SYKEHUSET I VESTFOLD

Informasjonssikkerhet - Kravspesifikasjon ved anskaffelser av MTU-løsninger med IKT-grensesnitt og tilkobling til nettverk

Gjelder for: []
Dokumenttype: Sjekklister
Sist endret: 20.09.2019

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 mer omfattende svar (>100 ord) som utdypes/dokumenteres i vedlegg. 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.*

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.

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. Hvis alternative løsningsforslag endrer prisbildet har vi en utdyping 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] Med "angitte» menes kravpunkter som Oppdragsgiver i utgangspunktet ikke har markert som uaktuelle fra sin side med kombinasjonen: «N» og «I/A»

SYKEHUSET I VESTFOLD

Informasjonssikkerhet - Kravspesifikasjon ved anskaffelser av MTU-løsninger med IKT-grensesnitt og tilkobling til nettverk

Gjelder for: []

Dokumenttype: Sjekklister

Sist endret: 20.09.2019

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), 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**			

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)
1.2	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 eventuelle behov for ekstern dataaksess. **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**			
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 overvåkes 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.	**B**			
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. Den tilbudte løsningen bør ha tydelige og veldokumenterte lisensieringsmekanismer. For Oppdragsgiver er det viktig å få vite hvorvidt det benyttes lokal lisensfil/sertifikat/dongle, eller dedikert lisensserver (intern/ekstern).

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)
	De etterfølgende kravpunktene besvares kun hvis den tilbudte løsningen inneholder lisensieringsmekanismer. **Merknad**: Uaktuelle kravpunkter besvares med «N» i kolonnen «Svar» og «I/A» i kolonnen «Utdyping».	**C**			
2.1	Den tilbudte løsningen bør ha tydelige og veldokumenterte lisensieringsmekanismer hvor eventuelle leverandørspesifikke tekniske krav og konsekvenser av disse er entydig dokumentert. **Merknad**: Leverandøren bes utdype hvorvidt det benyttes tidsbegrenset lokal lisensfil, sertifikat, dongle (USB, RS232, RJ45 e.l.) eller dedikert lisensserver (intern/ekstern).	**BCD**			
2.2	Den tilbudte løsningen bør ha tydelige og veldokumenterte rutiner for forvaltning og vedlikehold av lisens/sertifikat. Eksempler på viktige utdypingsområder er: • Hvordan aktiveres/deaktiveres tidsbegrenset lisens/sertifikat • Hvordan utføres versjonering av lisens/sertifikat	**BCD**			
2.3	Leverandøren bør på en oversiktlig måte utdype eventuelle begrensninger i bruk av løsningen som er en konsekvens av lisensieringsmekanismen. Eksempler på viktige utdypingsområder er begrensninger av teknisk eller funksjonell art: • i antall brukere • i antall tilkoblede enheter • lagringsvolumer • ved overskridelser av lisensgrenser	**BCD**			

3 NETTVERK

Sykehuspartner er i dag Oppdragsgiver sin leverandør av nettverksinfrastruktur med tilhørende nettverkskomponenter som svitsjer, rutere, brannmurer, fysisk kabling 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 (RJ45/Ethernet, RS232, 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 benytte IPv6 dersom den tilbudte løsningen har ekstern datautveksling over Ethernet med Oppdragsgivers systemer.	**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)
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 MDD 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: MDD og/eller CE? • 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**			

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)
3.7	Hvis den tilbudte løsningen implementerer dataoverføring basert på trådløs kommunikasjon bør det benyttes standard teknologier/protokoller (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**			
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.	**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)
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**			
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**			

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)
4.4	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**			
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 2012 R2 på servere, men dette skal endres til Windows 10 og Windows Server 2016. 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 2014 og Oracle Enterprise R12.

Enkelte av helseforetakene i HSØ benytter RES One Suite fra RES (res.com) for styring og sikring av klientarbeidsflater, inkludert tilgjengeliggjøring av klientapplikasjoner med alle tilhørende plugins/3.partskomponenter. Distribusjon av applikasjoner gjøres hovedsakelig via APP-V, alternativt via SCCM.

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)
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**			

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)
5.5	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 MDD, 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**			

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)
5.12	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 MDD, CE etc.	**B**			
5.13	Oppdatering av malwaresignaturer på *servere* bør skje automatisk. **Merknad**: Utdyp eventuelle krav til manuell oppdatering av malwaresignaturer.	**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**			

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)
5.20	Den tilbudte løsningens tilhørende klientapplikasjon(er) bør være kompatibel med Oppdragsgivers bruk av RES One 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 MTU. MTU skal beskyttes mot eksterne trusler, sykehusnettet og annet MTU. Sykehusnettet skal på sin side beskyttes mot MTU.

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/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
- Veileder i personvern og informasjonssikkerhet - medisinsk utstyr - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr

- «Normen» (på Engelsk) - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/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 som navn, fødselsnummer, rekvisisjonsnummer, diagnose, prøveresultat og lignende på permanent basis 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, i dag benyttes Bitlocker krypterte lagringsenheter 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)
	Kravpunktene under **skal** fylles ut hvis den tilbudte løsningen skal generere, prosessere eller lagre personopplysninger over 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**			
6.1	Leverandøren skal utdype de relevante avvik på lover og regler for informasjons- eller pasientsikkerhet som den tilbudte løsningen eventuelt har. **Merknad**: Oppdragsgiver er pålagt å etterleve Direktoratet for eHelse sin «Norm for informasjonssikkerhet» («Normen»).	**BCD**			
6.2	Leverandøren bør utføre nødvendige tilpasninger for å håndtere, og lukke eventuelle avvik kostnadsfritt for Oppdragsgiver innen et avtalefestet tidspunkt.	**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**			

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)
6.5	Individuell brukerautentisering bør gjøres mot grupper definert i Active Directory via LDAP. **Merknad**: Utdyp hvorvidt en LDAP 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. **Merknad**: Utdyp hvordan krav til tilgangskontroll og kryptering er tenkt ivaretatt i den tilbudte løsningen.	**BCD**			
6.7	Den tilbudte løsningen bør støtte rollebasert og eller beslutningsstyrt tilgangsstyring. 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 passord som kan hentes direkte fra brukermanualer eller annen form for tilgjengelig dokumentasjon.	**BD**			
6.10	Ved eventuelt behov for ekstern lagring eller videreformidling av person- eller pasientsensitiv data, bør den tilbudte løsningen benytte krypterte USB-lagringsenheter fra IronKey.	**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)
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	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**			

[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)
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 all integrasjon og samhandling internt i helseforetaket, mellom helseforetak og med eksterne aktører. Denne plattformen inneholder standardiserte integrasjonstjenester, basert på internasjonale og nasjonale meldingsstandarder. Eksempler på slike standarder er HL7, KITH og DICOM (DICOM er standard for MTU-kommunikasjon mot RIS / PACS). Eksempler på kjente og benyttede kommunikasjonsprotokoller er HTTP(S), FTP, SFTP/FTPS, CIFS.

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**			
8.3	Utveksling av medisinsk informasjon (HL7, KITH, DICOM, ASTM eller lignende) 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, CIFS, SMTP, SOAP (HTTP/HTTPS), MSMQ, DICOM.	**BC**			
8.4	Den tilbudte løsningen bør benytte integrasjon og informasjonsutveksling uten at det stilles leverandørspesifikke krav eller begrensninger til hvilke meldingsformater som kan benyttes Eksempler på slike formater er: XML, CSV, DICOM	**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. Eksempler på slik semantikk er: ASTM, HL7, ebXML, KITH.	**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)
8.6	Den tilbudte løsningen bør ha mulighet for logging av meldingsflyt og meldingskvitteringer ved bruk av integrasjonstjenester. **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**			

9 IKT-RELATERT DRIFT OG FORVALTNING

Helse Sør-Øst har standardisert på fjernaksess gjennom løsninger fra F5 BigIP og Citrix. Oppdragsgiver tilbyr i dag en standard fjernaksessløsning for alle eksterne utstyrsleverandører. Den benevnes «Leverandøraksess» og skal benyttes for all leverandørspesifikk drift og forvaltning der det ikke forutsettes personlig oppmøte i Oppdragsgivers lokaler. For å kunne bruke denne løsningen må Leverandør kunne benytte web-plugin for SSL VPN og Citrix Receiver web-klient på sine PC-er. Leverandøren får da tilgang til en aksesserver hos Oppdragsgiver, hvor nødvendig programvare og/eller fjernstyringsprogram mot MTU-klient/-server gjøres tilgjengelig. All bruk av fjernaksessløsningen skal knyttes til 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**			
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*. Bruk av egendefinert intern leverandøraksess med løsninger som 3G/4G- eller ADSL-modem, samt programvare som TeamViewer, LogMeIn etc. tillates *ikke* av Oppdragsgiver.	**BCD**			
9.2	Det bør kun være behov for leverandørtilgang til *tekniske produksjonslogger* for support. **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	Løsningens datalagrende enheter som kan inneholde personopplysninger bør benytte *«service tilgang» eller «service user modus»*, hvor opplysninger skjules/anonymiseres ifm. Leverandørbistand av den tilbudte løsningen.	**BD**			
9.5	Den tilbudte løsningen bør inneholde funksjoner for logging og lagring av loggdata. **Merknad**: Utdyp hvorvidt det benyttes logging til Windows EventLog, loggfiler, databaser, SNMP traps etc.	**BC**			
9.6	Den tilbudte løsningen bør logge og lagre tekniske hendelser eller feil.	**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)
9.7	Den tilbudte løsningen bør logge og lagre brukeroperasjoner (brukeraktivitet inklusiv uautorisert, eller forsøk på uautorisert, bruk).	**BD**			
9.8	Den tilbudte løsningen bør gi autoriserte brukere hos oppdragsgiver tilgang til logger gjennom et standardisert brukergrensesnitt. **Merknad**: Utdyp hvordan logger tilgjengeliggjøres.	**BC**			
9.9	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**			

Informasjonssikkerhet - Kravspesifikasjon ved anskaffelser av MTU-løsninger med IKT-grensesnitt og tilkobling til nettverk

Gjelder for: []

Dokumenttype: Sjekklister

Sist endret: 20.09.2019

Forkortelser og begreper

Begreper	Beskrivelse
3G/4G-modem	USB-modem benyttet til 3G/4G GSM-kommunikasjon
AD	Active Directory – Microsofts katalogtjeneste for autentisering og autorisering av brukere innenfor et Windows domene
ADSL	Asymmetric Digital Subscriber Line - linje for dataoverføring via kobberkabel/telefoninett
API	Application Programming Interface, grensesnitt for integrasjon
ASTM	Standardiseringsorgan for internasjonale standarder, bl.a. innenfor labkommunikasjon.
Bluetooth	Teknologi for trådløs kommunikasjon
CIFS	Common Internet File System - protokoll for fil-share
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	System som ivaretar særskilte funksjoner innen ett eller flere fagfelt. Eksempelvis LIMS eller EPJ
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

Begreper	Beskrivelse
IEEE 802.1x	Standard for autentisering av maskinvare tilkoblet nettverk. Må ikke forveksles med standarder for trådløst nett (WLAN).
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)
KITH	Standard for meldingsutveksling av klinisk og administrativ informasjon mellom helserelaterte informasjonssystemer
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
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
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
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

Begreper	Beskrivelse
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
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