases. Det er ikke ønskelig at nye løsninger etableres på eldre versjoner av operativsystemene, eller andre operativsystem.

7 Databaseplattform

Følgende databaseplattformer er støttet:

- Microsoft SQL Server 2016, inklusiv Always-On cluster
- Oracle 12, inklusiv Maximum Availability Architecture (MAA)

8 Lagring, backup og arkivering

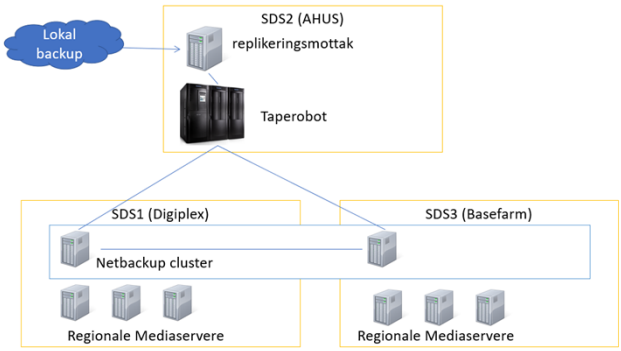
8.1 Lagring

Lagring kan foregå både på lokalt datasenter (SHKR) og fellesregionalt datasenter (SDS). Det benyttes både NAS- og SAN-basert lagring.

8.2 Backup

Symantec NetBackup benyttes for all backup.

Det er etablert to regionale backupmiljøer i SDS1 og SDS3, mens SDS2 benyttes til replikeringsmottak.



FIGUR 1 - BACKUP OG REPLIKERING PÅ SDS

Backupjobbene er normalt satt opp til å kjøre utenom normal arbeidstid (kl 17:00 til 05:00), med hovedtyngden av jobber etter midnatt. Jobber kan unntaksvis settes opp til å gå på dagtid, ved dokumenterte behov.

Det er definert forskjellige nivåer på backup (gull, sølv, bronse). De forskjellige nivåene vil normalt gjenspeile kritikaliteten til tjenesten.

Backupstatus blir overvåket daglig via NetBackup OpsCenter for både regionale og lokale backupmiljø.

8.3 Arkivering

Arkivering av lite brukt eller historiske data kan bestilles som opsjon.

9 Drift og forvaltning

9.1 Overordnet

Kundens tjenesteleverandør er drift- og forvaltningsansvarlig for Kundens tekniske plattform, og er normalt ansvarlig for drift og forvaltning av løsninger etablert i plattformen. Det er viktig at Leverandøren forholder seg til både de tekniske løsningene etablert i Kundens tekniske plattform, samt eksisterende rutiner, ved drift- og forvaltning av Løsninger etablert i Kundens tekniske plattform.

Det er i tillegg åpnet for prinsippet «delt forvaltning», der Kundens tjenesteleverandør kan tilby alt fra driftet nettverksaksess (Network as a Service) og opp til fulldriftet applikasjonsplattform (Software as a Service). Drift og/eller applikasjonsforvaltning på en

tjenesteleveranse (klient/server/devicer/applikasjon) kan dermed utføres av en ekstern leverandør.

Typiske eksempler på slik delt forvaltning er løsninger for medisinskteknisk utstyr (MTU), byggteknisk utstyr (BTU) og administrativteknisk utstyr (ATU), der Kundens tjenesteleverandør har drift av Kundens tekniske plattform opp til ønsket nivå, mens Kunden forvalter systemløsningen. En dedikert serversone for løsninger med delt forvaltning er under etablering. Den sikrer nødvendig separasjon og tilgangskontroll i forhold til løsninger som driftes og forvaltes i sin helhet av Kundens tjenesteleverandør.

Drift og forvaltning skal ikke utføres via direkteaksess. I stedet er det etablert en obligatorisk managementløsning basert på Citrix XenDesktop som sikrer adgangs- og tilgangskontroll, samt nødvendig sporbarhet og logging på aktiviteter. For eksterne leverandører har man i tillegg en VPN-portal som krever 2-faktor autentisering ved påloggingsforsøk.

Kunden er i ferd med å etablere en standardisert «filsluse» for kontrollert og sikker overføring av godkjente data mellom Kunden og Leverandør.

Kundens tjenesteleverandør har etablert faste frysperioder hvor det er streng regulering av hvilke endringer som kan gjøres i infrastrukturen eller i etablerte løsninger. Ved større driftsmessige hendelser i Kundens plattform, kan det etableres midlertidige frysperioder.

9.2 Fjernaksess for leverandører

Helse Sør-Øst har standardisert på fjernaksess gjennom løsninger fra F5 BigIP og Citrix-terminalaksess for eksterne leverandører. Den benevnes «Leverandørportalen» 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. En bruker av Leverandørportalen må være registrert i Kunden sitt personalsystem PAGA og bli tildelt en personlig bruker ID. Leverandøren får da tilgang til en jumpserver hos Kunden, hvor godkjente fjernstyringsprogram (RDP, SSH, WinSCP, UltraVNC) gjøres tilgjengelig. Ved spesielle behov kan annen programvare gjøres tilgjengelig etter godkjenning av Kunden.

All bruk av Leverandørportalen skal knyttes til personlige, identifiserte brukere hos Leverandøren. En bruker ID på Leverandørportalen er i utgangspunktet stengt, og åpnes kun etter avtale med Kunden og/eller med Kundens tjenesteleverandør. Åpninger gis for inntil 72 timer av gangen for vanlige supportbehov. Lengre intervaller (inntil 6 måneder) kan gis f.eks. ved installasjon, test og validering av større systemer

Bruk av Leverandørportalen forutsetter at det signeres taushetserklæring og inngås en Databehandleravtale mellom Kundens tjenesteleverandør og Leverandør.

9.3 Fjernaksess for drift og forvaltning

Kundens tjenesteleverandør gjør sin drift og forvaltning av Kundens tekniske plattform og løsninger etablert i plattformen via en «AdminDesktop» basert på Citrix XenDesktop.

Det er etablert en separat «Forvaltningsdesktop» for ansatte hos Kunden som har ansvar for drift og/eller forvaltning av internt etablerte løsninger, eksempelvis for MTU og BTU.

9.4 Overvåking

Kundens tjenesteleverandør har etablert sentraliserte løsninger for overvåking av Kundens nettverksinfrastruktur og IKT-plattform, samt underliggende komponenter og tjenester i Kundens tekniske plattform. Overvåking skjer gjennom en rekke agent-baserte og agentløse løsninger på forskjellige komponenter i infrastrukturen, hvor varsler og alarmer aggregeres opp i Micro Focus Operations Bridge.

9.5 Logging

Det er sentralt og viktig for både Kunden og Kundens tjenesteleverandør systemer etablert i Kundens tekniske plattform kan tilby drifts- og forvaltningsrelatert loggfunksjonalitet på flere nivåer, eksempelvis ved feilsituasjoner eller varsler tilknyttet hardware, operativsystem, tjenester i systemet, feilhendelser og andre varsler som kan bidra til at feilsituasjoner unngås eller man i etterkant av feilsituasjoner kan fremskaffe informasjon relevant for å avdekke feilårsak.

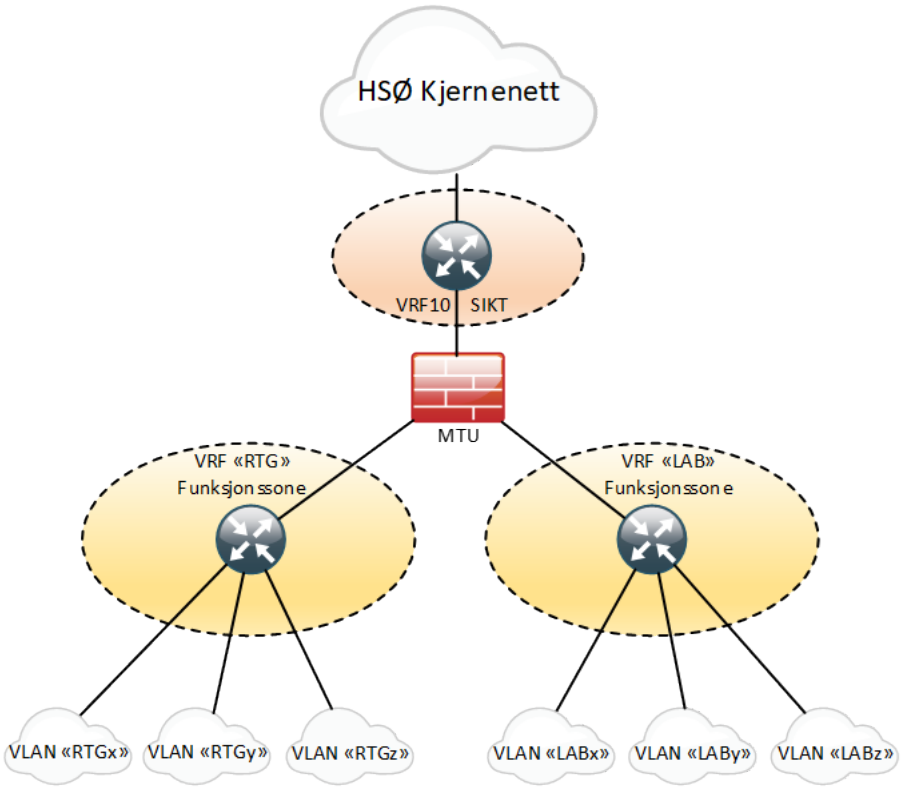
Kundens tjenesteleverandør har etablert et sentralt loggmottak for håndtering av relevante system- og sikkerhetslogger fra Kundens systemer. Sentralt loggmottak er basert på Splunk.

10 Medisinskteknisk, byggteknisk og administrativteknisk utstyr

10.1 Sonemodell

Det er etablert en sonemodell for bruk til MTU-, BTU- og ATU- løsninger, som ivaretar krav til sikkerhet, sporbarhet og delt forvaltning.

Sonemodellen er basert på standard etablerte mekanismer for separering og soneinndeling i et nettverk. Dette innbefatter bruk av eksisterende infrastruktur og tilhørende funksjonalitet som virtualiserte brannmurer, virtuelle rutinginstanser (VRF) og virtuelle LAN (VLAN) på nettverksutstyret. I tillegg benyttes mekanismer i active directory (AD) for tilgangsstyring der utstyret støtter dette.



FIGUR 2 EKSEMPEL - SONEMODELL MTU

BTU og ATU soner etableres etter samme prinsipp som for en MTU sone.

10.2 Medisinteknisk utstyr (MTU)

Medisinskteknisk utstyr (MTU) er definert som «*ethvert instrument, apparat, hjelpemiddel, materiell eller enhver gjenstand brukt til å diagnostisere, overvåke, behandle eller endre pasientens anatomi eller fysiologiske prosesser»*.

Det er stor variasjon i datakommunikasjonsmetoder til MTU. Noe utstyr er direkte tilkoblet nettverket, mens mange løsninger består av en PC-klient tilknyttet instrument via USB, RS232, Firewire etc, eller indirekte tilknyttet via Ethernet via MOXA/Digiboks o.l. konverteringsløsninger.

Det er i SIKT etablert sikkerhetsprinsipper og mekanismer for å håndtere eventuelle avvik, da ikke all MTU følger etablerte standarder for datakommunikasjon.

10.3 Byggteknisk utstyr (BTU) og Administrativt teknisk utstyr (ATU)

Byggteknisk utstyr (som f.eks. SD-anlegg) og Administrativt teknisk utstyr (f.eks. parkeringssystemer, kioskløsninger o.l.) etableres i egne, separate nettverkssoner tilrettelagt for formålet, og håndteres etter samme prinsipp som medisinskteknisk utstyr.

11 Lisensiering

For løsninger som har en lisensieringsmekanisme, foretrekkes det at slike etableres sentralisert for å sikre effektiv lisensforvaltning. Dette innebærer at:

- bruk av fysiske lisensdongler søkes unngått, grunnet utfordringer dette medfører i et virtualisert driftsmiljø
- bruk av distribuerte lisensfiler søkes unngått, grunnet utfordringer dette medfører mht vedlikehold av lisensfiler og applikasjonspakker lisensfilen evt. inngår i

12 Informasjonssikkerhet og personvern

12.1 Overordnet

Kunden plikter å oppfylle lovreglene i norsk lovverk, og stiller strenge krav til oppfyllelse av relevant lovverk vedr. informasjonssikkerhet ved anskaffelse, etablering, drift, forvaltning og avhending 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/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
- «Normen» (på Engelsk) - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/documents-in-english

For å understøtte Kundens forpliktelser og lovkrav tilknyttet informasjonssikkerhet, har Helse Sør-Øst definert et sett krav til informasjonssikkerhet i «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

Leverandøren forutsettes å ha satt seg inn i disse prinsippene, og sikrer at disse kan etterleves.

Kundens tjenesteleverandør benytter ISO 27001 som forvaltningsstandard i sikkerhetsarbeidet.

12.2 Risikostyring

Før løsningen kan etableres, og ved alle endringer av løsningen, må det gjennomføres og foreligge en godkjent risikovurdering. Risikovurderingen bygger på løsningens endelige løsningsdesign, med alle tilhørende komponenter, tjenester og konfigurasjon, slik løsningen er planlagt etablert hos Kunden. Dette vil normalt utarbeides av Kundens tjenesteleverandør, i samarbeid med Kunde og Leverandør. Endelig godkjenning av risikovurdering gjøres av Kunden.

Det er en målsetning at man for MTU legger ISO/IEC 80001 («Risk Management of Medical Devices on a Network») til grunn.

12.3 IAM og tilgangsstyring

Identitet- og tilgangsstyring (IAM) i Helse Sør-Øst består av flere komponenter og tjenester, men de tre viktigste tjenestene er Regional Provisjoneringstjeneste, Regional Autentiseringstjeneste og Regional Autoriseringstjeneste. Disse tjenester er helt avhengige av, og dermed integrert med, autoritative informasjonskilder og prosesser.

For nærmere beskrivelse, se *Bilag 3C: Kundens tekniske plattform – Identitet og tilgangsstyring.*

13 Integrasjon

For å sikre at den tekniske infrastruktur bygger opp under virksomhetsarkitekturen med fokus på tjenester, har Helse Sør-Øst etablert en SOA-Arkitektur for integrasjoner med Fagsystemer. Helse Sør-Øst har realisert SOA-Arkitekturen ved å etablere en regional integrasjonsplattform og en integrasjonspolicy. Integrasjonspolicyen legger klare krav og retningslinjer på hvordan integrasjoner skal etableres, og at disse skal gå gjennom integrasjonsplattformen.

For nærmere beskrivelse, se *Bilag 3B: Kundens tekniske plattform – Integrasjon*.

14 Forkortelser og begreper

Forkortelse / Begrep	Beskrivelse
AD	Active Directory – Microsofts katalogtjeneste for autentisering og autorisering av brukere innenfor et Windows domene
App-V	Microsofts teknologi for virtualisering og strømming applikasjoner.
ATU	Administrativteknisk utstyr
BTU	Byggteknisk utstyr
BYOD	Bring Your Own Device – privateide PC klienter, nettbrett eller mobiltelefoner, som ikke er eid av eller kontrollert av Kunden.
CDS	Central Driver Store
CRL	Certificatate Revocation List
DNS	Domain Name System - Systemtjeneste for å oversette mellom maskinnavn og IP-adresse
EAP-TLS	Extensible Authentication Protocol – benyttes i sammenheng med NAC
IAM	Identity and Access Management, Kundens systemer for sentral autentisering, autorisering og federering av brukere og rettigheter.
ID-porten	DIFI ID-porten benyttes for autentisering av brukere på sikkerhetsnivå 4 (BankID, BankID for mobil, Buypass og Commfides)
IDS	Intrusion Detection System

Forkortelse / Begrep	Beskrivelse
IEEE 802.1x	Standard for autentisering av maskinvare tilkoblet nettverk. Må ikke forveksles med standarder for trådløst nett (WLAN).
Kunden	I dette dokumentet benyttes dette som begrep for det aktuelle helseforetaket
Kundens tjenesteleverandør	Selskapet som har ansvar for drift- og forvaltningsansvar for Kunden sin samlede IKT-infrastruktur og IKT-tjenestekatalog. I denne sammenheng er tjenesteleverandør Sykehuspartner.
LDAP	Lightweight Directory Access Protocol – Standard protokoll for tilkobling/integrasjon mot Active Directory
MAC-adresse	Unik ID tildelt nettverksgrensesnitt på lag2 i OSI-modellen
MPLS	Multi Protocol Label Switching
MSI	Format for applikasjonspakker som skal installeres lokalt på PC-klient.
MTU	Medisinskteknisk utstyr
NAC	Network Access Control – Se IEEE 802.1x
PAGA	Kundens personalsystem
RADIUS	Remote Authentication Dial-In User Service – Nettverksprotokoll som benyttes for autentisering av maskiner ifm. bruk av NAC.
RDP	Remote Desktop Protocol – Microsoft protokoll for fjernstyring av Windows PC/server, tilgjengelig fra Leverandørportalen
SDS	Sentralt Datasenter - Helse Sør-Øsst fellesregionale datasentre driftet av Sykehuspartner.
SHKR	Sentralt Hovedkommunikasjonsrom - Datarom etablert i kundens lokaler.
SOA	Service Oriented Architecture
SSH	Secure Shell - Applikasjonsprotokoll med kryptert kommunikasjon for tilgang til pålogging og kommandolinje på fjernstyrt klient/server
SSID	Service Set Identifier – trådløst nett
TAP	Test Access Point – kloning av nettverkstrafikk

Forkortelse / Begrep	Beskrivelse
UltraVNC	Fjernstyringsverktøy, tilgjengelig fra Leverandørportalen
VLAN	Virtual LAN - en måte for logisk inndeling av nettverk i separate broadcastdomener
VPN	Virtual Private Network – kryptert, privat nettverksforbindelse
WAN	Wide Area Network - i denne sammenhengen benyttet som termineringspunkt for VPN
WinSCP	Fjernstyringsverktøy tilgjengelig fra Leverandørportalen
X.509 OU	Standard for sertifikater benyttet i sammenheng med NAC for etablering av PC-klienter i riktig VLAN, hvor OU (organizational unit) attributtet benyttes for å identifisere sone

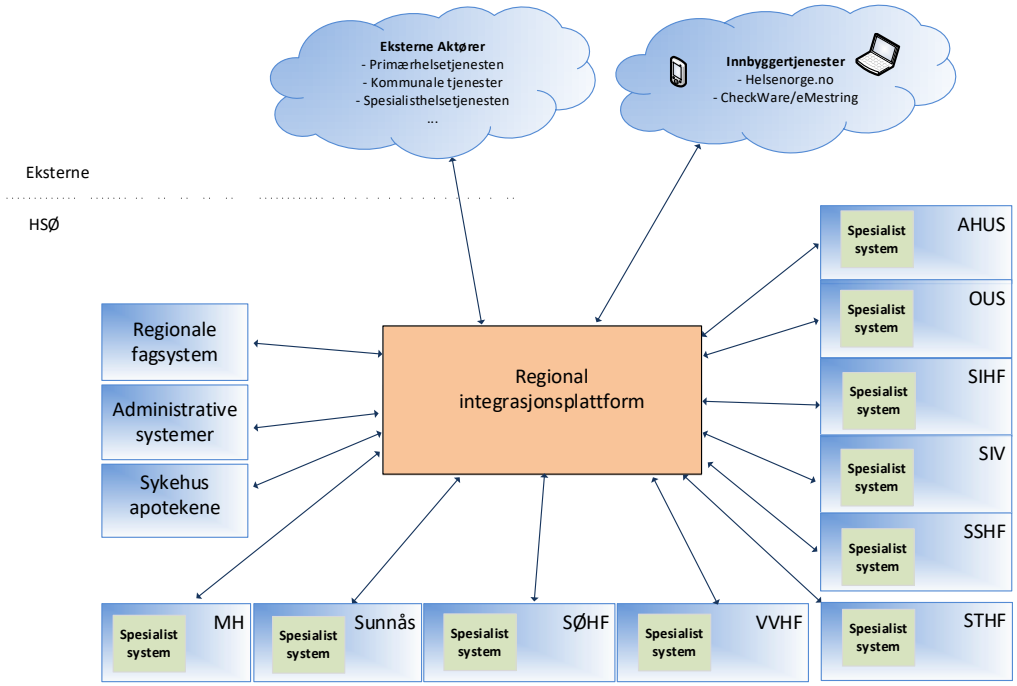
Sykehuspartner | HELSE SØR-ØST

Bilag D17 – Vedlegg D: Kundens tekniske plattform - Integrasjon

Innholdsfortegnelse

1 Integrasjon

For å sikre at den tekniske infrastruktur bygger opp under virksomhetsarkitekturen med fokus på tjenester, har Helse Sør-Øst etablert en SOA-Arkitektur for integrasjoner med Fagsystemer. Helse Sør-Øst har realisert SOA-Arkitekturen ved å etablere en regional integrasjonsplattform og en integrasjonspolicy. Integrasjonspolicyen legger klare krav og retningslinjer på hvordan integrasjoner skal etableres, og at disse skal gå gjennom integrasjonsplattformen. Den regionale integrasjonsplattformen består av ulike integrasjonsgrensesnitt, som skal gjenbrukes der det er mulig. Ved behov utvikles nye integrasjoner. Direkte kommunikasjon mellom to systemer skal unngås.



1.1 Regional Integrasjonsplattform

Regional Integrasjonsplattformen inngår som en viktig komponent i teknologi-laget i Helse Sør-Øst. Regionale Integrasjonsplattform består av ulike kapabiliteter. På de ulike kapabilitetene finnes det tjenester for administrative og kliniske områder. Kapabiliteter og tjenester vil endres og utvikles over tid.

2 Integrasjonskatalog

Integrasjonskatalogen er en overordnet oversikt over de integrasjonsområdene som er etablert på Regional Integrasjonsplattform. Beskrivelsen av den enkelte komponenten vil gi en indikasjon på hva som tilbys av ulike grensesnitt for å etablere en gitt integrasjon.

Integrasjonskatalogen er etablert i forbindelse med Integrasjonsoversikten i Helse Sør-Øst og blir vedlikehold i et eget register. Innholdet i dette dokumentet er derfor et utdrag av den totale listen slik at den inneholder det som er relevant for den enkelte anskaffelsen.

Domene	Område	Komponentbeskrivelse
Bestilling og Svar	Rekvisisjon	Rekvirering av lab undersøkelser skjer fra PAS/EPJ eller Primærhelsetjenesten gjennom Interaktive Henvisning og Rekvisisjon (IHR) til aktuelt lab system på helseforetaket. Siste tilgjengelige meldingsstandard fra eHelse for rekvisisjon er KITH Rekvisisjon 1.6.
Bestilling og Svar	Svar	Basert på elektronisk eller papirbasert rekvisisjon sendes foreløpige og endelig svarrapport tilbake til hoved og eventuelle kopirekvirenter. Siste tilgjengelige meldingsstandard fra eHelse for svar raport er KITH Svar 1.4
Bestilling og Svar	Apprec	Etter mottak av en KITH melding, skal disse kvitteres med en KITH Apprec 1.1 eller 1.0. Versjon av KITH Apprec avhenger av meldingstype og versjon. Apprec inneholder tilstrekkelig identifikatorer og behandlingsstatus slik at det er mottaker kan følge opp meldinger som ikke har kommet korrekt frem til mottakeren.
Bildebehandling	Overføring av bilder	Det er behov for å motta og sende radiologiske bilder fra MTU til kliniks bildelager og det spesifikke radiologi systemet på foretaket. Dette inkluderer også å hente ut allerede lagrede bilder basert på spørringer.
Brukertjenester	Innsynslogg	Applikasjoner med krav til innsynslogg, må tilby en tjeneste for å hente ut HL7 FHIR AuditEvent basert på FHIR profilen Norwegian Audit. Profile definerer at applikasjonen må være en actor AuditEvent Repository som betyr at applikasjonen må lagre Audit Event og tilby en tjeneste for uthenting. AuditEvent er definert i en nasjonal profil som enda ikke er godkjent. I påvente av dette kan man se på HL7 FHIR ressursen for AuditEvent[1].
Brukertjenester	PasientPåminnelse	For å skape en mer effektiv pasientbehandling og redusere andelen som glemmer å møte opp til oppsatt time, tilbyr integrasjonsplattformen mekanismer for å sende melding til bruker om oppsatt time. Standardvarsling for time er 3 dager frem i tid. Tjenesten benytter ekstern 3. part tjeneste for å sende SMS til brukeren. Tjenesten støtter foreløpig ikke tilbakemelding eller forespørsel om endring av time
EPJ	Klinisk Dokumentasjon	Kritisk informasjon og Cave finnes i dag både i PAS/EPJ og Kjernejournal. Det er et pågående arbeid for å etablere nødvendige prosesser og integrasjoner for å løfte disse tjenestene opp fra dagens bruk av DIPS API og DIPS Link Sensitiv View over til nasjonal tjeneste og ressurs basert på HL7 FHIR. Der vil prosess og samhandling mellom Kritisk Info og Cave og Kjernejournal bli beskrevet for de ulike relevante scenarier som blant annet inkludere ekstra informasjon på helseforetaket som ikke skal inn i Kjernejournal, og der bruker har valgt å reservere seg for Kjernejournal.
EPJ	Journal	PAS/EPJ er autoritativt datalager for de ulike journalnotater og dokumenter som oppstår i PAS/EPJ og andre RKL og spesialist applikasjoner. Alle dokumenter som skal sendes til eksterne partnere skal også sendes ut fra PAS/EPJ. PAS/EPJ tilbyr derfor et sett med tjenester for lagring og oppdatering av journalnotater og dokumenter, som må benyttes fra overføring av dokument fra spesialist system til PAS/EPJ. Formatet som benyttes er HL7 CDA via DocumentManager tjenesten.
EPJ	PasientLogistikk	PAS/EPJ er autoritativ kilde for pasient og administrasjon av pasient. Ved registreringer i PAS/EPJ relatert til planlegging av time, ankomstregistrering, overflyttinger, utskrivninger, poliklinisk til inneliggende pasient og motsatt og permisjoner, samt kanselleringsmeldinger for disse. Dette tilbys gjennom et bredt sett av HL7 v.2.x ADT (Admit Discharge Transfer) meldinger. Disse meldingene tilbys de som har et behov for dette, der tilsvarende behov ikke kan løses gjennom tjenestekall for PasientDemografi og Kontakt.
EPJ	Miniatyrbilde	Ved etablering av Regional MultimediaArkiv er det ønskelig med en tjeneste som kan hente ut et miniatyrbilde, både for visning i PAS/EPJ, men også for å lime inn i journal. Dette er en ny tjeneste, format og mekanisme er derfor ukjent. Tjenesten ønskes etablert på en internasjonal etablert standard, f.eks. HL7 FHIR.
EPJ	XDS-dokumentregister	Ved deling av informasjon kun med en dokumentreferanse, gjøres dette ved å registrere metadata om et gitt dokument i aktuelt dokumentregister via XDS. Applikasjonen som har registrert at den har følgene dokument, må da også tilby et sett med tjenester basert på XDS slik at andre kan hente selve dokumentet.
EPJ	Diagnose	PAS/EPJ er autoritativ kilde for blant annet pasientens diagnose. For enkelte spesialistsystemer er det hensiktsmessig å sende aktuell oppdatert diagnose tilbake til PAS/EPJ. Dette forutsetter at fagsystemet sitter på det samme diagnoseregisteret som PAS/EPJ slik at pasientens diagnose kan oppdateres med en gyldig verdi. Operasjonen for å sette Diagnose på pasienten er etablert som en tjeneste basert på HL7 FHIR Condition. Tjenesten støtter pt. kun å legge til og endre (slette og legge til ny) diagnose, men det er planlagt utvidelse for å kunne hente ut pasientens aktuelle diagnose i en senere versjon av tjenesten
EPJ	Prosedyre	I alle pasientbehandlinger så benyttes ulike prosedyrekoder. Både for intern bruk på foretaket og for å rette krav tilbake til Helfo gjennom BehandlerKravMeldinger (BKM). For spesialistsystemer som ikke sender egne BKM meldinger til Helfo, er det viktig at aktuelle prosedyrekoder blir registrert i PASS/EPJ. Dette forutsetter at fagsystemet sitter på det samme prosedyrekoderegisteret som PAS/EPJ slik at pasientens prosedyrekoder kan oppdateres med en gyldig verdi. Operasjonen for å sette Prosedyrekode på pasienten er etablert som en tjeneste basert på HL7 FHIR Procedure. Tjenesten støtter pt. kun å legge til og endre (slette og legge til ny) prosedyrekode, men

		det er planlagt utvidelse for å kunne hente ut pasientens aktuelle prosedyrekoder i en senere versjon av tjenesten
Kontakt og Time	Kontakt	PAS/EPJ tilbyr tjenestebasert grensesnitt for å hente ut planlagte, aktive og gjennomførte kontakter. Disse tjenestene vil bli tilbudt gjennom HL7 FHIR Encounter for å erstatte dagens tjenester som benytter HL7 v3 EncounterManager
Kontakt og Time	Arbeidsliste og Operasjonsplan	Består i dag av to tjenester. Den ene tjenesten returnerer operasjonsplan for en angitt pasient med intervall (+/- 24t). Den andre tjenesten henter ut operasjonsplan for en avdeling basert på angitt tidsintervall
Kontakt og Time	Timebooking	Timebok eksisterer i flere applikasjoner i hvert Helseforetak. Hovedtimebok ligger stort sett i PAS/EPJ, mens det også kan finnes parallelle timebøker i andre applikasjoner som f.eks. RIS. For å støtte applikasjoner og ulikt medisinsk utstyr som trenger timebøker finnes det noen integrasjonsgrensesnitt som kan understøtte melding om endringer timeboken. Dette gjøres stort sett i dag gjennom HL7 v2.x meldinger basert på SIU og noe ADT A05, men de har vesentlige mangler for å være komplett. For å hente ut aktuelle timer se IntegrasjonsKomponentPakken: Kontakt og Time-Kontakt.
Medikasjon	Medikasjon	Kurve er autoritativ kilde for medikasjonsdata. Denne informasjonen gjøres tilgjengelig for andre applikasjoner gjennom et tjenestebasert grensesnitt som vil tilbys via HL7 FHIR MedicationStatement og denne ressursen sin inkluderte FHIR Ressurser. Denne tjenesten skal erstatte den utgående tjenesten som i dag er eksponert på et leverandørspesifikt format.
Medikasjon	FEST (Felles Medikamentregister)	Løsning for forskrivnings- og ekspedisjonsstøtte (FEST). For å gi informasjon om legemidler og andre produkter som kan forskrives over resept er det etablert en nasjonal tjeneste for henting av varekatalog gjennom melding M30.
Pasient og Person	PasientDemografi	PAS/EPJ er autoritativ kilde for pasient og pasientdemografi, og tilbyr tjenester for å hente pasient, søke etter pasient og legge til pasient. Disse tjenestene vil bli tilbudt via et oppdatert grensesnitt basert på HL7 FHIR Patient som vil erstatte dagens tjeneste som benytter HL7 v3 PatientRegistry. Det finnes også tjeneste for å motta endringsmeldinger relatert til fletting, dødsfall og endring av navn og adresse via HL7 v2.x ADT (Admit Discharge Transfer) meldinger.
Pasient og Person	Folkeregister	Helse Sør-Øst regional plattform tilbyr sentralisert tjeneste for folkeregister. Tjenestene som tilbys er å hente ut pasient basert på kjent fødselsnummer eller søke etter person etter gitte søkeparametere. Disse tjenestene vil bli tilbudt via et oppdatert grensesnitt basert på HL7 FHIR Person som vil erstatte dagens tjeneste som benytter HL7 v3 PersonRegistry.

2.1 Standarder i Helse Sør-Øst

Oversikt over standarder som benyttes i Helse Sør-Øst, og hva som er bruksområdet til den enkelte standarden

Standard	versjoner	Status	Beskrivelse	Benyttes av
KITH	1.0 – 1.6	I produksjon	Er nasjonal standard for kommunikasjon med primærhelsetjenesten og offentlige etater, samt også mye brukt internt på foretakene	Rekvisisjon Svar Kvittering PLO Hodemelding m/vedlegg
HL7	v.2.5	I Produksjon	Internasjonal standard for helseinformasjon	PasientDemografi og logistikkmeldinger via ADT
HL7	v.3	I Produksjon	Via HL7.no er det etablert utvalgte implementasjonsguider for noen av v.3 ressursene	Pasient Person Kontakt
HL7	v.3 CDA	I Produksjon	Via HL7.no er det etablert utvalgte implementasjonsguider for noen av v.3 ressursene	DocumentManager
HL7	FHIR DSTU1	I Produksjon	Tjenestebaserte integrasjoner	Procedure Condition (Diagnose) DiagnosticOrder
HL7	FHIR DSTU2	Etableres	Nasjonal tjenesteprofil for bruk i applikasjoner med krav om innsynslogg	AuditEvent
HL7	FHIR DSTU2	Planlagt 2017	Fremtidig standard for etablering av tjenesteorienterte grensesnitt	Pasient Person Kontakt Appointment Schedule

				EpisodeOfCare Medication
IHE XDS	XDS.b	I Produksjon	Internasjonal standard for utveksling og deling av dokumenter	Dokument
Dicom	?	I Produksjon	Internasjonalt standard for sending, mottak og spørring etter bildemateriell og arbeidslister	Overføring av Bilder Finn Bilder Arbeidslister
Dicom Web	?	Planlagt ?	Internasjonalt standard for sending, mottak og spørring etter bildemateriell og arbeidslister. Mer moderne overføring av informasjon enn Dicom.	Overføring av Bilder Finn Bilder Arbeidslister
IHE XDS	XDS.i	Planlagt ?	Internasjonal standard for utveksling og deling av dokumenter relatert til bildemateriell	Bildemateriell og dokumenter
XACML SAML	2.0	I Produksjon	Attributt basert tilgangskontroll	Authlink

Sykehuspartner | HELSE SØR-ØST

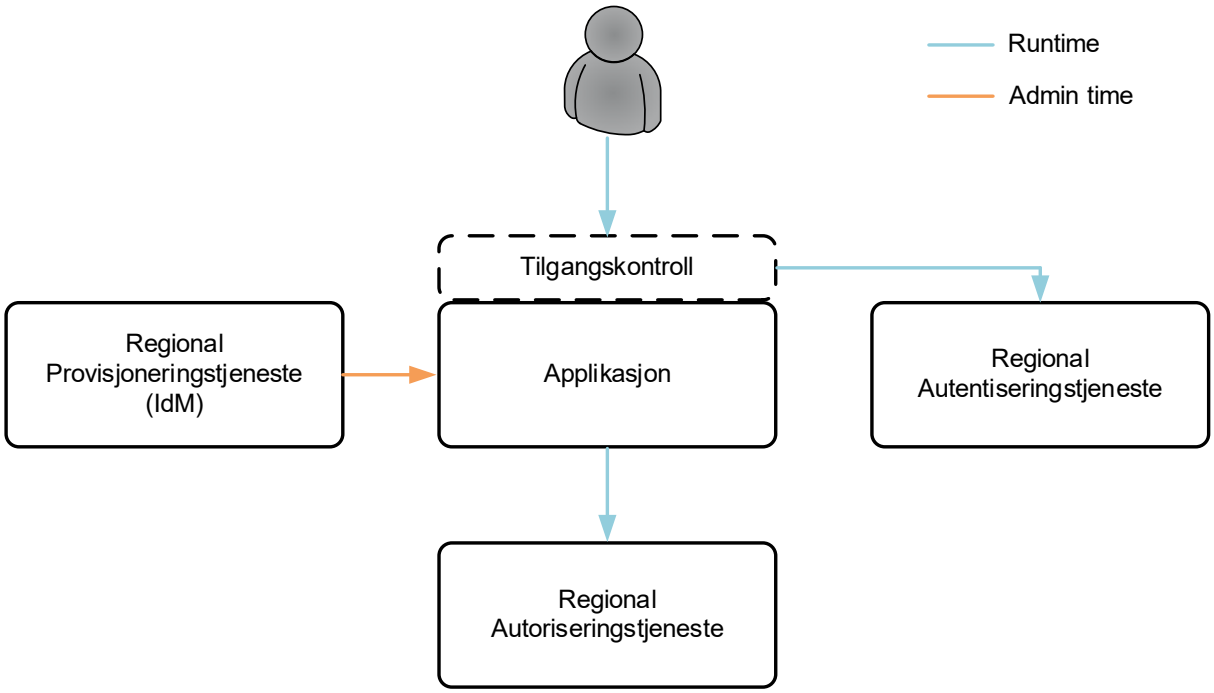
Bilag D17 – Vedlegg E: Kundens tekniske plattform – Identitet og tilgangsstyring

Innholdsfortegnelse

1 Identitet og tilgangsstyring

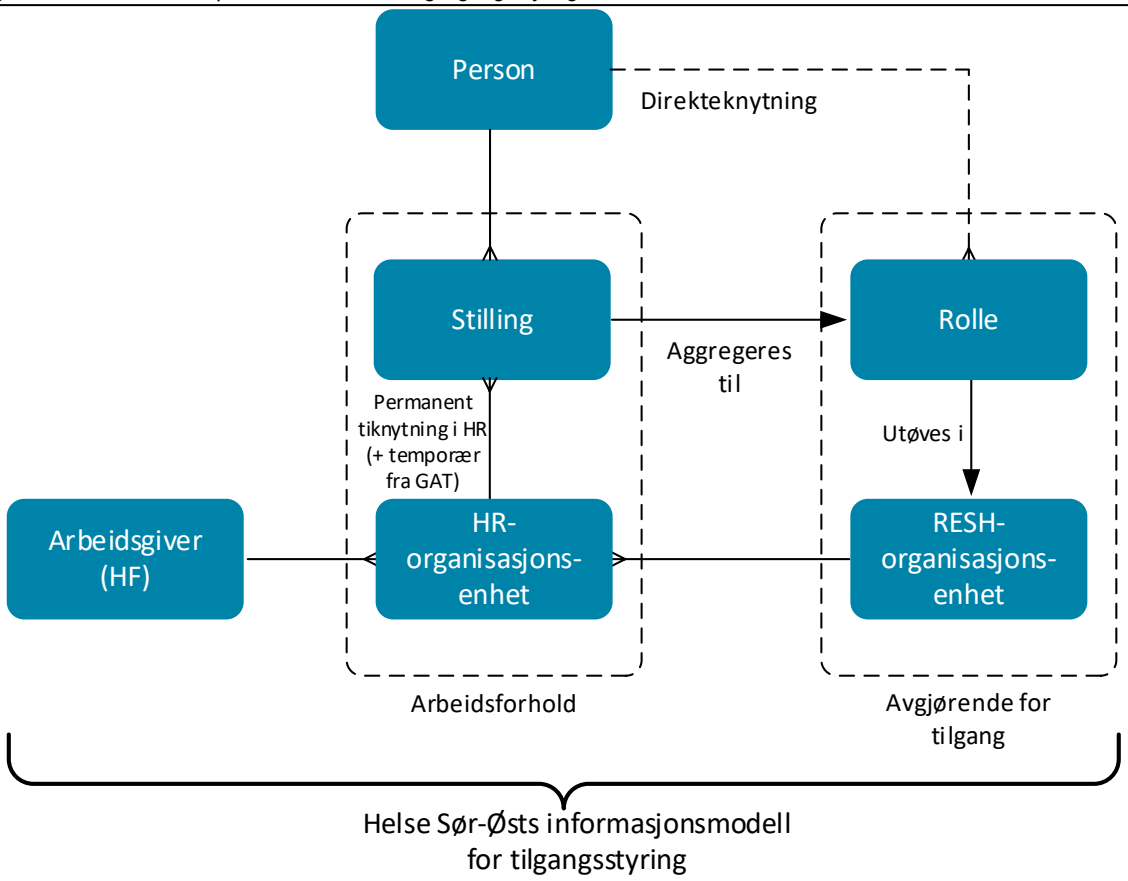
Identitet- og tilgangsstyring (IAM) i Helse Sør-Øst består av flere komponenter og tjenester, men de tre viktigste tjenestene er Regional Provisjoneringstjeneste, Regional Autentiseringstjeneste og Regional Autoriseringstjeneste. Disse tjenester er helt avhengige av og dermed integrert med autoritative informasjonskilder og prosesser.

Regional provisjoneringstjeneste benyttes til å provisjonere nødvendige brukerattributter til applikasjoner som har intern brukerdatabase. Applikasjonen håndterer selv brukersesjon mot applikasjonen og sørger for at bruker autentiserer seg med Regional Autentiseringstjeneste. Applikasjonen spør Regional autoriseringstjeneste om tilgang dersom intern tilgangskontrollmekanisme ikke kan avgjøre tilgang.



Figur 1, overordnet topologi - IAM for applikasjon

Helse Sør-Østs informasjonsmodell for tilgangsstyring baseres på personers arbeidsforhold (kan ha flere), aggregert/tilordnet rolle og organisasjonstilknytninger, hvor de to sistnevnte er avgjørende for tilgang.



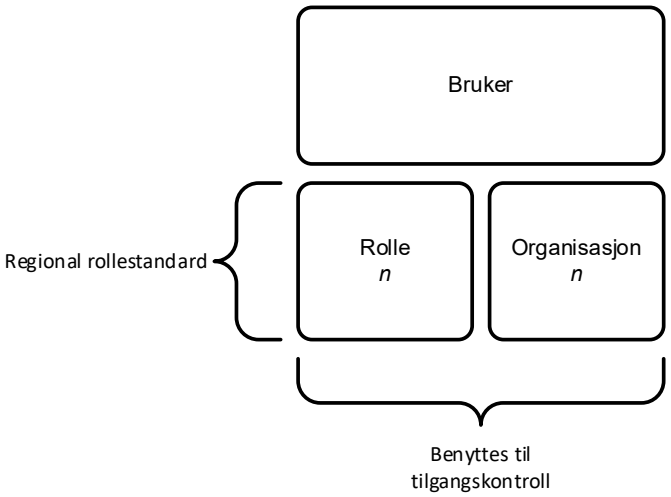
Figur 2, informasjonsmodell for tilgangsstyring

2 Regional provisjoneringstjeneste (IDM)

Dersom systemet/applikasjonen krever dedikert brukerdatabase må regional provisjoneringstjeneste benyttes for å administrere brukere og tildele tilganger i applikasjonen. Gitt det store antallet ansatte i Helse Sør-Øst er dette helt nødvendig for å automatisere og sentralisere brukeradministrasjonen. Det er en målsetning om å oppnå en automatiseringsgrad på 80% for tildeling av tilganger. Automatisering for fjerning av tilgang skal være tilnærmet 100%. Dette oppnås med at tjenesten er integrert med informasjonskilder beskrevet senere.

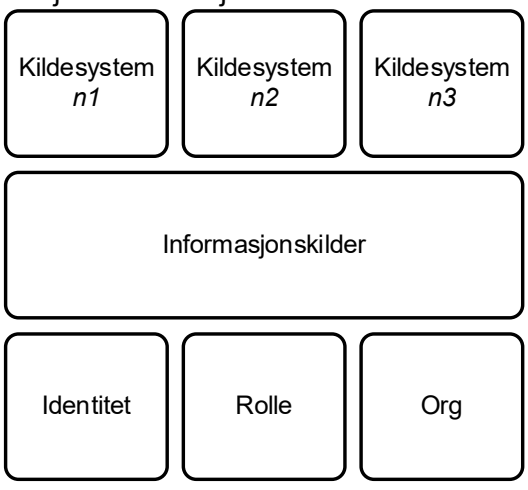
Regional provisjoneringstjeneste er en regional implementasjon av Quest One Identity Manager, som inneholder den sammenstilte metakatalogen med informasjon, regler (policy) og logikk for hvordan provisjonering av brukere foretas til applikasjonene. Eksempelvis AD og Exchange, men også kliniske applikasjoner som DIPS (EPJ) og Medikamentell Kreftbehandling (MKB). REST-API basert på SCIM-standarden er foretrukket som provisjoneringsgrensesnitt.

Applikasjonene benytter sammensetningen av tre forskjellige attributter for å gi tilgang til applikasjonen. Brukerident (brukerid), rolle (fra Regional rollestandard) og organisasjon (RESH) er de påkrevede attributtene for entydig identifisering av bruker.
Brukere tildeles én eller flere roller og org-tilknytninger i applikasjonen for å støtte at én og samme bruker kan ha flere arbeidsforhold og/eller roller i samme helseforetak (HF) eller på tvers av helseforetak. Merk at rolle og org-tilknytninger ikke aggregeres, hverken internt i samme HF eller på tvers av HF. Bruker opptrer kun i én kontekst per sikkerhetssesjon. Det er mulighet for å gi brukere individuelle utvidede roller.



Figur 3, rolle og org

Informasjonskilder:
Viktige attributter for å muliggjøre provisjonering, autentisering og autorisering kommer fra ulike informasjonskilder. Informasjonskildesystemene er autoritative for sin informasjon og tilgjengeliggjør nødvendige attributter for IAM-tjenestene. Eksempel på slik informasjon er identitets-, rolle-, og organisasjonsinformasjon.

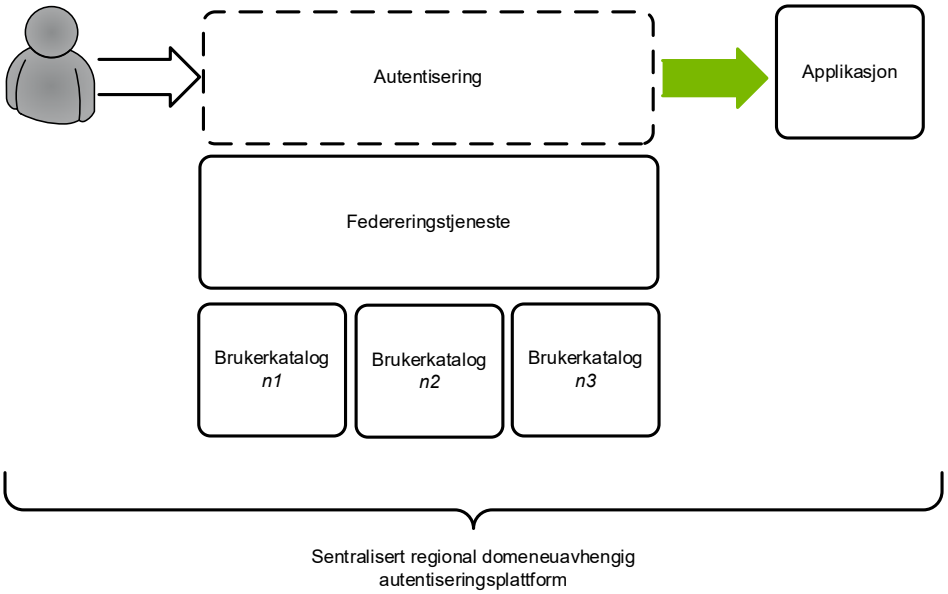


Figur 4, Informasjonskilder

Regional provisjoneringstjeneste benytter en rekke informasjonskilder for å innhente informasjon om ansatte og organisasjonsstruktur. Det regionale HR-systemet Personalportalen (PAGA) benyttes som primærkilde for ansattidentiteter i HSØ. Andre viktige informasjonskilder er de nasjonale registrene RESH (Register for enheter i spesialisthelsetjenesten) og HPR (Helsepersonellregisteret), og lokal installasjon av GAT (turnusplanlegging) på hvert enkelt helseforetak. Private/ideelle sykehus' HR-system er også en informasjonskilde som provisjoneringstjenesten benytter før de gis tilganger på regional plattform.

3 Regional autentiseringstjeneste (ID-FED)

Applikasjonene benytter Regional autentiseringstjeneste for autentisering. Løsningen er en sentralisert regional domeneuavhengig autentiseringsplattform som består av en federeringstjeneste. Dette muliggjør bruk av kun én brukerid på tvers av Helse Sør Østs helseforetak, noe som øker kontrollen samtidig som det gir økt brukervennlighet -ingen behov for å huske flere brukerkontoer og passord samt muligheten for single sign-on. Kilde til autentisering er Active Directory internt, men autentisering av eksterne partnere og borgere gjøres basert på offentlig godkjent nivå 4-autentisering..



Figur 5, autentisering

Autentiseringstjenesten sørger for sikker overføring av identitetsinformasjon som støtter opp under Single Sign-On mot applikasjonene ved å utstede et sikkerhetstoken. Sikkerhetstokenet inneholder nødvendige attributter for å gi initiell autorisering til å bruke applikasjonen. Produktet som benyttes er PingFederate og standardene SAML og OpenID Connect støttes for federering.

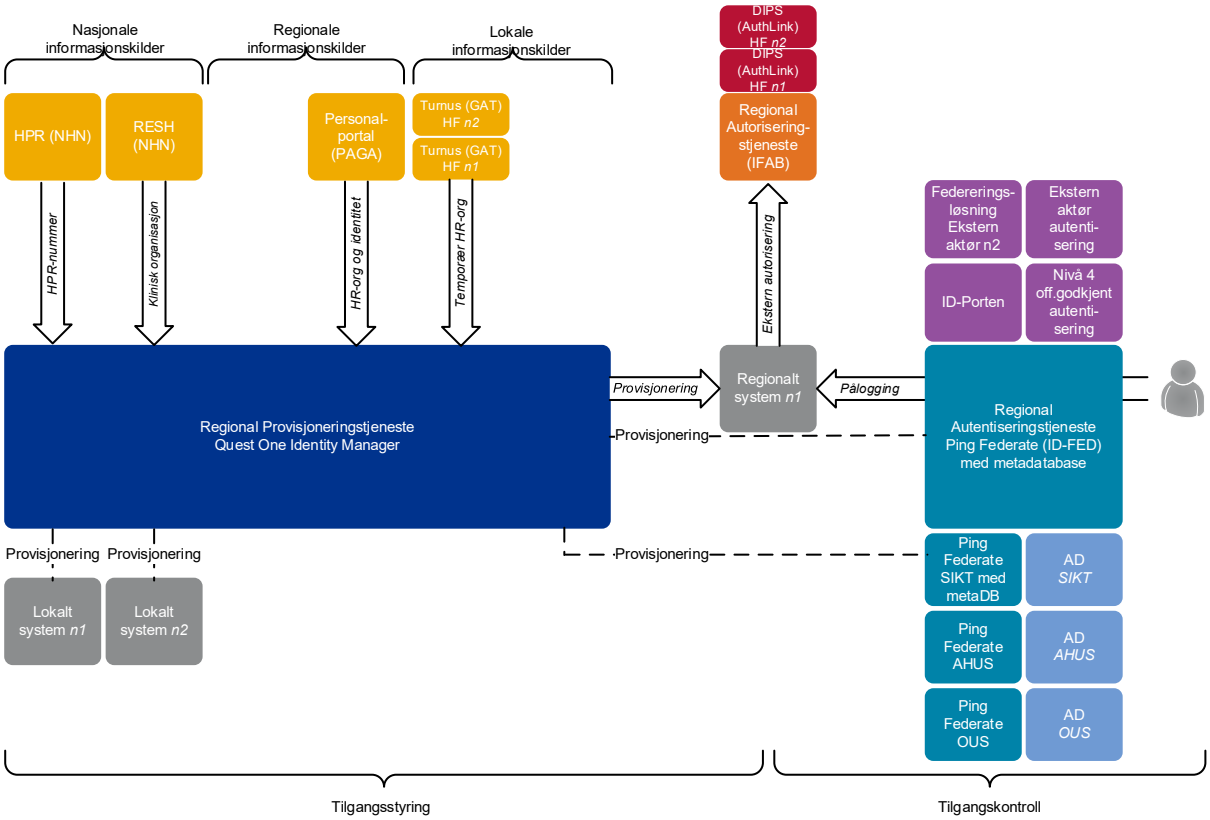
4 Regional Autoriseringstjeneste

For å etterleve sikkerhetskrav er autorisering nødvendig. Det er autoriseringen som avgjør hva sluttbruker får tilgang til i applikasjonen og systemet mht. funksjonalitet og data, eksempelvis hva sluttbruker kan utføre av arbeid (funksjoner) på hvilke pasienter (data).

Hver enkelt klinisk applikasjon gir selv implisitt tilgang til brukeren basert på valgt rolle og organisasjonstilknytning under pålogging og interne tilgangskontrollmekanismer (autorisering). Det er altså rollen og organisasjonstilknytningen som avgjør hva brukeren har implisitt tilgang til i en applikasjon. Det samme tilstrebes for administrative applikasjoner.

Dersom applikasjonen ikke kan avgjøre tilgang internt må Regional autoriseringstjeneste benyttes for å gi/avgjøre tilgang. Tjenesten er i dag en begrenset dynamisk autoriseringstjeneste basert på XACML for kliniske systemer som kan avgjøre om det finnes en aktiv behandler/pasient-relasjon for brukeren, gitt at pasienten er registrert i PAS/EPJ-systemet DIPS.

Komponentoversikt i figur:



Figur 6, IAM-komponentoversikt