



ByggHaugesund2020

B03 OMBYGGING
IKT Plattform i Helse Vest
Krav til entreprenører og leverandører

Versjon: 0
Dato: 18.02.2021

Innhold

1	GENERELL INFORMASJON	4
2	SERVER, SYSTEMER OG KLIENTER.....	4
2.1	KLIENTER.....	4
2.2	KATALOGTJENESTE.....	4
2.3	SERVER OS OG VIRTUELISERING	4
2.4	SERVERBRUKERE	4
2.5	DATABASE.....	5
2.6	SIKKERHETSOPPDATERING.....	5
2.7	DOMENE/SIKKERHET:	5
2.8	LAGRING:	5
2.9	DOMENESTRUKTUR:	5
2.10	TEKNOLOGIER FOR HØY OPPETID:.....	5
2.11	SERVERNAVN:	6
2.12	LISENSIERINGSTEKNOLOGI:	6
2.13	SIKKERHETSKOPI (BACKUP):.....	6
2.14	SERVER UTEN PÅLOGGING:	6
2.15	PROGRAMVARE OG DRIVERE MÅ LA SEG AUTOMATISERE FOR INSTALLASJON:	6
2.16	AVHENGIGHETER TIL ANNEN PROGRAMVARE:	7
2.17	AVHENGIGHET TIL «END OF LIFE» PROGRAMVARE:	7
2.18	INSTALLASJON AV PROGRAMVARE:	7
2.19	ARBEIDSFLATE/KLIENT OPERATIVSYSTEM:	7
2.20	INGEN FRYSS AV SIKKERHETSKONFIGURASJON PÅ SERVER ELLER PC:.....	7
2.21	AKTIV FORVALTNING:.....	7
2.22	NETTLESER PÅ PC:	7
2.23	LOGGING/OVERVÅKING:	7
2.24	VPN:	7
3	NETTVERK:	8
3.1	KABLET NETTVERKSTILKOBLING AV UTSTYR:	8
3.2	TRÅDLØS NETTVERKSTILKOBLING AV UTSTYR:	8
3.3	IPV6:.....	8

3.4	TCP KEEP ALIVE:	8
3.5	NETTVERKSSONER:	8
3.6	REGISTRERING AV UTSTYR PÅ NETTVERKET:	8
3.7	BRANNMURÅPNINGER:	8
3.8	SWITCHER:	8
4	SIKKERHET:	9
4.1	NORMEN:	9
4.2	AUTENTISERING:.....	9
4.3	AUTOMATISK TIMEOUT:	9
4.4	SPORBARHET:	9
4.5	KRYPTERING:	9
5	GRENSESNIITT IKT:	10

1 GENERELL INFORMASJON

Dette dokumentet gir en oversikt over Helse Vest sin tekniske plattform som forvaltes og driftes av Helse Vest IKT.

Entreprenør, underentreprenør og leverandør må følge beskrivelser og krav som fremgår i dette dokumentet.

Entreprenør må gjennomføre planleggingsmøter i forkant av leveransen, sammen med Helse Fonna og Helse Vest IKT. Entreprenør er ansvarlig for å oppgi alle opplysninger som er nødvendig for å gjennomføre leveransen. Alt arbeid som må utføres i forbindelse til dette, må legges frem i planleggingsmøtet.

Entreprenør er komplett ansvarlig for leveransen. Entreprenør skal legge til rette og bistå Helse Vest IKT i sitt arbeid forbundet med leveransen.

2 SERVER, SYSTEMER OG KLIENTER

2.1 KLIENTER

Helse Vest kjører i dag på en Windows 10 plattform. Det tillates ikke installasjon av programvare lokalt på PC. Ingen brukere er lokal administrator, og programvare gjøres kun tilgjengelig sentralt via RES Workspace.

Til administrasjon, distribusjon og patching av programvare benyttes Microsoft System Center Configuration Manager og Microsoft App-V. Programmene pakkes i MSI/App-V format ved hjelp av AdminStudio.

Plattformen benytter lokal Windows brannmur og System Center Endpoint Protection (SCEP). Microsoft har introdusert tjenesten «Windows as a Service». Med denne tjenesten oppgraderer Microsoft plattformen sin oftere. Microsoft vil nå kun støtte de to siste hovedbuildene, og det er krav at entreprenør etterlever dette konseptet. Løsningen som entreprenør leverer, må vedlikeholdes slik at den til enhver tid er gyldig (fungerer) på en eller begge støttede Windows 10 versjoner.

2.2 KATALOGTJENESTE

Microsoft Active Directory (Function Level: Windows Server 2016), benyttes som katalogtjeneste.

Domenet består av ett tre og alle klienter og Windows servere er med i samme domene.

Microsoft Active Directory Certificate Authority er satt opp som intern sertifikat løsning og benyttes per i dag for VPN, Direct Access, Brukerautentisering (smartkort), interne SSL Web sider o.l.

2.3 SERVER OS OG VIRTUELISERING

På serversiden benyttes Microsoft som primær infrastruktur plattform. Vi forvalter også UNIX/Linux servere. På databasesiden benytter Helse Vest IKT dedikerte clustrete databaseløsninger som kjører på Microsoft SQL eller Oracle.

Serverparken til Helse Vest er virtualisert. Helse Vest IKT benytter VMware ESX som primær virtualiseringsplattform. Entreprenørens løsning må installeres på virtuell server i Helse Vest sin serverpark. Det tillattes ikke fysiske servere i entreprenørens leveranse.

Nye servere settes opp med:

- Windows Server 2016 R2 x64 (eller nyere)
- Oracle Enterprise Linux 6 x64 (eller nyere)

2.4 SERVERBRUKERE

Systemet må følge Helse Vest IKT sin standard for brukere og passord for servere.

Helse Vest IKT standard for serverbrukere og passord:

- Lokale brukere benyttes ikke i forbindelse med drift. Det skal benyttes domenebrukere eller servicebrukere
- Krav til bestemte navn på brukere tillates ikke.

- Kravene til bestemte passord tillates ikke.
- Passord må kunne endres periodisk.

Løsning som skal i drift skal ikke kreve annet enn normal brukertilgang på server. Krever løsningen andre rettigheter, må dette oppgis, og dokumenteres hvorfor.

2.5 DATABASE

Systemet/løsningen bør støtte en av følgende databaseteknologier for sentral lagring i database:

- MS-SQL 2016 med «Availability Groups»
- Oracle databaser: Oracle Enterprise Linux 6 OS, 12.x.x.x eller høyere

Alle databaser leveres på x64 teknologi.

Helse Vest IKT kan tilby sentral database til entreprenørens løsning.

Andre databaser og versjoner kan benyttes, men blir da ikke driftet sentralisert. Databasen vil da regnes som en delkomponent i systemet og falle inn under forvaltning av det ene systemet.

2.6 SIKKERHETSOPPDATERING

Alle servere, med tilhørende teknologi/programmer installert må kunne sikkerhetsoppdateres, uavhengig av løsning. Med dette menes:

- Operativsystem
- Databaser
- Antivirus

Andre systemkomponenter installert på server skal kunne få installert sikkerhetsfikser uavhengig av godkjennelse fra entreprenør av løsningen som kjører på server.

2.7 DOMENE/SIKKERHET:

- Microsoft serverne må være medlem av Helse Vest sitt domene, og kjøre under standard domene sikkerhetsinnstillinger. Avvik fra dette må oppgis, og entreprenør må detaljere hvordan avviket skal håndteres.
- Serverne har antivirusprogram og kjører "realtime" skanning, og løsningen må støtte at serverne har denne typen sikkerhet installert. Er entreprenøren kjent med at dette er et problem, må entreprenør oppgi avvik, og komme med forslag til hvordan dette håndteres.
- 3.parts drivere som skal installeres på servere skal være WHQL-godkjente (Windows Hardware Quality Labs-certified)

2.8 LAGRING:

Helse Vest IKT tilbyr ulike typer lagring. Entreprenørene må spesifisere hvilke egenskaper som er viktige for den lagringen løsningen trenger for å fungere. Her vil kapasitet, ytelse, spelling, snapshots og type lagring (block, cifs, objekt) være viktige parameter.

Det gjøres oppmerksom på at servere kjøpes inn fra egen innkjøpsavtale fra Sykehusinnkjøp, og derfor vil HW som kjøpes inn, endres over tid.

2.9 DOMENESTRUKTUR:

Helse Vest IKT domenestruktur består i dag av 1 domene i en skog(forest). Fuctional level er satt til 2016. Løsningen kan ikke kreve opprettelse av eget subdomene, eller endringer Schemainnstillinger til Helse Vest.

2.10 TEKNOLOGIER FOR HØY OPPETID:

Løsningene må selv besørge høy oppetid ved flere aktiv/aktiv servere.

Tradisjonelle clusterløsninger for maskinvare feiltoleranse støttes ikke i vårt virtuelle servermiljø. Helse Vest IKT tilbyr lastbalansering i forkant av servere i form av:

- Citrix Netscaler for generell lastbalansering.

På MSSQL databaser støttes høy oppetid med MSSQL Always On Availability Group.

På Oracle databaser støttes høy oppetid gjennom RAC/Dataguard.

2.11 SERVERNAVN:

Løsningen kan ikke ha krav til navn på server, og må kunne støtte alle gyldige hostnavn i de respektive operativsystemer vi støtter. Løsning må takle at servernavn endres.

2.12 LISENSIERINGSTEKNOLOGI:

Lisensiering av løsning må følge Helse Vest IKT sine krav for implementering av lisenser i plattformen.

Helse Vest lisensieringskrav:

- Løsningen skal kunne benytte lisensnøkkel.

Lisensieringen kan ikke benytte:

- Dongler
- MAC-adresser
- IP-adresser
- hostname

Dette ødelegger virtualiseringsstrategien til Helse Vest, og vanskeliggjør oppgradering av servere/klienter.

Kan ikke vanlig lisensnøkkel benyttes, må tilbyder levere en programvarebasert lisensløsning som ikke bryter med Helse Vest sine krav.

2.13 SIKKERHETSKOPI (BACKUP):

Helse Vest har krav til at det ikke skal ligge sensitive data på PC. PC-er blir ikke tatt backup av.

Helse Vest kjører image/snapshot-basert backup av servere. Sentrale databaser har vi også administrert backup av.

Data som skal tas backup av, og som ikke inngår i sentrale databaser, må systemet håndtere selvstendig, ved å legge data tilgjengelig i filsystemet for videre prosessering. Område som skal tas backup av må dokumenteres og bli kommunisert til Helse Vest IKT når løsningen implementeres.

2.14 SERVER UTEN PÅLOGGING:

Løsningen må kunne kjøre uten at en bruker er pålogget server.

Ved server omstart må løsningen selv starte opp, uten at man må logge på med bestemt bruker, og starte programmet. I utgangspunktet vil dette si at løsningen starter som en service på serveren.

2.15 PROGRAMVARE OG DRIVERE MÅ LA SEG AUTOMATISERE FOR INSTALLASJON:

Helse Vest distribuerer programvare og drivere sentralt. Det vil si at programvaren må la seg automatisere, slik at den er tilgjengelig på PC uten brukerinvolvering.

Helse Vest benytter App-V, SCCM og Ivanti Res Workplace for automatisering og distribusjon.

Helse Vest leverer automatisering på alle nivå, men har en preferert rekkefølge på teknologivalg for automatisering:

- App-V
- MSI
- Scriptet installasjon (svarfil)

- Setup, hvor bruker selv må svare. Regnes egentlig ikke som automatisering, men det lar bruker installere odde programvare på PC, uten å være lokal administrator. Denne siste løsninger sees på som en nødløsning, og er ikke ønsket i Helse Vest.

"Step by step" dokumentasjon for installasjon må foreligge.

2.16 AVHENGIGHETER TIL ANNEN PROGRAMVARE:

Har programvare avhengigheter mot annen programvare for å fungere må dette synliggjøres. Det kan ha innvirkning på valg av automatiseringsteknologi.

2.17 AVHENGIGHET TIL «END OF LIFE» PROGRAMVARE:

Entreprenøren må dokumentere en oppdateringsplan av systemet og komponenter systemet er avhengig av. Det må ikke brukes system/komponenter som er/eller kommer til å bli EOL innen levetiden til systemet.

Eksempler:

- Avhengigheter til gamle versjoner av Adobe Reader.
- Avhengig av Internet Explorer 6, 8, 9
- Avhengig av .Net 1.1
- MS-XML 4.x

2.18 INSTALLASJON AV PROGRAMVARE:

Installasjon av programvare må kunne foretas uten at Helse Vest må slå av gjeldene sikkerhetsinnstillinger.

Gjeldene sikkerhetsinnstillinger på PC:

- Antivirus
- GPO
- UAC
- Kunne kjøre uten lokal administrator.
- RES Workspace Manager

2.19

ARBEIDSFLATE/KLIENT OPERATIVSYSTEM:

Helse Vest benytter Windows 10. Som entreprenør er det derfor vesentlig å ha et aktivt forhold til «Windows as a Service».

2.20 INGEN FRYSS AV SIKKERHETSKONFIGURASJON PÅ SERVER ELLER PC:

Programvare må takle kontinuerlig sikkerhetsoppdatering av PC/server plattformen.

Entreprenøren kan ikke ha krav til frys av PC-er/serverer i en gjeldene sikkerhetskonfigurasjon. Løsningen må være robust nok til å takle sikkerhetsoppdateringer.

2.21 AKTIV FORVALTNING:

Helse Vest IKT har krav om at løsningen forvaltes aktivt, og at entreprenøren har et aktivt forhold til operativsystemoppgradering og kan levere løsningen på nytt OS innen rimelig tid etter at nytt OS er i markedet.

2.22 NETTLESER PÅ PC:

Gjeldene nettleter for Helse Vest er i dag Microsoft Edge.

Internet Explorer 11 og Chrome støttes også.

2.23 LOGGING/OVERVÅKING:

Løsningen må benytte server eller PC-ens eget hendelsessystem til å logge alle hendelser (informasjon, advarsler og feil) som det produserer.

2.24 VPN:

Dersom det er behov for fjerntilgang til servere og utstyr må Helse Vest sin VPN-løsning BOMGAR benyttes. Det tillates ikke å benytte andre løsninger for VPN. Informasjon om Helse Vest sin VPN-løsning: <https://helse-vest-ikt.no/brukerstotte/for-leverandorar#fjernaksess>

3 NETTVERK:

3.1

KABLET NETTVERKSTILKOBLING AV UTSTYR:

Nytt endepunksutstyr som skal kobles direkte i Helse Vest sitt nettverk må støtte Helse Vest IKT standard nettverkskonfigurerings:

- Støtte for IPv4
- DHCP (RFC2131)
- Helst støtte for 802.1x, alternativt MAB-autentisering.

Nettverket består av følgende soner:

- Ansattnett (klientutstyr)
- Teknisk nett (bygg teknisk utstyr)
- Medisinsk teknisk nett (medisinsk teknisk utstyr som er pasientnært)

3.2 TRÅDLØS NETTVERKSTILKOBLING AV UTSTYR:

Nytt endepunksutstyr som skal kobles direkte i Helse Vest sitt nettverk må støtte Helse Vest IKT standard nettverkskonfigurerings:

- Støtte for IPv4
- DHCP (RFC2131)
- Støtte for 802.1x (sertifikat)
- 5Ghz – 802.11 n/ac – WPA2-Enterprise -802.1x-autentisering vha. sertifikat (EAP-TLS)

Det trådløse nettet består av følgende soner:

- Gjestenett (benyttes av pasienter og pårørende)
- Ansattnett (benyttes av ansatte, vikarer og innleide i Helse Vest)
- Teknisk nett (bygg teknisk utstyr)
- Medisinsk teknisk nett (benyttes av trådløst medisinsk teknisk utstyr som er pasientnært)
- Voicenet (benyttes av trådløse IP-telefoner)

3.3 IPV6:

Helse Vest IKT har startet forberedelsene til overgang til IPv6, og alt utstyr som kobles til nettverket bør ha støtte for dette.

3.4 TCP KEEP ALIVE:

Helse Vest sin brannmur kobler bort oppkoblinger som den mener har vært inaktive i mer enn 30 minutter. Løsning må støtte «TCP Keep alive» for applikasjoner/utstyr som sender data gjennom en brannmur.

Utfyllende forklaring til krav:

For utstyr som settes opp med statisk (fast) IP adresse, opplever man ofte at det ikke sender ut "jeg er i live"-meldinger. Dette gjør at løsninger da havner i en del uforklarlige feilsituasjoner.

3.5 NETTVERKSSONER:

Nettverket til Helse Vest er sonet, med brannmur mellom sonene. Basert på løsning, kan forskjellige nettverkskomponenter bli plassert i forskjellige nettverkssoner.

Utstyr må støtte lag 3 i OSI modellen. I praksis vil dette si at utstyr må kunne kommunisere på tvers av subnet.

3.6 REGISTRERING AV UTSTYR PÅ NETTVERKET:

Alt utstyr som kobles til datapunkt må først registreres i Helse Vest sin utstyrsportal. Entreprenør er ansvarlig for å lage oversikt over alt utstyr som skal kobles til nettverket, og det må blant annet opplyses om leverandørens kontaktperson, utstyrsnavn og beskrivelse og MAC-adresse. Dette må utføres i god tid før utstyret skal kobles til nettverket.

3.7 BRANNMURÅPNINGER:

Entreprenør er ansvarlig for å lage oversikt over alle nødvendige brannmuråpninger knyttet til løsning og utstyr. Det skal blant annet opplyses om navn og beskrivelse av utstyr, protokoll, portnummer og kommunikasjonsendepunkt. Dette må utføres i god tid før utstyret skal kobles til nettverket.

Entreprenør er ansvarlig for eventuell feilsøking. Helse Vest IKT skal bistå i dette arbeidet.

3.8 SWITCHER:

Totalentreprenøren sine leveranser skal ikke omfatte egne nettverksswitcher. Utstyr skal tilknyttes sykehuset sine nettverksswitcher.

Det gis unntak fra dette kravet for bygg teknisk utstyr som leveres med internswitch. Internswitch må være av typen unmanaged. Det tillates ikke å tilknytte internswitch direkte til sykehuset sine nettverksswitcher, det må etableres IP-gateway mellom internswitch og sykehuset sine nettverksswitcher. IP-gateway må støtte nettverkskravene som beskrevet i dette dokumentet.

4 SIKKERHET:

Spesialisthelsetjenesten har sterke krav til sikkerhet i sine løsninger, som tilbyr og forvalter en viktig samfunnsfunksjon. Pasienter og pårørende skal være trygg på at dataene deres behandles trygt og konfidensielt, i tråd med de lover og regler som til enhver tid gjelder.

4.1 NORMEN:

Overordnet for sikkerhet i Helse Vest er nasjonale føringer som lover og forskrifter, med tilhørende Norm for Informasjonssikkerhet i helsesektoren. Denne har en rekke faktaark og veiledere som finnes på www.normen.no. Entreprenørens løsning må følge dette.

4.2 AUTENTISERING:

Alt IP utstyr og brukere skal autentiseres før de gis tilgang til nettverk.

Utstyr som skal benytte Helse Vest sitt nettverk skal være godkjent før det tas i bruk. Utstyrets MAC-adresse kobles til en IP-adresse, eller tar i bruk et godkjent sertifikat fra Helse Vest IKT.

Ved ekstern pålogging til et system skal Helse Vest sitt valgte to-faktors system benyttes. Alle systemer som krever ekstern pålogging, skal gjennomgå en ROS-analyse og godkjennes, før man kan ta det i bruk.

Active Directory:

Microsoft Active Directory Domain Services (AD) er autorativ for brukerkontoer i Helse Vest, og en løsning skal derfor kunne integreres mot AD. AD skal styre kontoene, og integreres mot løsningen.

4.3 AUTOMATISK TIMEOUT:

Inaktive brukere bør logges automatisk av løsningen. Tidsrammen for "timeout" bør være konfigurert for grupper, lokasjoner og enheter.

4.4 SPORBARHET:

- Systemet må kunne logge hendelser. Hvilke hendelser som skal logges bør være konfigurert.
Beskrivelsen av hendelsene må være nøyaktige og tydelige. Formålet med å spore hendelser vil være:
- Dokumentere uønskede hendelser
 - o Identifisere hendelsen
 - o Er det et problem (Flere instanser av samme hendelse)
 - o Korreksjon
 - o Dokumentasjon av hendelse og tiltak.
- Sikkerhet
- Revisjon
- Etterlevelse av lover og forskrifter
-
- Som et minimum bør følgende logges:
 - PC navn
 - Bruker ident
 - Bruker rolle
 - Tilgang til dokumenter
 - Dato og klokkeslett
 - Beskrivelse av hendelsen
 - Forsøk på å skaffe seg uautorisert tilgang

4.5 KRYPTERING:

For å sikre systemet mot innsyn, må systemet kunne sikre data under transport og oppbevaring.

Helse Vest sin strategi er at dette skal håndteres av systemet, det vil si at systemet skal kryptere dataene før de sendes og dekrypteres når de kommer frem. Alternativt kan krypteringen foregå på transportlaget.

5 GRENSESNITT IKT:

Byggherren har som målsetting å etablere integrerte IKT-systemer. Dette for å oppnå en optimal drift- og vedlikeholds situasjon gjennom enhetlige systemer og enhetlig dokumentasjon. Sentrale elementer i måloppnåelsen er integrering mellom systemer og etablering av felles infrastruktur.

Det skal etableres en felles IKT infrastruktur som skal benyttes av alle systemer og løsninger på sykehuset. Felles IKT infrastruktur inkluderer:

- Kobber og fiber i stam-, stige- og spredenett
- Datanett, fast og trådløst, inkludert tjenester som DNS, DHCP, brannmur, mv.
- Katalogtjeneste (AD)
- Serverplattform, inkludert tilhørende tjenester som lagring, backup, antivirus, overvåking mv.
- Klientplattform, inkludert pakking og distribuering av applikasjoner
- Telefoniplattformen
- Øvrige tjenester levert av Helse Vest IKT

Entreprenør må sikre at infrastrukturgrensesnitt løses til riktig tid og gir riktig funksjonalitet til grensesnittpartene.

Entreprenør er selv ansvarlig for å melde inn behov for IKT Infrastruktur til byggherren så tidlig som mulig. Entreprenør er ansvarlig for at det gjennomføres planleggingsmøte med byggherren, dette må utføres i god tid før leveransen. Dette skal inngå i entreprenørens tidsplan for leveransen.

Byggherren, sammen med sin driftsleverandør Helse Vest IKT vil tilby et sett basistjenester levert sentralt:

- Datanett, fast og trådløst, inkludert tjenester som
 - DNS
 - DHCP
 - NTP
 - Brannmur, mv.
- Katalogtjeneste (AD)
- Serverplattform, inkludert tilhørende tjenester
 - Lagring
 - Backup
 - Antivirus
 - Overvåking mv.
- Klientplattform
 - Pakking og distribuering av applikasjoner
- Telefoniplattformen
 - Nummerplaner
- Tilgangsstyring, inkludert fjerntilgang

Listen er ikke uttømmende, og vil videreutvikles. Det er entreprenør sitt ansvar å melde behov for slike tjenester så tidlig som mulig.

Følgende overordnede føringer gjelder:

- Helse Vest IKT skal stå for leveranse av virtuelle servere, inklusive server OS. Entreprenør skal ikke prise eller levere servere som kan dekkes med Helse Vests IKT sin plattform.
- Det påligger entreprenør å fremskaffe all relevant informasjon som byggherren etterspør i løpet av planleggingsfasen.
- Det er entreprenørens ansvar å avdekke og melde behov for IKT infrastruktur til byggherren i løpet av planleggingsfasen.

- Alt arbeid med grensesnittavklaringer, både mot byggherren og mellom egne leveranser, skal være inkludert i leveransen. Dette gjelder også nødvendig arbeid for å implementere og teste entreprenørens side av grensesnittet.