# Vedlegg 4- Kundens tekniske plattform

# 1. Innledning

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

# 2. Ordliste

NHN: Norsk Helsenett SF
NGK: Neste Generasjon Kjernenett. Dette er nytt regionalt nettverk som blir levert av NHN.
DS1: Regionalt datasenter1
DS2: Regionalt datasenter2
DSS: Regionalt drifts og sikkerhetssenter

# 3. Dagens driftsmiljø

Helse Nord IKT forvalter, drifter og utvikler IKT-systemer for Helse Nord og regionens rundt 18000 brukere.

## 3.1. Prosess

For å legge til rette for tverrgående ITIL-prosesser (Information Technology Infrastructure Library) i Helse Nord IKT er det etablert et eget prosesstyret. Prosesstyret forvalter ITIL-prosessene med understøttende verktøy som er innført i organisasjonen.

For å håndtere og støtte opp arbeidsflyt for disse prosessene benyttes verktøyet HP Service Manager (HPSM). Verktøystøtten dekker per i dag ikke alle prosesser i prosesskartet.
I tillegg brukes det for Change Management i noen tilfeller en egenutviklet endringslogg gjeldende aktuell konfigurasjonsenhet.
Bestillinger (Request Management) håndteres i HPSM. Ved bestilling opprettes en egen change i HPSM for videre oppfølging. Disse sakene håndteres i dag primært manuelt.
For Access Management i HN IKT benyttes det IAM (Identity and Access Management) – automatisert tilgangsstyring. IAM ble innført i HN IKT oktober 2022. I mars 2023 har vi erstattet noen funksjoner i BAS med Tilgangsportalen som er den nye selvbetjeningsportalen. For andre helseforetak benyttes det fortsatt en egenutviklet løsning, BAS (Brukeradministrasjonssystem), for ressursprovisjonering og tilgangsstyring. BAS er integrert mot AD (Active Directory). I tillegg gjøres tilgangsstyring direkte i applikasjoner, der det er behov for det.  IAM-løsning innføres etter hvert også i alle de andre helseforetakene.
Service Asset & Configuration Management er etablert og man har automatisk fangst av Configuration items. Det arbeides med å få etablert innhold i en Configuration Management Database (CMDB) som vil støtte opp de andre ITIL-prosessene. For dokumentasjon og livssyklushåndtering av konfigurasjonsenheter (database, server, applikasjon, nett, linje, EDI, SAN) benyttes det primært egenutviklete løsninger.

## 3.2. Leverandørtilgang

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 (for databaser normalt kun lesetilgang, men utvidete rettigheter kan tildeles ved behov i særskilte tilfeller). Opprettelse av brukerkonto forutsetter at leverandøren har signert en databehandleravtale.

For privilegerte tilganger skal PAM Safeguard benyttes.

## 3.3. Drifts og sikkerhetssenteret

Helse Nord IKT har et drifts- og sikkerhetssenter som benytter seg av Checkmk, Splunk, Sysmon og andre verktøyer for å samle informasjon om konfigurasjonsenheten i CMDB.
Hendelser (events) som oppstår på forskjellige konfigurasjonsenheter fanges opp av overvåkningsverktøyene, og deretter registreres som incidents i HP Service Manager for videre håndtering.
DSS overvåker i dag ca. 5000 fysiske og logiske enheter med rundt 200000 målepunkter. I tillegg lagres sikkerhetslogger i Splunk.

## 3.4. Endringsprosessen (Change Management – ITIL)

Helse Nord IKT har etablert Change Management (ITIL) som skal sørge for at alle endringer registreres og gjennomføres på en trygg og forsvarlig måte, med minst mulig forstyrrelser for brukere og sørge for at endringer blir kommunisert ut til berørte parter. 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 endringsprosess.

Eksterne leverandører varsler senest 7 dager før arbeidet skal gjennomføres.

# 4. Datasenter

Helse Nord sine datasenter skal sikre IKT-tjenester med høy sikkerhet, driftskvalitet og tilgjengelighet for å understøtte en slik strategi.
Det er opprettet to datasenter i regionen. Begge sentrene ligger i Tromsø og muliggjør en High Availability-løsning.

## 4.1. Lokale datarom

På alle sykehus i Helse Nord er det lokale datarom. Lokale datasenter 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

## 5.1. Introduksjon til regionens nettverk

Helse Nord har stor geografisk spredning som dekker fylkene Finnmark, Troms og Nordland i tillegg til Svalbard. Stor geografisk spredning medfører utfordringer med linjeføringer, tilgjengelighet og forsinkelser i nettverket.
Helse Nord har i overkant av 65000 nettverkspunkter på LAN som varier i båndbredde fra 10 megabit half duplex og oppover til 10 gigabit.
Helse Nord har i tillegg rundt 2800 trådløse nettverkspunkter, og vi antar at antallet vil øke en del.
Nettverk for spesialisthelsetjenesten i Helse Nord er knyttet sammen på regionalt og nasjonalt nivå med leveranser fra Norsk Helsenett (NHN).
Under finnes en oppsummering av nettverksstrukturen i regionen.

## Regionalt nettverk:

Regionens klinikker og sykehus er koblet sammen i et regionalt nettverk (WAN) basert på en regional utbygging av Norsk Helsenett sitt nasjonale stamnett. Helse Nord sine elleve sykehus er koblet sammen i et regionalt nettverk levert på 10 Gbps samband. Antallet lokasjoner er rundt 100 og inkluderer alle klinikker i spesialisthelsetjenesten i Nord-Norge. Nettilkobling til disse er levert på en rekke forskjellige leveransetyper av regionens Internettleverandører.
Helse Nord IKT krypterer all trafikk over disse sambandene ved hjelp av GETVPN eller DMVPN.
All trafikk som forlater en lokasjon tvinges gjennom et sentralt demarkasjonspunkt og underlegges trafikkontroll, som hovedregel i form av en brannmur med ACL (Access Control List) 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.

## Lokalt nettverk

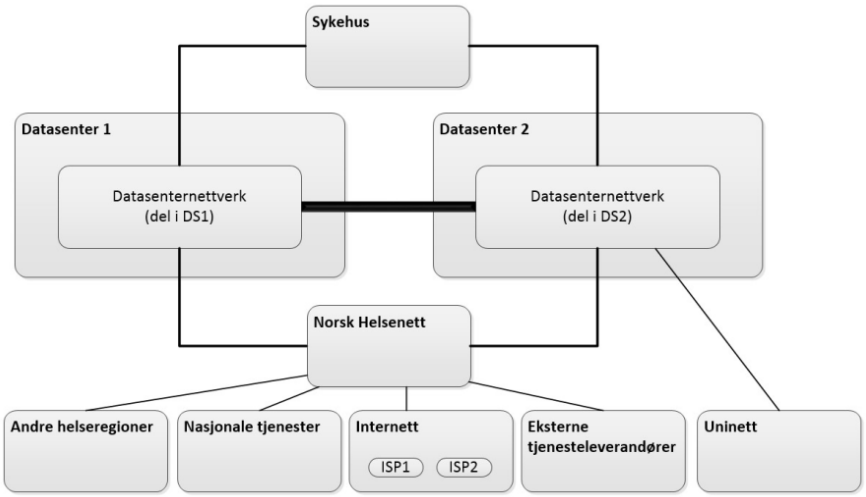
Lokale nettverk, som er nettverk inne på sykehusene, er bygget opp av svitsjer på flere nivå (LAN) i tillegg til trådløse aksesspunkt (WLAN), og basert på IPv4. Båndbredden på det kablede nettet varierer. IP-adresser i bruk er hovedsakelig RFC1918-adresser, men utstyr og tjenester må fungere med en blanding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

## Eksterne tilkoplinger

Tilkopling til eksterne nettverk gjøres gjennom datasenteret. Dette inkluderer:

- Tilgang til Internett via redundante tilkoblinger til internettleveranse fra NHN.
- Tilgang til NHN sine tjenester, samt regionale- og nasjonale tjenester, gjøres via én direkte tilkobling per datasenter til NHN sitt utstyr.
- Tilgang til eksterne tjenesteleverandører gjøres via NHN og én tilkobling per datasenter.
- Tilgang for forskningsenheter innenfor Helse Nord til Uninett gjøres via direkte tilkobling på Helse Nord IKT s rutere i datasenter. Sikkerhetsnivå på denne er lik internett.

I Figur 4 gis en oversikt over regionens nettverksstruktur.




*Figur 4 Oversikt over regionens nettverksstruktur*

## 5.2. Nettverksautentisering

Autentisering av brukere for drift av nettverksutstyr skjer ved hjelp av RADIUS, med mulighet for lokale brukerkontoer når RADIUS er utilgjengelig.

Network Access Control (NAC) gir en oversikt og kontroll over alle enheter som skal ha tilgang til systemer som er tilkoblet Helse Nords infrastruktur. Alle enheter som kobles til Helse Nords infrastruktur skal autentiseres, og må derfor støtte IEEE 802.1x (*dot1x)*.

## 5.3. Lastbalansering

Helse Nord IKT benytter i dag F5 BIG-IP-enheter for lastbalansering av tjenester. Dette miljøet understøtter ulike produksjons-, QA- og testmiljøer.
F5 BIG-IP-miljøene har frem til nå i all hovedsak blitt implementert for å dekke ulike tekniske og funksjonelle behov:

- «Reverse Proxy»-funksjonalitet for internett-eksponerte tjenester (eks. for Microsoft ActiveSync eller Microsoft ADFS).
- Sømløs skalering av applikasjonsservere som støtter dette (Sectra, DIPS, Integrasjon/ESB og innsynstjenesten)

De forskjellige «gjestene» har provisjonert ulike F5-moduler ut ifra plassering og ytelsesbehov. Blant annet er enkelte gjester provisjonert med Lag7-brannmur (ASM) for sikring av bl.a. webtjenester.
All tilgang mellom klient og lastbalanserte tjenester mot de individuelle systemsonene gjøres ved hjelp av SNAT (Source Network Address Translation).
I tillegg har Helse Nord IKT to fysiske Citrix Netscaler appliancer som utelukkende er benyttet av Citrix-løsning.

## 5.4. Nettverkssoner

Soner er opprettet etter prinsippet om klassifiseringene Sikker sone, Intern sone, Åpen sone og Eksterne nett. Tilgang mellom disse må igjennom minst to tekniske barrierer. Typisk er brannmur et av disse.
Dette har gjort at tilnærmingen for nettverkstilgang til tjenestene har vært via virtuelle brannmurer på sentralt brannmurcluster. Det er gjort samling av tjenester som er like av natur bak samme brannmur, f.eks. kliniske tjenester i produksjon. Mens det settes skille mellom enkelte soner selv om de har samme klassifisering. For eksempel vil det være brannmurer mellom kliniske tjenester og administrative tjenester selv om disse er definert til å være i Sikker sone.

# 6. Server

## 6.1. Eksisterende servermiljø

Helse Nord har en blanding av fysiske servere og virtuelle servere som kjører både som enkeltstående hoster og cluster. Som hypervisor kjører man VMware ESXi. Helse Nord har i tillegg anskaffet et hyperkonvergert miljø, heretter omtalt som SKM (Sentralt KjøreMiljø), hvor de fleste tjenestene i dag produseres. Helse Nord opererer per i dag med rundt 3000 servere hvorav 2500 av disse er virtuelle. De fysiske serverne er en blanding av Dell og HP, med et par Sun-servere.

## 6.2. SKM

Helse Nord sitt sentrale kjøremiljø er en privat skytjeneste basert på VMWare Cloud Foundation (SKM 2.0) og VMware Validated Design for Software Defined Datacenter (SKM 1.0). Maskinvare er primært HPE/Cisco/Dell EMC. Det er her Helse Nord skal kjøre mesteparten av serverne. SKM består av to tilgjengelighetssoner: DS1, og DS2.
Nye tjenester som anskaffes skal normalt implementeres her.
SKM kjører en full VMware stack med vSphere, vSan, og NSX basert Cloud Foundation. Det er noen ulike generasjoner av plattformer basert på når det ble etablert. Ny tjenester skal implementeres på siste versjon. Verktøy som brukes for å drifte de virtuelle komponentene av plattformen er vRealize operations manager, vRealize loginsight og vRealize network insight. Til nettverkskomponenter brukes Cisco/HP ICM og HP oneview for fysiske servere. Microsoft Endpoint protection benyttes for antivirus/ antimalware.

## 6.3. Operativsystem

Som operativsystem på serverne benyttes hovedsakelig MS-Windows Enterprise server, og Red Hat Enterprise Linux. Det finnes et mindre antall av andre Linux-varianter som appliances og

servere. Det finnes i tillegg noen få andre operativsystemer. Det er bygget maler på siste versjoner av operativsystemer, samt et utvalg av tidligere versjoner. Se også kapittel 10.3 om livssyklus.

### 6.4. Tilgang til servere

Tilgang til servere gis gjennom PAM Safeguard.

# 7. Backup og arkivløsning

## 7.1. Backup

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

## 7.2. Datasenter Disaster Recovery

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

# 8. Andre tekniske tjenester

## 8.1. Katalogtjenester

Microsoft Active Directory (2016) benyttes som katalogtjeneste for brukere og tjenester samt som intern DNS og DHCP.
AD og DNS er satt opp som redundante tjenester på alle DC-noder. Hoveddomenet HN er en enkel forest hvor hver lokasjon er definert som en site. Det er full-mesh replisering mellom sites.
DHCP er ikke redundant, og lokalt i hver enkelt site. DHCP design er under redesign og konkrete behov bør avklares mot nytt design.
Alle ansatte og innleide må være definert som brukere og autentisere seg mot Active Directory for å få tilgang til tjenester og ressurser i Helse Nord IKT s nettverk.
Hvert helseforetak er lagt inn som en egen organisasjonsenhet (OU) hvor tilknyttede brukere og utstyr er plassert i underenheter (sub-OU).

## 8.2. Fjernaksess

Helse Nord IKT har en fjerntilgangsløsning basert på Citrix Xenapp
Tilgang eksternt, definert som utenfor Helsenettet, tilbys via Citrix Netscaler Gateway.
Sikker autentisering ivaretas med tofaktorautentisering.

Det er i tillegg etablert en fjerntilgangsløsning for utstyr tilkoblet Siemens eller Phillips Remote services.

## 8.3. 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) og disse støttes i siste sertifiserte hovedversjon, men med mulighet for bruk av forrige hovedversjon i unntakstilfeller.

## 8.4. Web tjenester

Helse Nord IKT tilbyr en standardisert, regional web-plattform for å hoste primært egenutviklede web-applikasjoner hos Helse Nord.
Man tilbyr webtjenester basert på IIS 10 (Internet Information Services) og Apache Tomcat 7, med MSSQL og MySQL databaser. Som lastbalanserer/frontend benyttes F5 Big IP.
Alle servere tilknyttet løsningen kjøres virtuelt på SKM.

## 8.5. Fil- og Printtjeneste

### Filtjenester

Filservere er i hovedsak virtuelle servere med lagring mot SAN/NAS.
Fillagring er basert på Windows OS SMB 1.1 og nyere.
Filtjenesten benyttes primært for felles- og hjemmeområder samt som programområde og for software-distribusjon. Helse Nord IKT har filservere på alle lokasjoner for å sikre rask responstid.
Det benyttes DFS for noe data
Helse Nord IKT har pr. i dag ingen arkivløsning for filtjenesten.

### Printtjeneste

Windows Print servere på alle lokasjoner. Det er ingen redundans for utskriftstjeneste.
Printerobjektene er delt i Active Directory og printerne blir koblet opp automatisk via tilgangsstyring i AD. Alternativt brukerinitialisert oppkobling gjøres basert på særegne behov.
Helse Nord IKT har valgt Ysoft SafeQ som regional løsning for sikker utskrift.

## 8.6. Desktop infrastruktur

Helse Nord IKT har standardisert maskinvaren gjennom en nasjonal avtale for klientutstyr.
Helse Nord har rundt 16000 Stasjonære PCer hvorav det er management på 13000 av disse. I tillegg så har Helse Nord estimert rundt 3200 laptoper som per i dag ikke har noe management.
Maskinvaren er standardisert på følgende modeller: tre bærbare, en tablet, en desktop og en arbeidsstasjon. Tilbyderne på avtalen re-rangeres årlig, dermed kan man få et årlig modellskifte.
Komponenter som .Net og lignende kjøres alltid i siste versjon.
Klientene håndteres via Symantec Client Management Suite (CMS). Løsningen har en sentral infrastruktur og en desentralisert del på alle sykehus og større sentre.
Helse Nord IKT benytter Vpro som driftsverktøy og det er utført en stor mengde prosessautomatiseringer via Symantec Workflow.

Helse Nord benytter antivirus/ antimalware, per i dag er det Symantec Endpoint Protection.
RealVnc benyttes til fjernstyring av klienter.

## 8.7. Terminalservertjenester

Terminalservertjenesten er basert på Xenapp, og kjører på SKM. Serverne bruker Windows 2016 og applikasjonene er i hovedsak virtualisert med app-v.

## 8.8. Integrasjonstjenesten

Integrasjonsplattformen i Helse Nord består i hovedsak av MS BizTalk og IIS. Den brukes til å integrere fagsystemer med hverandre.
Integrasjonene benytter seg av standarder som HL7 v3, FHIR og KITH.XML.
Det er tre separate miljøer for Produksjon, Test og QA.

## 8.9. Sentral meldingsformidling

Helse Nord har etablert en sentral løsning for meldingsformidling for alle HF i Helse Nord levert av Ascom. Hensikten er å kunne la ansatte på sykehusene benytte mobiltelefoner og WiFi-baserte enheter for mottak av alarmer og tale.

Ascom-løsningen benytter:

- Android-baserte Myco 3 og Samsung xCover 5 for meldingsformidling. Kan utvides med flere tjenester mot Ascom Healthcare Platform.
- Unite Platform Server for meldingshåndteringen
- Unite Axess for å sende meldinger til og fra smartenheter (som Ascom Myco 3)

Tjenesten benytter mobile device management (MDM)/ enterprise mobility management (EMM) med støtte for Android og iPhone.

## 8.10. Sårbarhetssjekk

Helse Nord IKT gjør jevnlige ports- og sårbarhetssjekker av Helse Nords infrastruktur, og til dette benyttes vanligvis verktøyene Nmap[1]og Nessus Pro[2]. Verktøyene vil kunne byttes ut etter behov. Helse Nord benytter også HelseCERT[3] til å gjøre årlige penetrasjonstester mot Helse Nords infrastruktur. Enkelte komponenter i infrastrukturen vil da kunne bli utsatt for ekstra grundige sjekker.

## 8.11. Identitets-og tilgangsstyring

Tjenesten leverer PAM (Privileged Access Management), IAM (Identity and Access Management) og autorisasjonsløsninger for Helse Nord.

PAM
Software: One Identity Safeguard
Pr 1.1.22 skal all privilegert tilgang (admin-tilganger) til servere gjøres gjennom PAM.
I fremtiden skal all privilegert tilgang til system, nettverksutstyr, klienter etc også gjøres gjennom PAM.

IAM
Software: One Identity Manager
IAM ble innført i Helse Nord IKT i oktober, 2022. Det betyr at alle nye ansatte automatisk får en bruker i AD, en e-postboks i Exchange og tilgang til Teams, distribusjonslister og filområder. Hvilken tilgang en nyansatt skal få er kartlagt med den enkelte linjeleder, og baseres på stillingskode og organisasjonstilhørighet. Tilganger gis på bakgrunn av en aktiv arbeidskontrakt i Personalportalen. I mars 2023 er deler av BAS erstattet med Tilgangsportalen som er den nye selvbetjeningsportalen for å bestille og administrere tilganger i HN IKT.

Planen er videre er rulle IAM-løsning i de andre helseforetakene.
Nye systemer og applikasjoner må kontakte IOTS for å forhånds definere roller og tilganger for å få aktivert automatisert tilgangsstyring.

AUTORISASJON

[1] https://nmap.org/
[2] https://www.tenable.com/
[3] https://www.nhn.no/helsecert/

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 tofaktorautentisering ved pålogging til skytjenester der det behandles personopplysninger, virksomhetsintern informasjon eller annen sikkerhetskritisk informasjon.
Tjenester og applikasjoner skal ikke benytte interne/egne autentiseringsløsninger men basere autentiseringen på godkjente regionale autentiseringsløsninger.
Ved anskaffelse av nye tjenester eller oppgradering av eksisterende tjenester og applikasjoner skal autentisering baseres på internasjonalt anerkjente åpne protokoller.

# 9. Støttetjenester

## 9.1. Service Desk

Helse Nord IKT har en regional servicedesk som single point of contact for Helse Nord.
Servicedesken er lokalisert i Tromsø og er bemannet kl. 08.00-15.30, i tillegg til en 24/7 driftsvakt. Ansatte er fordelt mellom generell brukerstøtte og klinisk brukerstøtte på sykehusenes journalsystem (DIPS og MetaVision).
ITIL er valgt som prosessrammeverk for håndtering av kundehenvendelser. HP Service Manager brukes som verktøy. Det mottas mellom 100 000-120 000 henvendelser til servicedesken pr. år.

## 9.2. Pakking og distribusjon av Software

På Windows 10 klientoperativsystem brukes Microsoft App-v som virtualiseringsteknologi, på VDI brukes også Appvolumes, før april 2026 må leverandørene støtte MSIX da App-V når EOL.
Pakkene leveres så direkte til enhet med CMS (Symantec Client Management Suite) eller strømmes til bruker med Microsoft App-V.
I de få tilfeller hvor virtualisering ikke er mulig benyttes MSI eller annen scriptbasert installering.

# 10. Livssyklus for tredjepartsprodukter

## 10.1. Bakgrunn

Livssyklus for operativsystemer knyttet til nettverksutstyr, lagringsløsninger, servere, databaser etc. defineres av SPM-prosessen (Service Portfolio Management). Hensikten er å sikre en effektiv og forutsigbar livssyklusstyring, slik at vi unngår operasjonelle- og sikkerhetsmessige risikoer.
Tabellen under er gjeldene for alle produkt og skal benyttes av samtlige prosesser som innfører nye system

## 10.2. Avvik

Avvik tillates i utgangspunktet ikke. Hvis det gjøres unntak, så skal det være som følge av en behandling i porteføljeprosessen, eller tjenestestyret.

## 10.3. Oversikt over produkters livssyklus

Leverandører har sin start- og sluttdato (end-of-life, EOL) for sine produkt. I utgangspunktet støttes siste versjon av et produkt innenfor EOL, men da HN IKT trenger noe tid på å sertifisere produktene så innebærer dette at HN IKT må ha en egen livssyklus startdato for et produkt som er noe etter det leverandøren har. Som et eksempel kan dette være Windows server 2016. HN IKT kan ikke være klar til å støtte dette på samme dag som Microsoft slipper dette, dermed er HN IKT sin startdato være noe etter det Microsoft har.

Tilsvarende så må HN IKT ha en egen end-of-life dato for å sikre at vi har utfaset alle komponenter den dagen leverandøren slutter å støtte produktet. I eksempelet over så vet vi at support opphører i 2027. Da må HN IKT ha utfaset alle installasjoner innen den dato, det betyr at HN IKT sin dato for end of life er tidligere. Videre vil det også være en enda tidligere dato for når vi slutter med nyinstallasjoner. Denne siden har informasjon om alle sentrale produkt med livssyklus, både leverandørens og HN IKTs.

### RedHat Enterprise

| Produktversjon | HN IKT Start | HN IKT End | End of Full Support | End of Maintenance Support 2 (Product Retirement) |
|---|---|---|---|---|
| RedHat Enterprise 7 | | *Kommer* | Q4 2019 | 30.06.2024 |
| RedHat Enterprise 8 | | | 31.05.2024 | 31.05.2029 |
| RedHat Enterprise 9 | | | 31.05.2027 | 31.05.2032 |

### Windows Server

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Support end | Extended support end-date |
|---|---|---|---|---|---|
| Windows Server 2016 Datacenter Core | 15.10.2016 | | *Kommer* | 11.01.2022 | 11.01.2027 |
| Windows Server 2016 Standard | 15.10.2016 | | *Kommer* | 11.01.2022 | 11.01.2027 |
| Windows Server 2019 | 13.11.2018 | | *Kommer* | 09.01.2024 | 09.01.2029 |

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Support end | Extended support end-date |
|---|---|---|---|---|---|
| Windows Server 2022 | 18.08.2021 | | *Kommer* | 13.10.2026 | 14.10.2031 |

## Windows klient

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Support end | Extended support end-date |
|---|---|---|---|---|---|
| Windows 10 21H2 | | 01.06.2019 | N/A | 01.12.2027 | 01.12.2027 |
| Windows 11 | | *Kommer* | N/A | | |

## Andre versjoner av Linux OS

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Support end | Extended support end-date |
|---|---|---|---|---|---|
| Oracle Linux 6 | | | | | |
| Oracle Linux | | | | | |
| Ubuntu Linux | | | | | |
| Suse Linux | | | | | |

## MS SQL Server

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Sup.port end | Extended support end-date |
|---|---|---|---|---|---|
| MS SQL Server 2016 SP2 | 24.04.2018 | | Ingen ny install på denne versjon | 13.07.2021 | 14.07.2026 |
| MS SQL Server 2017 | 29.09.2017 | 13.12.2018 | N/A | 11.10.2022 | 12.10.2027 |
| MS SQL Server 2019 | 04.11.2019 | 20.11.2020 | | 07.01.2025 | 08.01.2030 |

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Sup.port end | Extended support end-date |
|---|---|---|---|---|---|
| MS SQL Server 2022 | 16.11.2022 | | | 11.01.2028 | 11.01.2033 |

## MySQL

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Support end | Extended support end-date |
|---|---|---|---|---|---|
| MySQL 5.7 | 01.10.2015 | 01.10.2015 | 01.10.2023 | 01.10.2020 | 01.10.2023 |
| MySQL 8 | | 2020 | | | |

## Oracle

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Support end | Extended support end-date |
|---|---|---|---|---|---|
| Oracle 19c | | 2020 | Senest April 2027 | April 2024 | April 2025 no fees<br><br>April 2027 with fees |

## Microsoft .NET Framework

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Support end | Extended support end-date |
|---|---|---|---|---|---|
| Microsoft .NET Framework 3.5 SP1 | 18.11.2008 | | 10.10.2021 | 10.10.2023 | 10.10.2028 |
| Microsoft .NET Framework 4.5.2 | 05.05.2014 | | | | Følger livssyklus til OS |
| Microsoft .NET Framework 4.6.1 | 30.11.2015 | | | | Følger livssyklus til OS |
| Microsoft .NET Framework 4.6.2 | 02.08.2016 | | | | Følger livssyklus til OS |
| Microsoft .NET Framework 4.7 | 11.04.2017 | < 2018 | N/A | N/A | Følger livssyklus til OS |

| Produktversjon | Start lifecycle | HN IKT Start | HN IKT End | Mainstream Support end | Extended support end-date |
|---|---|---|---|---|---|
| Microsoft .NET Framework 4.7.1 | 17.10.2017 | < 2018 | | | Følger livssyklus til OS |
| Microsoft .NET Framework 4.7.2 | 30.04.2018 | N/A | | | Følger livssyklus til OS |
| Microsoft .NET Framework 4.8 | | | | | Følger livssyklus til OS |

## 10.4. Arbeidsstasjon

Dersom skanneren leveres med tilhørende arbeidsstasjon (pc) bør følgende krav kunne oppfylles:

1. Installere HN IKT sin Antivirusprogramvare.

2. Kjøre Microsoft Security Baseline. Dette innebærer:

- Applocker

- Bitlocker

- Credential Guard

- Konto som det logges på med skal ikke være lokaladministrator

3. Følgende bør kunne patches:

- Firmware (Bios og annet hardware)

- Operativsystem med runtime kompontenter (.NET vcred og lignende)

- Tredjeparts software (For eksempel Adobe eller lignende)

4. Det bør innlemmes i management system for å kunne administreres (Per nå betyr dette Altiris Agent).