Helse Nord IKT

# IKT infrastruktur i Helse Nord

*Generelle krav for tilknytning til IKT infrastruktur i Helse Nord*

# Innholdsfortegnelse

# Versjonshistorikk

| Versjon | Dato | Ansvarlig | Endringer |
|---|---|---|---|
| 0.1 | 8. mai 2012 | Terje Bless | Første utkast |
| 0.1.1 | 13. mai 2012 | Terje Bless | Innarbeidet rettinger og mindre endringer fra HS |
| 0.1.2 | 07. november 2012 | Sveinung Fylkesnes | Innarbeidet rettinger og tilegg fra Server |
| 0.3 | 12. februar 2013 | Mats Kristensen | Laget del om lagring, samt endret litt ang. versjoner |

# Innledning

Helse Nord består av 11 sykehus, over 100 utelokasjoner, og over 10,000 ansatte. For å best mulig utnytte regionens felles IKT ressurser er Helse Nord IKT etablert som en felles IKT-driftsorganisasjon for hele regionen. All IKT-infrastruktur i regionen driftes og forvaltes av Helse Nord IKT, og etableres i et stordriftsregime utviklet for å mest mulig effektivt understøtte regionens kjernevirksomhet.

Dette medfører at leverandører av utstyr og systemer som har en IKT-komponent, eller som er avhengig av å virke i eller integreres mot, regionens IKT-infrastruktur må oppfylle en del generelle krav, samt levere en del standard dokumentasjon. Siden enkelte kategorier IKT-infrastruktur og IKT-utstyr skal leveres og driftes av Helse Nord IKT (e.g. nettverksutstyr, servere, og databaser) er det derfor kritisk at alle leverandører tydelig oppgir kompatibilitet med og behov for slike komponenter og tjenester, slik at et fullstendig og korrekt kostnadsbilde for tilbud løsning kan evalueres.

*Der en tilbudt løsning forutsetter bruk av tjenester som ikke er tilgjengelig som standard, eller typer eller versjoner av standardiserte komponenter, vil dette medføre en øket kostnad for regionen som vil måtte tas med i evaluering av aktuelt tilbud.*

Dokumentet tar kun for seg de mest allment anvendelige krav og en overordnet beskrivelse av regionens IKT-infrastruktur for å bistå prosjekter og leverandører med å tilpasse seg denne med minst mulig uforutsette hindringer. Der informasjon om et gitt emne ikke er tilgjengelig, eller er uklart, i dette dokumentet, må de nødvendige tiltakene for å innhente eller avklare nødvendige opplysninger påregnes.

# Generelle krav for IKT infrastruktur

## *1 Sikkerhet og lovkrav*

Helseforetakene i regionen er som en del av spesialisthelsetjenesten underlagt en rekke lover og forskrifter som er spesielt relevante for IKT-relaterte systemer og utstyr. Krav og rammer gitt i lovs form (herunder også forskrifter og eventuelle fortolkninger, og de forskjellige tilsynsmyndigheters forståelse av disse) kan normalt ikke fravikes i avtale. Det er derfor av avgjørende viktighet at leverandører av utstyr eller tjenester på dette området gjør seg kjent med disse.

I kontekst av IKT-infrastruktur er det mest relevante førende dokumentet *Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren*[1] ("Normen") og tilhørende Faktaark. Normen er "et omforent sett av krav til informasjonssikkerhet basert på lovverket." Ut over hvert enkelt Helseforetaks selvstendige ansvar for å virke innenfor rammene av sitt styringssystem for informasjonssikkerhet så er alle Helseforetak i regionen også forpliktet å etterleve Normen.

Løsninger eller utstyr som ikke er forenelig med disse kan ikke benyttes i Helse Nord.

## *2 Fjerntilgang*

All fjerntilgang til utstyr eller tjenester plassert i Helse Nords IKT-infrastruktur, og da særlig utstyr eller systemer som er pasientnære eller som er logisk plassert i et sykehus' sikrede sone, skal skje gjennom Helse Nords standard løsning for fjerntilgang. Denne løsningen består av en standard IPSec VPN klient (i "Remote Access" modus, ikke i "LAN to LAN" modus) som kobler opp til regionens VPN-mottak, samt en Citrix ICA-basert terminaltjenerklient som kobler opp til en dedikert terminaltjener for fjerntilgang. Fra VPN-klienten er det kun tilgang til nevnte terminaltjener og det er eksplisitt ikke tillatt med direkte IP forbindelse fra eksterne nettverk og til utstyr plassert i sikret sone. Både VPN og terminaltjener autentiseres med en personlig brukerkonto tildelt av Helse Nord IKT, og forutsetter undertegnet taushetserklæring.

Se for øvrig også Normen's "Veileder for fjernaksess".

## *3 Nettverk*

Regionens nettverk driftes av Helse Nord IKT.

Lokalnettverk (LAN) er basert på Ethernet og IPv4. Eksisterende nettverkspunkter har varierende grensesnitthastighet fra 10Mbps, 100Mbps, og 1000Mbps. Nye nettverkspunkter etableres som

[1] http://normen.no/

10/100/1000Mbps. Alle nettverkspunkter termineres i standard RJ45 modulærkontakter. Power over Ethernet (PoE) basert på IEEE 802.3af-2003 er tilgjengelig som standard på alle nettverkspunkter. Utstyr som skal knyttes til LAN må kunne fungere i henhold til denne standarden. PoE basert på IEEE 802.3at-2009 (”PoE+”) kan unntaksvis være tilgjengelig. Alle access-porter i LAN er satt opp med sikkerhetsfunksjonalitet som vil blokkere porten dersom ikke-tillatt trafikk eller oppførsel detekteres. Dette inkluderer, men er ikke begrenset til, mottak av BPDU’er, uautoriserte DHCP pakker, tilsynelatende looper, eller uautoriserte nettverksenheter (e.g. switcher el.).

Regionens WAN er basert på det norske Helsenettet (se http://www.nhn.no/ for mer informasjon) og applikasjoner og tjenester må til enhver tid forholde seg til de kvalitets- og funksjonelle egenskaper som er gjeldende for dette. Dette gjelder særlig egenskaper som roundtrip delay (”Latency”), Jitter, og pakketap. Aksesshastighet for de fleste sykehus er 1Gbps redundant, men denne båndbredden er delt mellom alle applikasjoner og tjenester.

QoS er ikke tilgjengelig eller støttet i regionens nettverk.

Multicast er ikke støttet i regionens nettverk.

Bruk av broadcast, ut over det som er normalt og forventet for IP-baserte applikasjoner, er ikke støttet i regionens nettverk.

IPv6 er ikke støttet i regionens nettverk.

Tildeling av IP-adresser for annet utstyr enn servere levert av Seksjon for servertjenester skjer dynamisk gjennom DHCP, men en fast IP adresse kan tilbyes gjennom reservasjoner i DHCP. Servere settes opp med fast IP adresse og DNS innslag (både A og PTR RR).

IP adresser i bruk er hovedsakelig RFC1918 adresser, men utstyr og tjenester må fungere med en blanding av private og offentlige adresser. IP adresseplan er i henhold til Helsenettets nasjonale IP plan.

All kommunikasjon over WAN, inkludert mellom lokasjoner innen samme helseforetak, krypteres på nettverksnivå med bruk av GET VPN (IPSec i Transport mode). Dette medfører at MTU og MSS ikke kan forutsettes å ha noen spesiell defaultverdi, og at nettverket kan transparent endre MSS verdien i pakker som traverserer nettverket.

All trafikk som forlater en lokasjon tvinges gjennom et sentralt demarkasjonspunkt og underlegges trafikkontroll, som hovedregel i form av en brannmur med ACL og protokollinspeksjon. ACL’er bygges opp slik at trafikk per default blokkeres, og kun eksplisitte porter og destinasjoner tillates. Protokollinspeksjon gjør at pakker som ikke er i samsvar med relevant standard vil forkastes. Det er derfor kritisk viktig at alle kommunikasjonsprotokoller som er i bruk i en gitt tjeneste eller utstyr dokumenteres nøye, med spesiell oppmerksomhet til at dokumentasjonen skal benyttes for å

utforme brannmurregler. En større range av dynamisk tildelte porter (e.g. diverse RPC-protokoller med en portmapper funksjon) tillates normalt ikke.

Direkte IP kommunikasjon ut over grensene for en juridisk enhet (i.e. et helseforetak) tillates ikke, og da spesielt ikke mot Internett eller andre eksterne nettverk. Direkte IP kommunikasjon mellom lokasjoner innenfor samme juridiske enhet (e.g. mellom sykehusene i samme Helseforetak) tillates etter Risikoanalyse dersom andre krav er oppfylt.

# *4 Server*

Maskinvare og operativsystem med tilhørende standard tjenester anskaffes, monteres, installeres, konfigureres, og driftes av HN-Ikt/ Seksjon for servertjenester. Type og spesifikasjon av maskinvare er standardisert i regionen, og utstyr monteres i et av regionens datarom (herunder i noen tilfeller i sentraliserte datasenter geografisk fjernt fra det aktuelle sykehus).

Nye installasjoner skal normalt gjøres på regionens standard virtualiseringsplattform (per dato VMWare vSphere 5.1) og systemer må derfor kunne fungere på en virtuell maskin hostet på denne plattformen. Der et system har spesiell krav til maskinvare eller ikke kan benyttes på virtualisert maskinvare må dette dokumenteres, egen godkjenning innhentes, og resulterende økte driftskostnader vil iberegnes totalkostnad for tilbudt system.

## 4.1 Sertifiserte serveroperativsystem

Følgende serveroperativsystemer er sertifisert for bruk:

a. Microsoft Windows Server 2008 R2 (Standard, Enterprise og Datacenter)
b. Red Hat Enterprise Linux 6

## 4.2 Sertifiserte filsystem

Godkjente filsystem for både system og datalagring er NTFS for Windows Server og ext4 for Red Hat Enterprise Linux. Rå tilgang til disk devices støttes ikke.

## 4.3 Generelle krav til serveroperativsystem

a. Sertifiserte versjoner av serveroperativsystem inkluderer alltid implisitt siste tilgjengelige servicepack eller vedlikeholdsoppdatering
b. Patcher og feilrettinger fra leverandør av serveroperativsystem (i.e. Microsoft, Red Hat) installeres fortløpende av Helse Nord IKT basert på operative driftshensyn
c. Alle servere inngår i regionens Active Directory og underlegges felles Group Policy, herunder også sentralisert policystyring av Linux-servere
d. All tilgang til servere skjer ved hjelp av domene-konto (i.e. ingen lokale brukerkontoer)
e. Lokal brannmur på serveren må være slått på, med eksplisitte unntak kun for nødvendige porter brukt til management og applikasjoner og tjenester
f. Windows-servere må støtte å ha siste versjon av Internet Explorer og .Net Framework installert

g. Alle applikasjoner og tjenester må kunne kjøre uten at noen er pålogget konsollet; i.e. som en Windows Service
h. Dersom en service må kjøre i brukerkontekst skal denne kontoen ikke ha administrator rettigheter
i. Seksjon for servertjenester ivaretar sikkerhetskopiering (backup) i henhold til bestilling forutsatt nødvendig dokumentasjon (herunder forventet datavolum og endringsrate) og med regionens felles backupsystem (for tiden Symantec NetBackup)
j. Alle applikasjoner og tjenester bør kunne autentisere brukere mot regionens Active Directory
k. Applikasjoner må være environment variable aware. Som et minimum for alle Microsoft standard variabler.
l. Forventet behov for lagring og vekst i dette behovet må dokumenteres
m. Installasjon og lagring av alt som ikke er OS-spesifikkt må skje mot andre volumer enn systemdisk
n. Eventuell kommunikasjon mot Internett (e.g. for henting av supplerende data) skal skje via Helse Nords web proxy løsning, inkludert autentisering med en Active Directory konto
o. Fjernstyring av server skal, der aktuellt, skje ved hjelp av RDP og autentisering skjer ved bruk av personlige kontoer i regionens Active Directory
p. Applikasjonen eller tjenesten må fungere selv om det er en antivirusløsning installert på serveren
q. Alle servere konfigureres med fast IP adresse, og WINS og broadcast blir disablet
r. Lisensdongler må ha støtte for IP (f.eks. USB over IP) slik at de kan fungere i et virtuelt miljø.

## 4.4 Generelle krav til webservere

- Systemet må benytte enten Microsoft Information Server eller Apache webserver.
- Systemrammeverk for websystem (MS .Net, PHP, Java osv.) må kunne oppdateres til nyeste versjoner.

# *5 Database*

Databaseløsninger i regionen driftes av Helse Nord IKT i et standardisert stordriftsregime. Regionen har standardisert på tre godkjente databasemotorer og disse støttes i siste sertifiserte hovedversjon, men med mulighet for bruk av forrige hovedversjon i unntakstilfeller. Systemer som benytter databaser skal i hovedsak støtte bruk av en sentralisert databasemotor (i.e. ikke kreve bruk av en sk. ”embedded” databasemotor); kunne sameksistere med andre applikasjoner på den samme databasetjeneren; og må støtte å kjøre mot en databaseklynge (cluster).

Masterpassord og administratorkontoer (e.g. sysadmin/administrator for MS SQL, sys/system for Oracle, etc.) gjøres normalt ikke tilgjengelig for leverandøren. Tilgang for vedlikehold eller feilsøking skjer ved hjelp av en dedikert brukerkonto for aktuell leverandør og system med de nødvendige tilganger (normalt kun lesetilgang, men utvidete rettigheter kan tildeles ved behov i særskilte tilfeller).

Sikkerhetskopi (backup) og programvareoppdateringer ivaretas av Seksjon for databasedrift.

## 5.1 Sertifiserte databasemotorer

Følgende databasemotorer er sertifiserte for bruk:

a. Microsoft SQL Server 2008
b. Oracle 11g
c. MySQL 5

## 5.2 Alternative databasemotorer

Følgende databasemotorer er sertifiserte men under utfasing, eller er av andre årsaker ikke en del av standard driftsplattform for nye installasjoner:

a. Microsoft SQL Server 2005
b. Oracle 10g

## 5.3 Generelle krav til databaser

a. Leverandør skal angi filsystem, operativsystem og databaseplattform som databasedelen av løsningen kan kjøre på
b. Angi oppgraderingsplan for databaseplattform som løsningen skal kjøre på
c. Databaseløsningen skal ha design basert på høy tilgjengelighet som inkluderer bruk av klyngeteknologi. Databaser som krever standalone servere er et unntak og vil medføre høyere kostnader til etablering og drift
d. Databaseløsninger som krever egne servere for den gitte applikasjonen, skal kunne være skalerbar
e. Databaseløsningen skal kunne installeres adskilt fra applikasjonsserverløsningen og andre applikasjonsspesifikke komponenter
f. Databasen skal håndtere skandinavisk og samiske tegnsett korrekt både ved registrering og søking
g. Databasen skal håndtere ulike typer spesialtegn (for eksempel α, β, γ, μ) korrekt både ved registrering og søking
h. Tilbudt løsning skal ved installasjoner og oppgraderinger ikke kreve tilgang via brukere eller rettigheter tilsvarende sa, sys eller system
i. Overvåkning og backup gjøres etter interne rutiner ved Seksjon for databasedrift i Helse Nord IKT
j. Seksjon for databasedrift ivaretar oppgradering av databasemotor og databaser i samråd med leverandør

# *6 Lagring*

Helse-Nord IKT har standardisert på lagringsløsninger fra EMC.

Ved alle sykehus har vi SAN løsninger (EMC CX4 eller EMC VNX) for blokk lagring (gjennom FC-FibreChannel). FC-switchene er levert av Cisco.

I Tromsø har vi også NAS lagring (EMC Isilon) for ustrukturerte fildata. Protokollene som brukes her er SMB og NFS.

Totalt har Helse-Nord IKT ca. 1900TB data samlet i hele regionen.

# *7 Samhandling/ Integrasjoner*

a. Vi ønsker et brukergrensesnitt å arbeide mot.
b. Verktøy skal være tilgjengeliggjort for drift, vedlikehold og konfigurasjon
c. Det skal tilgjengeliggjøres et overvåkingsverktøy eller spesifiseres hvilket overvåkingsverktøy som skal benyttes.