**Kravspesifikasjon**

**IKT- tjenester og Informasjonssikkerhet for MTU**

*Innholdsfortegnelse*

[VIKTIG INFORMASJON 3](#_Toc44421973)

[*Formål* 3](#_Toc44421974)

[*Forklaring til skjema for kravspesifikasjon IKT-tjenester og Informasjonssikkerhet for MTU* 3](#_Toc44421975)

[*Oppdragsgivers bestemmelser gjeldende Leverandørens besvarelse* 3](#_Toc44421976)

[*Vurdering av kvalitet på dokumentasjon* 4](#_Toc44421977)

[1 Overordnet systembeskrivelse 5](#_Toc44421978)

[2 Lisenshåndtering 9](#_Toc44421979)

[3 Nettverk 11](#_Toc44421980)

[4 Maskinvare 15](#_Toc44421981)

[5 Operativsystem og programvare 16](#_Toc44421982)

[6 Informasjonssikkerhet og TILGANGSSTYRING 20](#_Toc44421983)

[7 Backup 24](#_Toc44421984)

[8 Integrasjoner 25](#_Toc44421985)

[9 IKT-RELATERT DRIFT OG FORVALTNING 27](#_Toc44421986)

[*Forkortelser og begreper* 32](#_Toc44421987)

|  |
| --- |
| 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).  Løsninger som skal tilknyttes datanettverk skal risikovurderes før de settes i drift.  Alle løsninger blir risikovurdert etter Helse Sør-Østs [Sikkerhetsprinsipper og -krav for IKTinfrastruktur og applikasjoner](https://www.helse-sorost.no/Documents/Informasjonssikkerhet%20og%20personvern/Styringssystem%20for%20informasjonssikkerhet/Regionalt%20styrende%20dokumenter/Styrende/NO-19%20-%20Sikkerhetsprinsipper%20og%20-krav%20for%20IKT-infrastruktur%20og%20applikasjoner.pdf).  Dette dokumentet baseres på ovennevnte sikkerhetsprinsipper, men er en forenklet utgave med hensikt å vurdere tilbudt løsning.  SØHF er pålagt å følge Direktoratet for e-Helse sin Norm for informasjonssikkerhet.  Dette dokumentet er inndelt etter [Veileder i personvern og informasjonssikkerhet -medisinsk utstyr - ehelse](https://ehelse.no/normen/veiledere/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr) i Norm for informasjonssikkerhet.  Veilederen kategoriserer medisinsk utstyr (MU) slik:   1. Frittstående MU, herunder:    1. Frittstående MU uten lagring.    2. Frittstående MU uten lagring, med utskrift på papir.    3. Frittstående MU som lagrer i et internt arkiv. 2. Frittstående/nettverkstilkoplet MU som viser sanntids pasientdata. 3. Nettverkstilkoplet MU som henter arbeidsliste (worklist) med pasientidentifikasjon over nettet. 4. Nettverkstilkoplet MU som lagrer data/rapport både eksternt og internt.     I tabellen på de neste sidene er det krysset av for hvilken av de fire kategoriene av medisinsk utstyr kravet gjelder for.  Oppdragsgiver har i dette dokumentet utformet kravene som ”obligatorisk”, ”bør”, ”redegjør” og ”informasjon”. Dette kommer frem i egen kolonne hvor det enten vil stå ”O”, ”B”, ”R” eller ”I”.  **O - Obligatorisk krav**. Leverandør som svarer nei, skal avvises. Leverandør må møte dette kravet for å være med videre i konkurransen. Kravet vil ikke bli evaluert blant tildelingskriteriene.  **B – Bør krav**. Kravet er et ønske og svarene fra leverandør vil bli evaluert.  **R- Redegjøre.** Leverandør skal gi en grundig beskrivelse/redegjørelse av kravet. ”R”. Leverandør som ikke redegjør for de ulike kravene, kan bli trukket i poeng i evalueringen.  **I - informasjon.** Informasjon fra oppdragsgiver til leverandør. |

| Overordnet systembeskrivelse SØHF kravspesifikasjon | | | | | | | | Leverandørens besvarelse | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nr | Kravbeskrivelse | Kravet gjelder for | | | | | Krav | Svar | Utdyping |  |
|  |  | 1 | 2 | 3 | 4 | (O, B, R, I) | |  |  |  |
| 1 | **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. | X | X | X | X | O | |  |  |  |
| 1.2 | Dersom løsningen benytter eksterne tjenester, f.eks. skylagring, skal tilbyder fremlegge detaljert løsningsdesign, systemdokumentasjon og dataflyt. Sikkerhetstiltak må fremkomme. |  |  |  | X | O | |  |  |  |
| 1.3 | Leverandøren skal ikke gjøre endringer i produksjonssatte løsninger uten at dette er nærmere avtalt med Oppdragsgiver. Leverandør må følge rutiner for endringer. | X | X | X | X | O | |  |  |  |
| 1.4 | Leverandøren bør sikre at produsentens anbefalinger følges ved sikkerhetsoppdatering av programvare, konfigurasjon, kodeverk, nomenklatur eller andre registre for å ivareta den tilhørende endringsprosessen på tilbudt løsning. | X | X | X | X | B | |  |  |  |
| 1.5 | Vedlikeholdsavtaler og oppdateringer bør gjelde alle komponenter i løsningen hvis ikke annet er avtalt. Redegjør. | X | X | X | X | B/R | |  |  |  |
| 2 | **Lisens** |  |  |  |  |  | |  |  |  |
| 2.1 | Lisenser bør ikke distribueres via lisens-dongler. | X | X | X | X | B | |  |  |  |
| 2.2 | Beskriv hvilke lisenser som inngår i tjenesten. | X | X | X | X | R | |  |  |  |
| 3 | **Nettverk** |  |  |  |  |  | |  |  |  |
| 3.1 | Den tilbudte løsningen bør benytte standard teknologier/protokoller for kablet datatrafikk, hvis aktuelt.  Beskriv løsningsens tilbudte teknologi og spesifiser eventuelle krav til nettverk. |  | X | X | X | B/R | |  |  |  |
| 3.2 | Den tilbudte løsningen bør benytte standard teknologier/protokoller for trådløs datatrafikk, hvis aktuelt.  Beskriv løsningsens tilbudte teknologi og spesifiser eventuelle krav til nettverk. |  | X | X | X | B/R | |  |  |  |
| 3.3 | Løsningen bør kunne settes i Oppdragsgivers segmenterte nettverk. Beskriv løsningens begrensninger i bruk av VLAN og segmentering. |  | X | X | X | B/R | |  |  |  |
| 3.4 | Den tilbudte løsningen bør benytte kryptering ved overføring av personopplysninger. Beskriv sikkerhetstiltak i datakommunikasjon. |  |  |  | X | B/R | |  |  |  |
| 3.5 | Den tilbudte løsningen bør håndtere brudd i nettverkskommunikasjon. Beskriv tiltak for kontinuitet. |  |  | X | X | B/R | |  |  |  |
| 4 | Maskinvare |  |  |  |  |  | |  |  |  |
| 4.1 | Leverandørens tilbudte serverløsning (hvis aktuelt) bør implementeres på virtuell serverplattform som kan leveres av Oppdragsgiver. |  |  |  | X | B | |  |  |  |
| 4.2 | Leverandørens tilbudte løsning bør kunne implementeres på IKT-klient levert av Oppdragsgivers. Beskriv krav til IKT-klient. | X | X | X | X | B/R | |  |  |  |
| 4.3 | Periferutstyr bør kunne leveres av Oppdragsgiver. Beskriv krav til preriferutstyr. | X | X | X | X | B/R | |  |  |  |
| 4.4 | Den tilbudte løsningen bør kunne skrive ut til Sikker Print/FollowMe-print. |  |  |  |  | B | |  |  |  |
| 5 | Operativsystem og programvare |  |  |  |  |  | |  |  |  |
| 5.1 | Spesifiser all programvare i alle komponenter i løsningen. | X | X | X | X | R | |  |  |  |
| 5.2 | Beskriv hvilken programvare som kan leveres av Oppdragsgiver. Spesifiser hvilken programvare i løsningen som ikke inngår i tilbudet. | X | X | X | X | R | |  |  |  |
| 5.3 | Oppdatering av programvare bør kunne gjøres av Oppdragsgiver. Beskriv oppdateringsrutiner og -krav for programvaren, herunder behov for administratorrettigheter. | X | X | X | X | B/R | |  |  |  |
| 5.4 | Tilbudt programvare bør sikres mot skadevare.Spesifiser hvordan programvaren sikres mot skadevare, gjennom eksempelvis herding og kryptering.All programvare skal beskrives. | X | X | X | X | B/R | |  |  |  |
| 5.5 | Spesifiser begrensninger i bruk og oppdatering av basis sikkerhet, herunder antivirus, sikkerhetsoppdateringer etc. | X | X | X | X | R | |  |  |  |
| 5.6 | Sikkerhetsoppdateringer av OS og programvare mot skadevare bør leveres og oppdateres av Oppdragsgiver. | X | X | X | X | B | |  |  |  |
| 5.7 | All leverandørspesifikke programvare som inngår i den tilbudte løsningen bør ha mulighet for å meldes inn i Oppdragsgivers AD. |  |  | X | X | B | |  |  |  |
| 6 | Informasjonssikkerhet og tilgangsstyring |  |  |  |  |  | |  |  |  |
| 6.1 | Den tilbudet løsningen bør oppfylle kravene til innebygget personvern. Redegjør. ([Personvernforordningen, artikkel 25](https://lovdata.no/lov/2018-06-15-38/gdpr/a25)).  **Dette kravet vektlegges høyere.** |  |  | X | X | B/R | |  |  |  |
| 6.2 | Tilgang til informasjon i tjenesten skal kun gis til den som har tjenslig behov og tilgangsrettighetene skal tilpasses den enkelte bruker/rolle. Beskriv hvordan tjenesten ivaretar dette. ([Norm for informasjonssikkerhet, Veileder tilgangsstyring](https://ehelse.no/normen/veiledere/veileder-tilgangsstyring)) |  |  | X | X | B/R | |  |  |  |
| 6.3 | Administratortilgang bør være basert på individuelle brukerkontoer.  Beskriv tilgangsrettighetene til opplysninger for administrator-brukere. |  |  | X | X | B/R | |  |  |  |
| 6.4 | Den tilbudte løsningen bør være tilrettelagt for effektiv brukerforvaltning. Beskriv brukerforvaltning og hvordan kravene til autorisasjonsregister er ivaretatt. ([Norm for informasjonssikkerhet, faktaark 47](https://ehelse.no/normen/faktaark/faktaark-47-autorisasjonsregister)) |  |  | X | X | B/R | |  |  |  |
| 6.5 | Beskriv sikkerhetsfunksjonalitet ved pålogging, herunder mulighet for tilknytning til AD, kryptering av passord og tofaktor-autentisering. |  |  | X | X | R | |  |  |  |
| 6.6 | Kommunikasjon over åpne nettverk, f.eks. ved bruk av skytjenester, skal løsningen tilby PKI-løsning på høyeste sikkerhetsnivå. ([Norm for informasjonssikkerhet, faktaark 49](https://www.ehelse.no/normen/faktaark/faktaark-49-krav-ved-bruk-av-pki-ved-ekstern-kommunikasjon)) |  |  |  | X | O | |  |  |  |
| 6.7 | Den tilbudte løsningen skal logge behandling av personopplysninger. Beskriv hvilken informasjon som blir logget ved behandling av personopplysninger. Beskriv også hva som ikke blir logget. ([Norm for informasjonsikkerhet, faktaark 15](https://ehelse.no/normen/faktaark/faktaark-15-logging-og-oppfolging-av-logger)) |  |  | X | X | B/R | |  |  |  |
| 6.8 | Den tilbudte løsningen skal logge systemhendelser- og endringer. Beskriv hvilken informasjon som blir logget av tekniske hendelser og ved systemteknisk arbeid i løsningen. Beskriv også hva som ikke blir logget. ([Norm for informasjonsikkerhet, faktaark 15](https://ehelse.no/normen/faktaark/faktaark-15-logging-og-oppfolging-av-logger)) | X | X | X | X | B/R | |  |  |  |
| 6.9 | Den tilbudte løsningen må sende driftsalarm ved stans til sentralt alarmmottak. Beskriv alarmløsninger. |  |  |  | X | O/R | |  |  |  |
| 6.10 | Logg skal være sikret mot endringer. Beskriv hvordan logg er sikret. ([Norm for informasjonsikkerhet, faktaark 15](https://ehelse.no/normen/faktaark/faktaark-15-logging-og-oppfolging-av-logger)) | X | X | X | X | B/R | |  |  |  |
| 6.11 | Den tilbudte løsningen bør ha funksjonalitet for skjerming/sperring av tilgang til personopplysninger for enkeltbrukere og grupper av brukere. ([Norm for informasjonssikkerhet, Veileder tilgangsstyring](https://ehelse.no/normen/veiledere/veileder-tilgangsstyring)) |  |  |  | X | B | |  |  |  |
| 6.12 | Løsningen bør ha funksjonalitet for automatisert sletting av personopplysninger når disse er prossesert eller bekreftet overført til fagsystem. |  | X | X | X | B | |  |  |  |
| 7 | Backup |  |  |  |  |  | |  |  |  |
| 7.1 | Den tilbudte løsningen bør ha baskup. Beskriv løsningens muligheter for backup av hhv systemdata og personopplysninger, herunder mulighet for full/inkrementell backup, sentralisert/automatisert backup og gjenoppretting . |  |  | X | X | B/R | |  |  |  |
| 8 | Integrasjoner |  |  |  |  |  | |  |  |  |
| 8.1 | Den tilbudte løsningen bør inkludere API eller tekniske løsninger for å tilpasses en Integrasjonsløsning basert på internasjonale stanrdarder, eksempelvis: Webservice, fileksport/import, WCF, HL7, DICOM. |  |  | X | X | B | |  |  |  |
| 8.2 | 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. |  |  | X | X | B | |  |  |  |
| 8.3 | Beskriv integrasjonene og hvilke sikkerhetsmekanismer som innbygget i overføring av data. |  |  | X | X | R | |  |  |  |
| 9 | Leverandør |  |  |  |  |  | |  |  |  |
| 9.1 | Leverandør bør benytte Oppdragsgivers tilbudte fjernaksessløsning. *Kravet gjelder kun hvis elektronisk fjerntilgang er aktuelt.*  **Dette kravet vektlegges høyere.** |  | X | X | X | B | |  |  |  |
| 9.2 | Beskriv hvilke informasjonstyper leverandør har tilgang til ved feilsøking. | X | X | X | X | R | |  |  |  |
| 9.3 | Behandling av personopplysninger bør ikke skje utenfor EU. Beskriv hvordan personopplysninger behandles ved uttrekk til leverandør, eksempelvis om det utleveres opplysninger til USA eller tredjeland. | X | X | X | X | B/R | |  |  |  |