

Prosjekt:

Sykehusprosjektene i Oslo

Tittel:

Bilag D16U

Prosedyre for IKT-grensesnitt for funksjonsutstyr

01	For implementering		05.03.25	ELG	ENE	DAB
Rev.	Formål med utgivelsen		Rev. Dato	Utarbeidet	Kontroll	Godkjent
Kontraktor/leverandørs logo:		Bygg nr:	Etasje nr.:	Systemgr.:		Antall sider:
						Side 1 av 12
Prosjekt:	Utgivernr:	Fag:	Dok.type:	Løpenr:	Rev.nr.:	Status:
HSØ	0000	U	SP	0021	01	G

Revisjonsendringer

Rev.:	Beskrivelse av endring

Innholdsfortegnelse

1	Formål	3
2	Innledning.....	3
3	Begreper	3
3.1	Integrasjon	3
3.2	IKT-infrastruktur	3
3.3	IKT-plattform.....	4
4	Kartlegging av leverandørens behov for IKT-tjenester	4
4.1	Ansvar IKT infrastrukturkoordinator	4
4.2	Leverandørens ansvar	5
4.3	Håndtering av grensesnitt IKT-infrastruktur- og IKT-plattform	6
5	Vedlegg - definisjoner	7

1 Formål

Formålet med prosedyren er å beskrive ansvarsforhold og samspill med hensyn på identifisering, avklaring/koordinering, implementering og testing av IKT-grensesnitt. Dette gjelder både IKT-infrastruktur (nettverk), IKT-plattform (servere, klienter) og IKT-integrasjoner (mellom ulike systemer internt i leveransen og mot andre entrepriser).

2 Innledning

Oppdragsgiver skal på vegne av de lokale helseforetakene og den regionale IKT-leverandøren Sykehuspartner HF etablere Helse Sør-Øst sin felles infrastruktur for IKT i de nye sykehusbyggene. Dette for å:

- Sikre funksjonelt samspill mellom ulike systemer, funksjoner og utstyr
- Ivareta krav til informasjonssikkerhet, tilgjengelighet og pålitelighet
- Oppnå en optimal drift- og vedlikeholdssituasjon gjennom enhetlige systemer og dokumentasjon

3 Begreper

3.1 Integrasjon

Integrasjon omfatter informasjonsintegrasjon, infrastrukturintegrasjon og teknisk integrasjon.

Informasjonsintegrasjon - informasjonsutveksling mellom ulike systemer. Dette avklares bilateralt med andre entrepriser/kontrakter, eller med ulike tilpasningsprosjekter i regi av Oppdragsgiver. Det skal benyttes standardiserte løsninger (industrielle, de facto), i den grad det er mulig. Oppdragsgiver vil organisere ulike tilpasningsprosjekter som vil integrere byggeprosjektets leveranser med Helseforetakets systemløsninger.

Infrastrukturintegrasjon definerer hvordan de enkelte systemer forholder seg til bruk av felles infrastruktur mht. IKT-rom, kabling, nettverk, IT-sikkerhet (brannmurer), IKT plattform og leverandøraksess.

Teknisk integrasjon definerer integrasjon mellom funksjonsutstyr og tekniske systemer som for eksempel SD-anlegg.

3.2 IKT-infrastruktur

Samspill mellom systemer forutsetter at de kommuniserer over en felles infrastruktur (kabel/nettverk). Infrastruktur omfatter etablering av felles infrastrukturelementer som kommunikasjonsrom, kabling, nettverk, samt fellessystemer som telefoni, meldingsformidling, Intranett osv.) med tilhørende felles IT-sikkerhetsfunksjoner.

Den felles infrastruktur for IKT består bl.a. av:

- Sentrale hovedkommunikasjonsrom (SHKR) med lokal datasenterfunksjon og Hovedkommunikasjonsrom (HKR) plasseres strategisk i bygningsmassen
- Lokale kommunikasjonsrom (KR)

- Strukturert kablingssystem (stamnett, og spredenett) basert på kobber og fiberoptisk kabel
- Nettverksløsninger (datanett – kablet og trådløst)
- Sikkerhetsløsninger (tilgang til nettverket, brannmurer mm.)
- Tjenester i nettverket
- Ekstern kommunikasjon (leverandør tilgang)
- Rack for plassering av servere, lagring og annet utstyr i SHKR, HKR og KR, inkl. kabling

Alle IT-systemer og tekniske systemer/installasjoner skal såfremt det er teknisk og av sikkerhetsmessige hensyn forsvarlig, bruke den felles infrastrukturen som blir etablert. Ingen aktører kan etablere egne løsninger for kabling og nettverk uten at det foreligger forhåndsgodkjennelse fra Oppdragsgiver.

Detaljert beskrivelse av IKT-infrastruktur i Helse Sør-Øst er angitt i vedlegg B, C og D i *Bilag C20U Grensesnitt*.

3.3 IKT-plattform

Med IKT plattform menes arbeidsstasjoner/mobile klienter, nettverk og serverløsninger. Alle systemløsninger vil være avhengig av sykehusets IKT-plattform som leveres og driftes av Sykehuspartner HF (SP). IKT-basisplattform består av følgende elementer:

- Maskinvare (fysiske og/eller virtuelle servere/arbeidsstasjoner/mobile klienter/lagringsløsninger)
- Operativsystem
- Basis programvare (antivirus, end system protection) og applikasjoner (Office mm)
- Katalogtjenester (for utstyr og brukere)
- IT-sikkerhetsløsninger
- Leverandørtilganger

Det henvises til vedlegg til vedlegg A-D i *Bilag C20U Grensesnitt*.

4 Kartlegging av leverandørens behov for IKT-tjenester

4.1 Ansvar IKT infrastrukturkoordinator

Byggherren benytter ressurser fra Sykehuspartner HF som IKT infrastrukturkoordinator.

IKT infrastrukturkoordinator skal koordinere og implementere de ulike aktørenes (entreprenører/leverandørers) behov og bruk av felles infrastruktur og IKT-plattform.

IKT infrastrukturkoordinator har ansvaret for å kartlegge de ulike systemenes bruk av infrastruktur (plassering i rom, kabel, nett, IKT-utstyr, samspill, mv.) og behov for IKT-plattform (mobile klienter, arbeidsstasjoner, servere). Koordinator har ansvar for å dokumentere og verifisere dette i forbindelse med installasjon og idriftsettelse. Dette skal sikre at nødvendig utstyr er installert og tilgjengelig med rett programvare (IKT-plattform), og at det er plass til utstyr, kabling og nettverkspunkter, når leverandøren skal installere og teste.

Infrastrukturkoordinator har bl.a. ansvar for å:

- Etablere et opplegg for koordinering av grensesnitt. Dette omfatter etablering av en systematikk for kartlegging, dokumentasjon, testing og godkjenning av hvert grensesnitt/leveranse inkludert av IKT-plattform (servere, arbeidsstasjoner, mobile klienter).
- Etablere en samlet oversikt over tjenester som vil være tilgjengelig i den felles infrastrukturen som grunnlag for kartleggingsarbeidet mot andre entreprenører/leverandører.
- Sørge for utarbeidelse av design for å levere de tjenester som det er behov for i hvert enkelt grensesnitt. I dette inngår å gjennomføre en risiko- og sårbarhetsvurdering av foreslått løsning i samarbeid med leverandør.
- Identifisere samspillet mellom ulike systemer mhp. protokoll, tjenester, tilgjengelighet og informasjonssikkerhet.
- Tildele plass til leverandørens utstyr i relevante kommunikasjonsrom iht. retningslinjer definert av Oslo universitetssykehus HF.
- Etablere et opplegg for å administrere/koordinere tilknytninger mot de(t) offentlige tele-/datanett slik at behov for eksterne tjenester blir tilfredsstillende dekket.
- Utføre eller få utført vha. andre all nødvendig patching i sprede-, stige- og stamnett (for både kobber og fiberoptisk nett).
- Utarbeide IP-adresseplan (IPv4 og IPv6), vedlikeholde denne og tildele IP-adresser til alle brukere av infrastrukturen. Sykehuspartner HF har ansvaret for å administrere både offentlige og private adresser.
- Utarbeide en navneplan for DNS, vedlikeholde denne og tildele DNS-navn til alle systemer som skal benytte den felles infrastrukturen.
- Utarbeide en katalogstruktur for brukere, IT-utstyr/periferiutstyr og tilgangsrettigheter til dette, etablere en katalogtjeneste og vedlikeholde denne i prosjektperioden samt overlevere denne til Sykehuspartner HF drift.
- Kartlegge bruk av frekvenser i byggeprosjektet, inkludert leveranser, samt holde denne oversikten oppdatert frem til overlevering. Identifisere og løse konflikter mhp. frekvenser og sendestyrke med andre eksisterende og planlagte løsninger i de nye byggene.

4.2 Leverandørens ansvar

Entreprenør/Leverandøren skal delta i kartleggingsmøter med Oppdragsgiver / Sykehuspartner HF slik at man i fellesskap kan finne frem til løsninger basert på kartleggingen beskrevet i kap 4.1, ref. vedlegg til *Bilag C20U Grensesnitt*.

Som utgangspunktet for kartleggingsarbeidet skal leverandøren fremskaffe forslag til systemdesign, ref. *Bilag D2U Prosjektgjennomføring funksjonsutstyr*.

Leverandørens systemdesigndokumenter skal oppdateres iht. omforent grensesnittsløsning med Sykehuspartner HF.

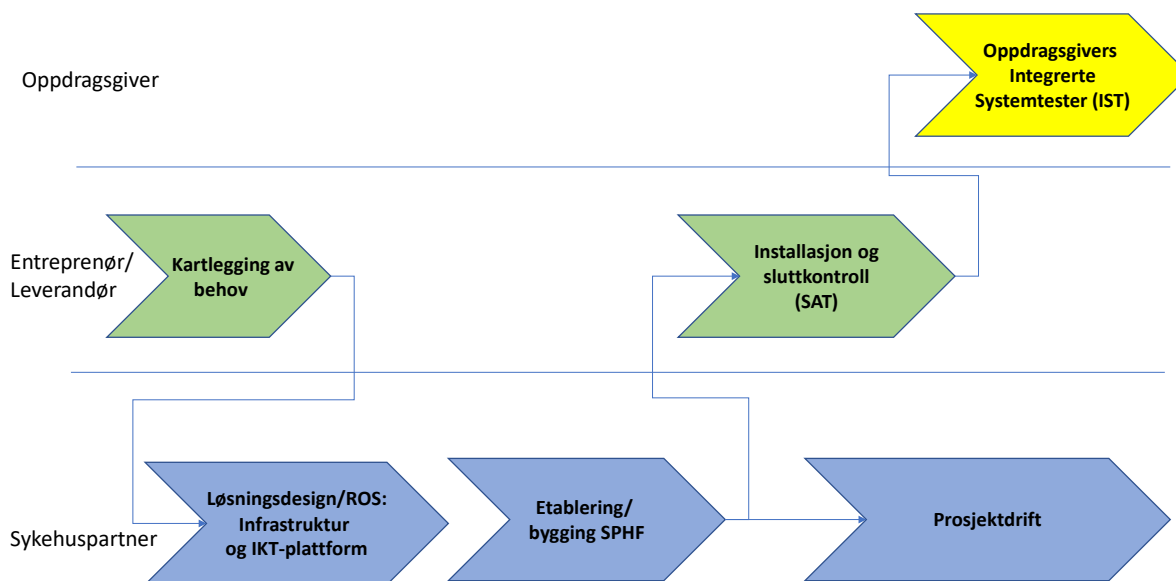
Ved endringer i etterkant av kartleggingen skal leverandøren uten opphold varsle infrastrukturkoordinator om dette slik at grensesnittsdokumentasjonen kan oppdateres iht. nytt omfang.

4.3 Håndtering av grensesnitt IKT-infrastruktur- og IKT-plattform

Implementeringen vil bli etablert gjennom følgende trinn, illustrert i [Figur 1](#):

- Kartlegging av behov:
 - Leverandørens tidsplaner vs. gjeldende fremdriftsplaner for prosjektet
 - kabling og plassering av utstyr i kommunikasjonsrom
 - nettverksbehov
 - klienter, servere
 - leverandøraksess
 - frekvensbruk mm.
 - integrasjoner
 - kommunikasjongsrensesnitt
- Løsningsdesign/ROS
Basert på kartleggingen vil SPHF utarbeide et løsningsdesign (LD) og gjennomføre risiko- og sårbarhetsvurdering (ROS)
- Etablering av løsning
Sykehuspartner vil etablere løsningen i nytt bygg iht. avtalt fremdrift
- Installasjon og sluttkontroll
Leverandør gjennomfører installasjon av sin løsning/utstyr og forbereder eventuelt grensesnitt mot helseforetakets applikasjoner, og gjennomfører sin sluttkontroll (SAT)
- Integrerte systemtester (IST)
Oppdragsgiver vil gjennomføre integrerte systemtester mellom leverandørens utstyr/systemløsninger og helseforetaket sine løsninger. Testene gjennomføres i samarbeid med Oslo universitetssykehus og Sykehuspartner. Leverandøren skal bidra i gjennomføring av tester
- Prosjektdrift
Etter at leverandør har verifisert at leveranser fra Sykehuspartner er i henhold til avtalt grensesnittsdokument, vil Sykehuspartner HF etablere en prosjektdrift som leverandøren kan henvende seg til dersom det oppstår feil i de avtalte leveransene fra Sykehuspartner HF

Behov for kabling og innplassering av utstyr i IKT-rom (Kommunikasjonsrom) meldes av leverandør til oppdragsgivers prosjektleder slik at dette kan videreformidles til byggeprosjektets prosjekterende.



Figur 1 – Prinsipp for gjennomføring

5 Vedlegg - definisjoner

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 helse relaterte 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)
Lagringsløsning	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-adresse/Port-range til en annen
Oppdragsgiver	I dette dokumentet benyttes dette som begrep for de(t) aktuelle helseforetak(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-services 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

	<ul style="list-style-type: none">· 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
Tjenesteleverandør	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 fjernaksesløsning
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