

Bilag 3: Kundens tekniske plattform

Januar 2025

Dato: 31.01.2025

1.	Innledning	3
2.	Ordliste	3
3.	Dagens driftsmiljø	4
3.1	Drifts og sikkerhetscenteret (DSS)	4
3.2	Prosess	4
4.	Datasenter	5
4.1	Lokale datarom	5
5.	Nettverk	5
5.1	Nettverksautentisering	5
5.2	Lastbalansering	6
5.3	Nettverkssoner	7
6.	Server	8
7.	Endepunktutstyr	9
7.1	Windows klient operativsystem (WaaS)	9
7.2	Virtuell Desktop Infrastruktur	9
7.3	Mobiler og Nettbrett med Android og iOS	10
7.4	Pakking og distribusjon av programvare	10
8.	Backup og arkivløsning	10
8.1	Backup	10
8.2	Datasenter Disaster Recovery	10
9.	Andre tekniske tjenester	10
9.1	Katalogtjenester	10
9.2	Leverandørtilgang og fjernaksess	10
9.3	Databasetjenester	11
9.4	Webtjenester	11
9.5	Filtjenester	11
9.6	Integrasjonstjenesten	11
9.7	Sårbarhetssjekk	11
9.8	Identitet- og tilgangsstyring (IOTS)	11
10.	Støttetjenester	12
10.1	Service Desk	12
11.	Livssyklus, forvaltningsplan og tredjepartsprodukter	12
11.1	Bakgrunn	12
11.2	Avvik	12
11.3	Oversikt over produkters livssyklus	13

1. Innledning

Dette bilaget utgjør Kundens beskrivelse av den tekniske plattformen for leveransen. I dette bilaget er det ikke fremsatt krav.

Helse Nord består av 11 sykehus, rundt 150 utelokasjoner, og rundt 19.000 ansatte. For best mulig utnyttelse av regionens felles IKT-ressurser er Helse Nord IKT HF (HN IKT) etablert som en felles IKT-driftsorganisasjon for hele regionen. All IKT-infrastruktur i regionen skal driftes og forvaltes av HN IKT, og er etablert i et stordriftsregime utviklet for mest mulig effektiv understøttelse av 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. Det derfor kritisk at alle leverandører tydelig oppgir kompatibilitet med og behov for slike komponenter og tjenester.

Enkelte krav er ufravikelige (f.eks. krav til oppdatert antivirusløsning, operativsystem på server og klient m.m.). System som ikke etterlever de mest sentrale kravene, vil ikke kunne innføres i regionen.

Dokumentet tar kun for seg de mest allment anvendelige krav og er 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, må dette innhentes.

2. Ordliste

NHN: Norsk Helsenett SF

NGK: Neste Generasjon Kjernenett. Dette er nytt regionalt nettverk som blir levert av NHN.

DSS: Regionalt drifts og sikkerhetssenter

SKM: Sentralt Kjøremiljø

IOTS: Identitet- og tilgangsstyring

3. Dagens driftsmiljø

Helse Nord IKT drifter, forvalter og utvikler IKT-systemer for Helse Nord.

Helseforetakene i Helse Nord er underlagt krav til informasjonssikkerhet i en rekke lov- og forskrifter, Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen) og felles styringssystem for informasjonssikkerhet i Helse Nord. Normen er juridisk bindende for HN IKT og helseforetakene gjennom avtale med Norsk Helsenett SF. Virksomheter som følger Normen vil i utgangspunktet ivareta alle krav til informasjonssikkerhet som følger av lovverket. Felles styringssystem for informasjonssikkerhet beskriver blant annet Helse Nord's felles sikkerhetspolicy, sikkerhetsmål og sikkerhetsstrategi. Den er førende for å ivareta sikkerhetskravene i regionen. Leverandører av utstyr og tjenester må til enhver tid være kjent med og etterleve alle Helse Nord's krav til informasjonssikkerhet.

3.1 Drifts og sikkerhetscenteret (DSS)

Helse Nord IKT har etablert et drifts- og sikkerhetscenter som benytter seg av overvåknings- og loggverktøyer for å samle informasjon om konfigurasjonseenheter. DSS overvåker både fysiske og logiske enheter med rundt 200000 målepunkter. Sikkerhetslogger lagres i vårt sentrale loggsystem.

Eksterne leverandører

Eksterne leverandører som utfører arbeid/vedlikehold (endringer) som kan berøre tjenester/brukere i Helse Nord må sørge for å ha etablerte rutiner for å varsle arbeidet til HN IKT, slik at det kan registreres og håndteres av HN IKT sin endringspraksis. Eksterne leverandører skal varsle senest 7 dager før arbeidet skal gjennomføres.

3.2 Prosess

HNIKT har valgt å benytte ITIL4 og IT4IT som rammeverk for å strukturere opp arbeidsprosesser med definerte roller og ansvar.

Figur: HN IKT – overordnet arbeidsflyt og leveranser innenfor hovedprosessene



4. Datasenter

Helse Nord sine datasenter skal sikre IKT-tjenester med høy sikkerhet, driftskvalitet og tilgjengelighet. Løsninger med høye krav til tilgjengelighet (opetid/ytelse) må kunne eksistere i en konfigurasjon strukket over to fysiske datasentre

4.1 Lokale datarom

På alle sykehus i Helse Nord er det lokale datarom. Lokale datarom skal sikre minimumsfunksjonalitet på sykehuset i tilfelle feil på nettverk eller regionale datasenter. Hvilke funksjoner som skal etableres på de ulike sykehusene vil være avhengig av de ROS-analyser som gjøres for hvert enkelt sykehus.

5. Nettverk

Helse Nord har stor geografisk spredning som dekker fylkene Nordland, Troms og Finnmark i tillegg til Svalbard. Stor geografisk spredning medfører utfordringer med linjeføringer, tilgjengelighet og forsinkelser i nettverket. Nettverk for spesialisthelsetjenesten i Helse Nord er knyttet sammen på regionalt og nasjonalt nivå med leveranser fra Norsk Helsenett (NHN).

Regionalt nettverk:

Regionens klinikker og sykehus er koblet sammen i et WAN (Wide Area Network) basert på en regional utbygging av Norsk Helsenett sitt nasjonale stamnett med kompletterende sambandsprodukt fra dem. Helse Nord sine elleve sykehus er koblet sammen i et regionalt nettverk levert på som er redundant og med full diversitet. Antallet andre lokasjoner er rundt 130 og inkluderer alle klinikker og ambulansestasjoner i spesialisthelsetjenesten i Nord-Norge.

Helse Nord IKT krypterer all trafikk over disse sambandene. 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 regler i brannmurer. Et større spann av dynamisk tildelte porter tillates normalt ikke.

Lokalt nettverk

Lokale nettverk, som er nettverk inne på sykehusene, er bygget opp av svitsjer på flere nivå (LAN) i tillegg til trådløse aksesspunkt (WLAN), og basert på IPv4 med støtte for IPv6. Design er basert på en kjerne, distribusjon og aksess topologi. Båndbredden på det kablede nettet varierer. IP-adresser i bruk er hovedsakelig RFC1918 og RFC6598 adresser, men utstyr og tjenester må fungere med en blanding av private og offentlige adresser. IP adresser i produksjon er i henhold til Norsk Helsenetts nasjonale IP-plan.

5.1 Nettverksautentisering

Autentisering av brukere for drift av nettverksutstyr og tilkobling av endeutstyr som har mobildata som kommunikasjonsform skjer ved hjelp av sentralisert autentiseringstjeneste.

Network Access Control (NAC) benyttes som intern sikring i lokale nettverk, både for kablet og trådløs tilkobling. Endeutstyr som skal ha tilgang verifiseres, dersom kjent utstyr gis tilgang basert på dette. Verifisering gir kontroll over alle enheter som får tilgang til produksjonssystemer levert via

Helse Nords infrastruktur. Av prinsipp skal alle enheter som kobles til Helse Nords infrastruktur autentiseres. Derfor må de støtte IEEE 802.1x (dot1x) med tilhørende mekanismer.

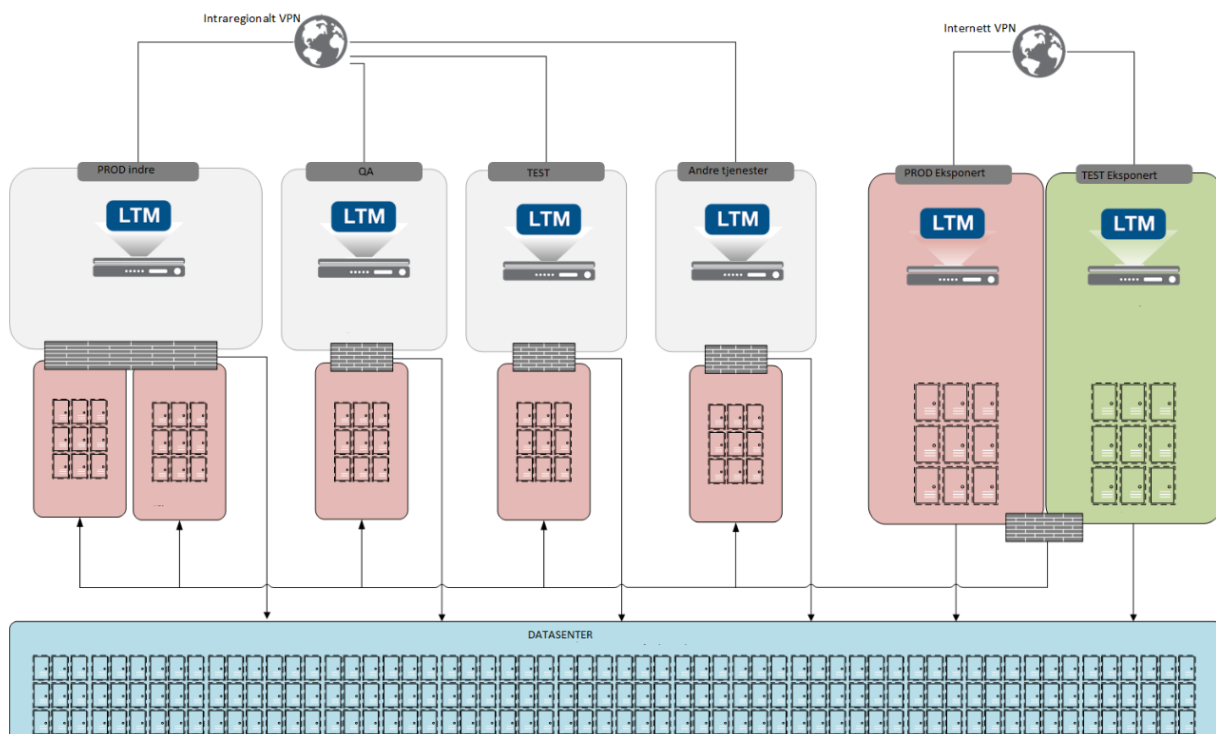
5.2 Lastbalansering

Helse Nord IKT benytter i dag primært F5 BIG-IP produkt for lastbalansering av tjenester. Dette miljøet understøtter ulike produksjons-, QA- og testmiljøer.

F5 er implementert for å dekke ulike tekniske og funksjonelle behov så som:

- Eksponeringspunkt for tjenester
- Sømløs skalering av applikasjonsservere som har støtte for slik design

Helse Nord IKT driver også fjerntilgangstjenesten Omnissa Horizon som er lastbalansert med Netscaler. Dette produkt benyttes også til andre tjenester som er egnet for å produsere på den samme teknologien.

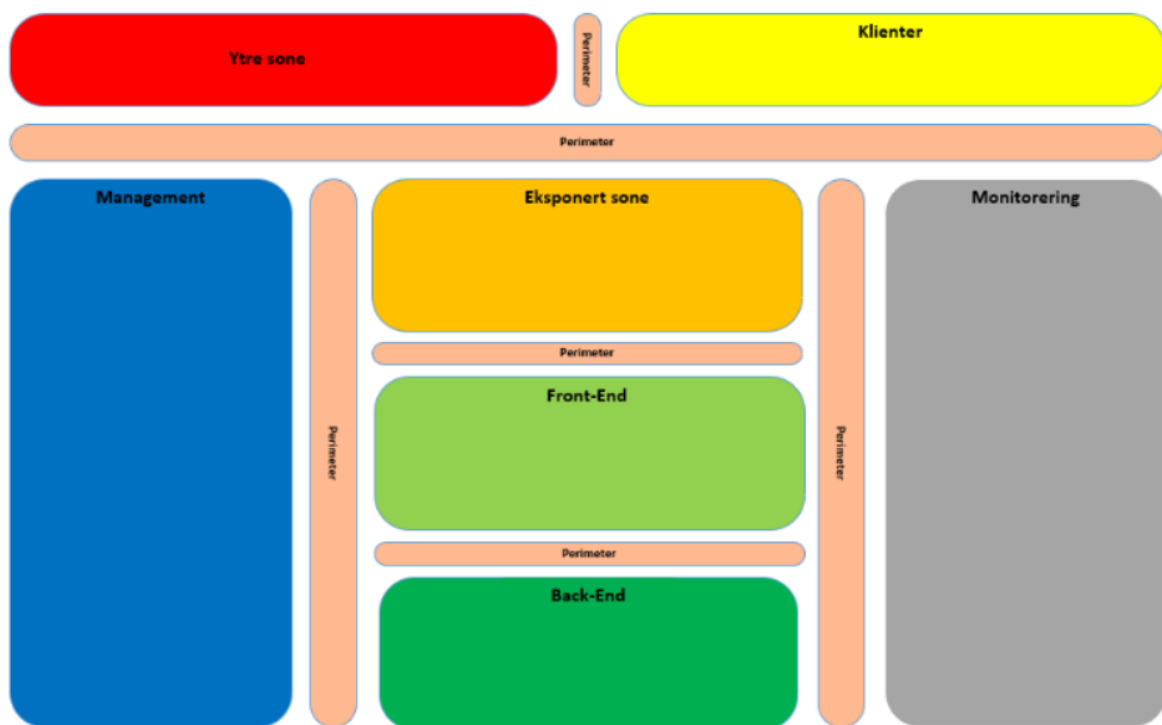


Figur - F5 topologi Helse Nord

5.3 Nettverkssoner

Sonemodellen representerer hele regionen og skal benyttes som «kart» for blant annet plassering av endestyr og hvor klassifisert data får lagres samt transporteres. Det skal være mulig å kontrollere og sikre data i ro og ved transport. Nedenfor er en oppsummering av ulike dimensjoner av modellen. Et prinsipp i design av modellen er at soner skal baseres på en topologi med kategorier slik som åpen, intern og sikker sone. Videre skal modellen legge et godt grunnlag for å håndheve et Zero Trust prinsipp.

Sikkerhetssoner	Sikringsmekanismer	Sonetyper
Åpen: Ytre sone, Eksponert sone Intern: Klienter, Front-End Sikker: Back-End, Management og Monitorering	Skallsikring Internsikring Tilgangskontroll	Transitt-sone(Transport): Sone for å ta imot og videresende data Multi-sone: Sone for å ta imot, mellomlagre og videresende data Lagrings-sone: Sone for lagring av data



Figur: Hovedsoner i sonemodellen.

6. Server

Sentralt Kjøremiljø (SKM)

Helse Nord sitt sentrale kjøremiljø (SKM) er en felles IT-infrastruktur som brukes av helseforetakene i Helse Nord. SKM er en plattform som baserer seg på virtualisering og automatisering som igjen gir en standardisert og sikker måte å kjøre applikasjoner på tvers av helseforetakene i regionen. SKM er Helse Nord sin private skytjeneste basert på VMWare Cloud Foundation.

SKM har støtte og ressurser for å ta i bruk det nyeste innen container-teknologi for å kjøre applikasjoner. SKM tilgjengeliggjør virtuelle maskiner og støtter en rekke applikasjoner som brukes av helseforetakene i regionen. Dette inkluderer elektronisk pasientjournal (EPJ), radiologisystemer, laboratorieinformasjonssystemer (LIS) og andre spesialsystemer. Hver applikasjon kjører i sin egen virtuelle maskin eller container og er isolert fra andre applikasjoner som kjører på samme plattform.

Plattformen er designet for å sikre høy tilgjengelighet, slik at kritiske helsetjenester og applikasjoner alltid er tilgjengelige for helsepersonell. Den inkluderer også strenge sikkerhetsprotokoller for å beskytte pasientdata og andre sensitive opplysninger.

Som operativsystem på serverne benyttes hovedsakelig MS-Windows Enterprise server, og Red Hat Enterprise Linux.

Generell strategi innenfor OS-området:

- Operativsystem med mainstream end date innen 8 måneder vil ikke støttes (Se også kap. 11.3 for oversikt)
- Automatisk oppdatering skal være påslått med mindre det er en godt dokumentert rutine for månedlig oppdatering som er godkjent av seksjonsleder/avdelingsleder i HN IKT Infrastruktur og Plattform
- I spesielle tilfeller der leverandør kommer med egne installasjons filer (ISO/OVA) må dette meldes til HN IKT / Infrastruktur og Plattform / Skytjenester slik at agenter for endepunkt-tjenester og antivirus kan installeres.
- Oppslag mot AD/domene skal være kryptert eller signert (Signed LDAP)
- Det skal ikke benyttes usikre eller utdaterte protokoller (les SMBv1 eller lignende)

Spesifikke krav for Windows server:

- Agent for endepunkt-tjenester skal installeres (Både for server og klient)
- Leverandørs beste praksis for serversikring skal følges – Microsoft Security Baseline
- Lokal brannmur skal alltid være påslått.
- Benytte standardisert antivirus-tjeneste i Helse Nord
 - Antivirus skal til enhver tid være aktiv
 - Unntak i Antivirus må bestilles (Unntak av hele diskstasjoner er ikke godkjent)

Spesifikke krav for Linux server:

- Kun Red Hat Enterprise Linux (RHEL) støttes
- Kun versjoner av RHEL som er innenfor Full support (ref. <https://endoflife.date/rhel>)
 - Versjoner som ikke er i Full Support, men fortsatt i Maintenance Support **kan** provisjoneres unntaksvis)

- Linux-servere skal etterleve det til enhver tid gjeldende sikkerhetsrammeverk. Pr. 2024 er dette CIS IG 1.
- Skal nås (les: brannmursåpning) av sentralisert automatiseringsplattform for Linux (Red Hat Ansible Automation Platform)
- Skal nås (les: brannmursåpning) av Red hat Satellite og bruke Red Hat Satellite for henting av pakker/patcher.
- Servere skal sikkerhetsoppdateres automatisk via sentralisert automatiseringsplattform. Hvis manuelt skal det foreligge en plan for dette.
- Skal meldes inn i AD

7. Endepunktutstyr

7.1 Windows klient operativsystem (WaaS)

Som operativsystem på klienter benyttes Microsoft Windows (Enterprise). Operativsystemet leveres på siste versjon av Windows, med mainstream end date innen 12 måneder vil ikke støttes. Operativsystemet herdes ved bruk av Microsoft Security Baselines, Bitlocker, Applocker, credential guard, brannmur og antivirus.

Helse Nord IKT har standardisert maskinvaren for bærbare PC-er og desktooper med Windows. Disse kjøpes igjennom en nasjonal innkjøpsavtale som er forhandlet frem av Sykehusinnkjøp.. Helse Nord IKT benytter flåtestyring, tredjepart tilpassinger og egenutviklede verktøy for å administrere disse enhetene.

7.1.1 Klienter som ikke er eid av Helse Nord (Leverandør-PC)

Følgende krav stilles til en leverandør-PC for å kunne plassere denne i HN-domenet:

Skal ha installert Antivirus.

Skal kunne kjøre med Microsoft Security Baseline. Dette innebærer:

- Applocker, Bitlocker og Credential Guard
- Konto som det logges på med skal ikke være lokal administrator (Denne er svært viktig)
- Følgende må kunne patches
- Firmware (Bios og annet hardware)
- Operativsystem med runtime komponenter (.NET, vc red og lignende)
- Tredjeparts software (For eksempel Adobe eller lignende)
- De må innlemmes i management system for å kunne administreres. (Altiris Agent)
- Se Patch nivå og kunne sende ut patcher til enheten.
- Må kunne rapportere på tilstanden.

7.2 Virtuell Desktop Infrastruktur

Helse Nord IKT benytter Omnissa Horizon (tidligere VMWare) til leveranse av virtuelle arbeidsflater med Windows. Felles maskiner benytter i stor grad virtuelle arbeidsflater med sesjonsvandrings funksjonalitet. Det er derfor særdeles viktig at programvare som skal benyttes på slike enheter støtter denne typen virtualiseringsteknologi og bruksmønster.

7.3 Mobiler og Nettbrett med Android og iOS

Android og iOS enheter er underlagt den regionale EMM løsningen i Helse Nord. Disse enhetene er anskaffet via en nasjonal avtale forhandlet frem av Sykehusinnkjøp. Løsningen baserer seg på Workspace ONE® Unified endpoint management (Workspace ONE® UEM). Løsningen er uavhengig av nettverksbærer. Løsningen er etablert som en regional tjeneste for administrasjon og vedlikehold av mobile enheter, som nettbrett og smarttelefoner. Løsningen dekker behovet for å sikre enheter, data og kommunikasjon, i tillegg til sentralisert administrasjon og vedlikehold. Løsningen tilgjengeliggjør administrative og kliniske applikasjoner, dersom kommunikasjon til interne tjenester er påkrev leveres dette ved bruk av pr app VPN.

7.4 Pakking og distribusjon av programvare

Programvareinstallasjoner i Helse Nord skal kunne automatiseres.

For Windows klient operativsystem er Microsoft MSIX preferert virtualiseringsteknologi. App-V støttes, men er under utfasing. Produsenter må levere programvare med støtte for MSIX før 1. Januar 2026. På virtuelle arbeidsflater benyttes også Omnissa Appvolumes (tidligere VMWare).

I de få tilfeller hvor virtualisering ikke er mulig benyttes MSI eller annen scriptbasert installering for begrensede volum på fysiske klienter. Programvare på virtuelle arbeidsflater må støtte virtualisering nevnt over.

8. Backup og arkivløsning

8.1 Backup

Helse Nord bruker agentbasert backup for servere. De fleste tjenester er migrert til SKM backup-løsning (CommVault).

8.2 Datasenter Disaster Recovery

I SKM benyttes Commvault som DSDR. E-post og e-post arkiv skal migreres til Microsoft365.

9. Andre tekniske tjenester

9.1 Katalogtjenester

Microsoft Active Directory (AD) benyttes som katalogtjeneste for brukere, tjenester og maskiner. AD og AD-Domain Name System (AD-DNS) er satt opp som redundante tjenester på alle domenekontrollere. Hoveddomenet hn.helsenord.no er en enkel "forest", som inneholder alle helseforetakene i Helse Nord. Alle ansatte og innleide må være definert som brukere og autentisere seg mot AD for å få tilgang til tjenester og ressurser i Helse Nord.

9.2 Leverandørtilgang og fjernaksess

All fjerntilgang til utstyr eller tjenester plassert i Helse Nord's 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 Nord's standard løsning for fjerntilgang.

9.3 Databasetjenester

Databaseløsninger i regionen driftes av HN IKT i et standardisert stordriftsregime. Regionen har standardisert på tre databasemotorer (MSSQL, Oracle (Cloud at Customer) og MySQL).

9.4 Webtjenester

Helse Nord IKT tilbyr en standardisert, regional web-plattform for å hoste primært egenutviklede web-applikasjoner hos Helse Nord. Alle servere tilknyttet løsningen kjøres virtuelt på SKM.

9.5 Filtjenester

Filtjenester

Filservere er i hovedsak virtuelle Windows-servere med lagring mot SAN/NAS. Fillagring er basert på SMB 2.0 og nyere med DFS. Helse Nord benytter OneDrive for data tilhørende enkeltbruker og SharePoint for fellesområder..

Print-tjeneste

All Nettverksbasert utskrift gjøres via sikker utskrift. Løsning SafeQ fra Ysoft benyttes i hele regionen.

9.6 Integrasjonstjenesten

Integrasjonstjenesten er en regional løsning som utvikles for å støtte det økende behovet for effektiv pasient-, arbeids- og informasjonsflyt i Helse Nord.

Den erstatter punkt-til-punkt-integrasjoner med felles tjenester som kan gjenbrukes av flere fagsystemer. Tjenesten er primært bygget på Microsoft BizTalk og IIS.

Integrasjonene bruker åpne standarder som HL7 v3, FHIR og KITH.XML, og plattformen leverer også infrastrukturen for kommunikasjon mot [Helsenorge.no](https://helsenorge.no).

Plattformen består av flere separate miljøer, inkludert flere testmiljøer, QA og produksjon.

9.7 Sårbarhetssjekk

Helse Nord IKT gjør jevnlig ports- og sårbarhetssjekker av Helse Nord's infrastruktur. Helse Nord benytter også HelseCERT[3] til å gjøre årlige penetrasjonstester mot Helse Nord's infrastruktur. Enkelte komponenter i infrastrukturen vil da kunne bli utsatt for ekstra grundige sjekker.

9.8 Identitet- og tilgangsstyring (IOTS)

Tjenesten leverer PAM (Privileged Access Management), IAM (Identity and Access Management) og autorisasjonsløsninger for Helse Nord. All privilegert tilgang (admin-tilganger) til servere og klienter skal gjøres gjennom PAM. I fremtiden skal all privilegert tilgang til system, nettverksutstyr etc. også gjøres gjennom PAM. Helse Nord benytter sentral autentiseringstjeneste basert på Microsoft Azure AD. Alle eksterne applikasjoner må imøtekomme krav om støtte for OIDC/OAuth2 eller SAML.

Det skal benyttes fler-faktorautentisering ved pålogging til skytjenester der det behandles personopplysninger, virksomhetsintern informasjon eller annen sikkerhetskritisk informasjon. Autentiseringen skal utføres på godkjente regionale autentiseringsløsninger.

HelseID skal benyttes for ekstern kommunikasjon hvor pasientdata er involvert.

SERVICEKONTOER OG ADMIN-KONTOER

Alle tjenester etableres med dedikert servicekonto med lavest mulige rettigheter. Servicekontoer skal etableres med rutiner for periodisk bytte av passord iht. Helse Nords rutiner for passordstyrke og rullering.

10. Støttetjenester

10.1 Service Desk

Helse Nord IKT har en regional servicedesk som single point of contact for Helse Nord, og er bemannet kl. 08.00-15.30, i tillegg til en 24/7 driftsvakt. ITIL er valgt som prosessrammeverk for håndtering av kundesøknader og benytter et dedikert saksbehandlingsverktøy.

11. Livssyklus, forvaltningsplan og tredjepartsprodukter

11.1 Bakgrunn

Livssyklus for operativsystemer knyttet til nettverksutstyr, lagringsløsninger, servere, databaser etc. defineres av SPM-prosessen (Service Portfolio Management). I utgangspunktet støttes siste versjon av et produkt innenfor EOL (End of Life).

For å motvirke etablering av ny teknisk gjeld i Helse Nords infrastruktur og skal alle nye tjenester som produksjonssettes leveres med en tilhørende forvaltningsplan.

Forvaltningsplanen skal beskrive løsnings livsløp, herunder både kontinuerlig vedlikeholdsarbeid for å holde løsningen up to date (sikkerhetspatching, oppgraderinger og annet), syklisk fornyelse av tilhørende hardware og også sanering av løsnings utdaterte komponenter.

Eksterne leverandører av løsninger til Helse Nord skal kravstilles slik at løsningen kan forvaltes etter denne planen.

11.2 Avvik

Avvik tillates ikke.

Hvis det gjøres unntak, så skal det være som følge av en behandling med blant annet gjennomføring av ROS og risikoreduserende tiltak som godkjennes i porteføljeprosessen, eller ledergruppen HN IKT representert ved avdelingsledelse Infrastruktur og Plattform.

Det er utarbeidet egne rutiner knyttet til godkjenning av avvik, disse inkluderer også krav knyttet til mitigerende tiltak og varighet

11.3 Oversikt over produsers livssyklus

Produsenter har en start- og sluttdato for sine produkter. I utgangspunktet støttes siste versjon av et produkt innenfor EOL ("End of Life") fra produsenten. HN IKT beregner noe tid for å verifisere produktene, som innebærer en egen start- og sluttdato som er noe senere en produsenten.

For eksempel kan dette være Windows Server 2022. HN IKT kan ikke være klar til å støtte dette på samme dag som Microsoft, dermed er startdato noe etter Microsofts utgivelsesdato.

Tilsvarende må HN IKT ha en egen sluttdato for å sikre at vi har utfaset alle komponenter den dagen produsenten slutter å støtte produktet. I eksempelet over vet vi at support på Windows Server 2022 opphører i 2026. Da må HN IKT ha utfaset alle installasjoner innen da. Det betyr at HN IKT sin sluttdato er tidligere. Videre vil det ikke bli tilbudt nyinstallasjoner av en versjon 12 måneder etter at en nyere versjon har blitt utgitt. Denne siden har informasjon om alle sentrale produkter med tilhørende livssyklus for både produsent og HN IKT.

Merk at ansvarlig tjeneste kan bli belastet for merkostnader knyttet til utvidet support, inkludert interne kostnader forbundet med ekstraordinære tiltak. Dette inkluderer utvidet support lisenser fra leverandører, tiltak for å redusere risiko og bistand til opprettelse av utvidet support.

HN IKT startdato = Produsentens utgivelsesdato + 3 måneder. Ny versjon tilbys som standard
HN IKT slutt på nyinstallasjon = HN IKT startdato (på ny/neste produktversjon) + 12 måneder
HN IKT sluttdato = Operativ systemet skal være avviklet.

Red Hat Enterprise Linux

Produktversjon	Produsent utgivelsesdato	HN IKT startdato	HN IKT slutt på nyinstallasjon	HN IKT sluttdato
Red Hat Enterprise Linux 7	11.12.2013	01.03.2014	01.11.2019	31.12.2019
Red Hat Enterprise Linux 8	07.05.2019	01.08.2019	01.08.2023	31.12.2023
Red Hat Enterprise Linux 9	17.05.2022	01.09.2022	TBA	31.12.2026
Red Hat Enterprise Linux 10	Q2 2025	Q3 2025	TBA	

Microsoft Windows Server

Produktversjon	Produsent utgivelsesdato	HN IKT startdato	HN IKT slutt på nyinstallasjon	HN IKT sluttdato
Windows Server 2016	15.10.2016	01.01.2017	01.02.2020	01.09.2021
Windows Server 2019	13.11.2018	01.02.2019	01.11.2022	01.09.2023
Windows Server 2022	18.08.2021	01.11.2021	01.06.2025	01.07.2026
Windows Server 2025	01.11.2024	01.03.2025	TBA	

Microsoft Windows Klient

Produktversjon	HN IKT startdato	HN IKT sluttdato	Mainstream support end	Extended support end
Windows 10 21H2	01.06.2019	TBA	01.12.2027	01.12.2027
Windows 11	01.05.2023	TBA		

Microsoft SQL Server

Produktversjon	HN IKT startdato	HN IKT sluttdato	Mainstream support end	Extended support end
MS SQL Server 2016 SP2	-	Tilbys ikke	13.07.2021	14.07.2026
MS SQL Server 2017	13.12.2018	TBA	11.10.2022	12.10.2027
MS SQL Server 2019	20.11.2020	TBA	07.01.2025	08.01.2030
MS SQL Server 2022	01.11.2023	TBA	11.01.2028	11.01.2033

MySQL

Produktversjon	HN IKT startdato	HN IKT sluttdato	Mainstream support end	Extended support end
MySQL 5.7	01.10.2015	01.10.2023	01.10.2020	01.10.2023
MySQL 8	01.01.2020	TBA		

Oracle Database

Produktversjon	HN IKT startdato	HN IKT sluttdato	Mainstream support end	Extended support end
Oracle 19c	01.10.2020	01.04.2027	01.04.2024	01.04.2025

Microsoft .Net Framework

Produktversjon	Start Lifecycle	End Date
Microsoft .Net Framework 3.5 SP1	18.11.2008	09.01.2029
Microsoft .Net Framework 4.5.2	05.05.2014	26.04.2022
Microsoft .Net Framework 4.6.1	30.11.2015	26.04.2022
Microsoft .Net Framework 4.6.2	02.08.2016	12.01.2027
Microsoft .Net Framework 4.7	11.04.2017	TBA
Microsoft .Net Framework 4.7.1	17.10.2017	TBA
Microsoft .Net Framework 4.7.2	30.04.2018	TBA
Microsoft .Net Framework 4.8	18.04.2019	TBA
Microsoft .Net Framework 4.8.1	09.08.2022	TBA