Sykehuspartner | HELSE SØR-ØST

Purchase Agreement

Agreement governing the purchase of software and equipment

The Norwegian Government's Standard Terms and Conditions for IT Procurement

SSA-K 2018

Tender for delivery of Advanced Unit Dose Packaging and Dispensing Solution

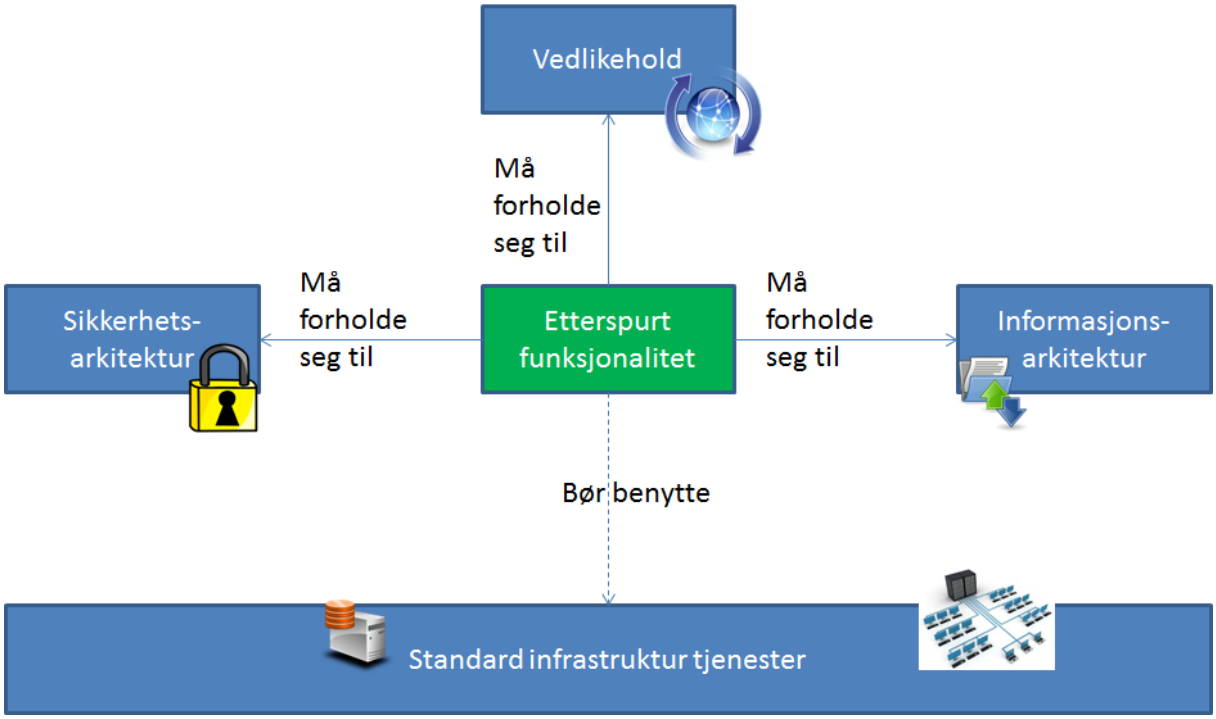
SSA-K Appendix 3a Customer Technical Platform

Case number: 2022/512

Innholdsfortegnelse

1 Introduksjon

Sykehuspartner søker på vegne av Helse Sør-Øst at løsninger som anskaffes tilfredsstiller grunnleggende krav som dekker sikkerhet, integrasjon og vedlikeholdbarhet. Dette dokumentet fremstiller de overordnede prinsippene som gjelder på disse områdene.



2 Arkitekturprinsipper

Helse Sør-Øst mener det er visse egenskaper som er viktige for alle løsninger som skal innføres. Disse egenskapene er nedfelt som arkitekturprinsipper.

Helse Sør-Øst anser visse egenskaper som viktige for alle løsninger som skal innføres. Disse egenskapene er nedfelt som arkitekturprinsipper, og er nærmere beskrevet i følgende dokumenter:

- DIFIs «Overordnede IT arkitekturprinsipper for offentlig sektor»
- DIFIs «Arkitekturprinsipper for samhandling»
- Nasjonal IKT «Arkitekturprinsipper i spesialisthelsetjenesten»

Det vises også til prinsippskissene rundt referansearkitektur beskrevet i kapitel 3.

2.1 Bimodal IT

Helse Sør-Øst ønsker å tilfredsstille de relevante brukergruppenes behov på en best mulig måte samtidig som man sikrer sikker og stabil drift. Man ønsker så langt det er mulig å legge til rette for å inkludere alle relevante brukergrupper så som innbyggere, pasienter, pårørende, helsearbeidere og forskere. Dette medfører en balansegang mellom proaktiv videreutvikling av løsninger i tett samarbeid med brukergruppene opp mot restriktiv endringskontroll på tjenester som er kritiske.

2.2 Skybasert

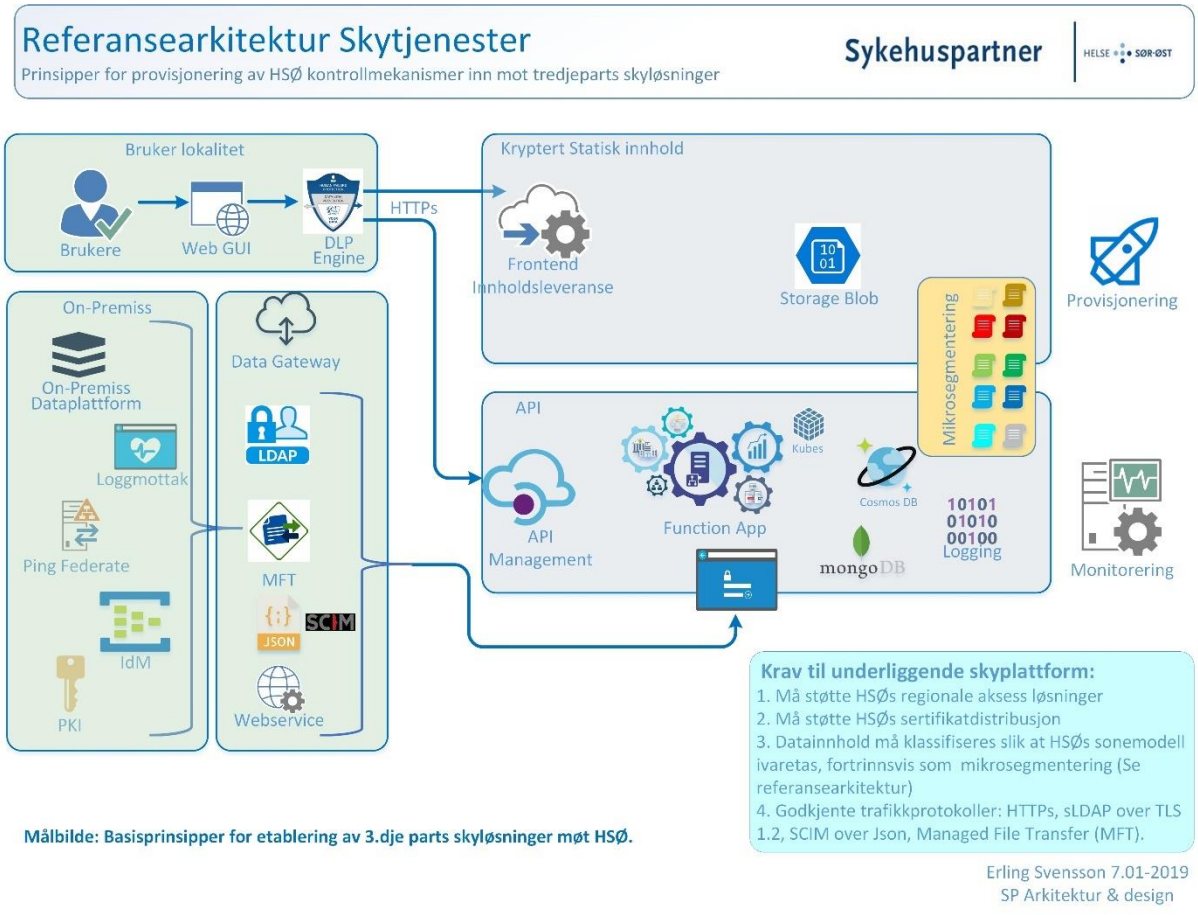
Helse Sør-Øst ser at de prinsippene som gjelder for skybasert løsninger har stor verdi også for løsninger som skal tilbys helseforetakene. Sykehuspartners Managed Private Cloud (MPC) skal benyttes som driftsplattform. Prinsippene for skybasert løsninger er tydeligst uttrykt i NIST standarden hvor de viktigste elementene er:

- Selvbetjening
- Skalering og tilgjengeliggjøring av ressurser ved behov
- Kostnader som korrelerer med bruk
- Det er spesielle krav til plassering av informasjon i kontekst 3 og 4 i ski baserte løsninger. Det vises til direktoratet for e-helse sine retningslinjer i så måte.

Det er for øvrig protokolkrav til autentisering/autorisering, kryptering samt krav til slusemekanikk i forhold til slike løsninger.

Det vises til bilag 3 i så måte.

Prinsipp rundt sky baserte løsninger er antydet i referansearkitektur nedenfor:



2.3 Informasjonsdeling

Helse Sør-Øst ønsker å legge til rette for at informasjon fra fagsystemene gjøres tilgjengelig til brukere der disse måtte befinne seg på en sikker måte. Det betyr at Helse Sør-Øst erkjenner at for enkelte typer informasjon så vil det være nødvendig at denne kan deles med individer som ikke er ansatt i Helse Sør-Øst og som derfor heller ikke har Helse Sør-Øst definert utstyr eller tilgang til Helse Sør-Øst sine lokasjoner. Tilganger for ikke-autentiserte brukere

2.4 Grønn IT

Helse Sør-Øst ønsker å fremme bærekraftig bruk av IT. Dette gjelder både bruk av råmaterialer, energi og menneskelige ressurser både hos leverandøren og eventuelle underleverandører. Helse Sør-Øst forholder seg til føringer fra Grønn IT (https://www.ikt-norge.no/bransjenormer-guider/gronn-it/) ved anskaffelse, etablering, drift og forvaltning av IKT-plattformen og løsninger etablert i IKT-plattformen.

2.5 Livssyklus

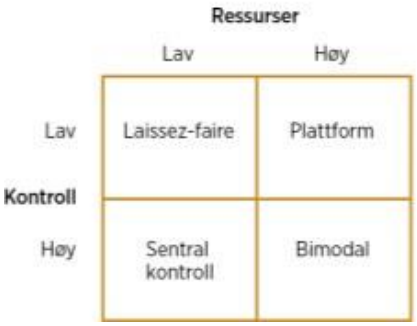
Helse Sør-Øst er opptatt av at løsninger skal kunne vedlikeholdes og videreutvikles løpende, såkalt «Lifecycle Management». Operativsystem og programvare vil normalt støttes i gjeldende hovedversjon, samt forrige hovedversjon (n, n-1). Dette gjelder eksempelvis komponenter og tjenester:

- levert av Kundens tjenesteleverandør, og ikke inngår i leveransen av løsningen
- levert som en del av løsningen
- levert av 3.part

Løsningen må derfor kontinuerlig oppdateres og vedlikeholdes for å imøtekomme dette prinsippet. Merk at dette også medfører at løsningen må støtte løpende patching og oppgraderinger i Kundens tekniske plattform.

2.6 Oversikt over styringsmodeller

STYRINGSMODELLER



DEFINISJONER

Ressurser: Tiltak for å legge til rette for innovasjon med lettvekts-IT

Kontroll: Tiltak for å regulere bruken av lettvekts-IT

Laissez-faire: Tillater lokal eksperimentering og bruk, men ingen sentral støtte

Sentral kontroll: Bruken av lettvekts-IT er underlagt den sentrale IT-avdelingen

Plattform: Klargjort ansvars- og oppgavefordeling mellom tungvekt- og lettvekts-IT

Bimodal: Lettvektsløsninger utvikles hos lokale enheter, men settes i produksjon i henhold til standarder og retningslinjer satt av den sentrale IT-avdelingen

3 Referansearkitektur

Referansearkitektur skal etablere grunnleggende prinsipper i forhold til ulike scenarioer

3.1.1 Operativsystem

Plattformkrav er den til enhver tid siste versjon n av plattformene Microsoft Windows server og RHEL. Det kan leveres n-1. Andre versjoneringer må begrunnes.

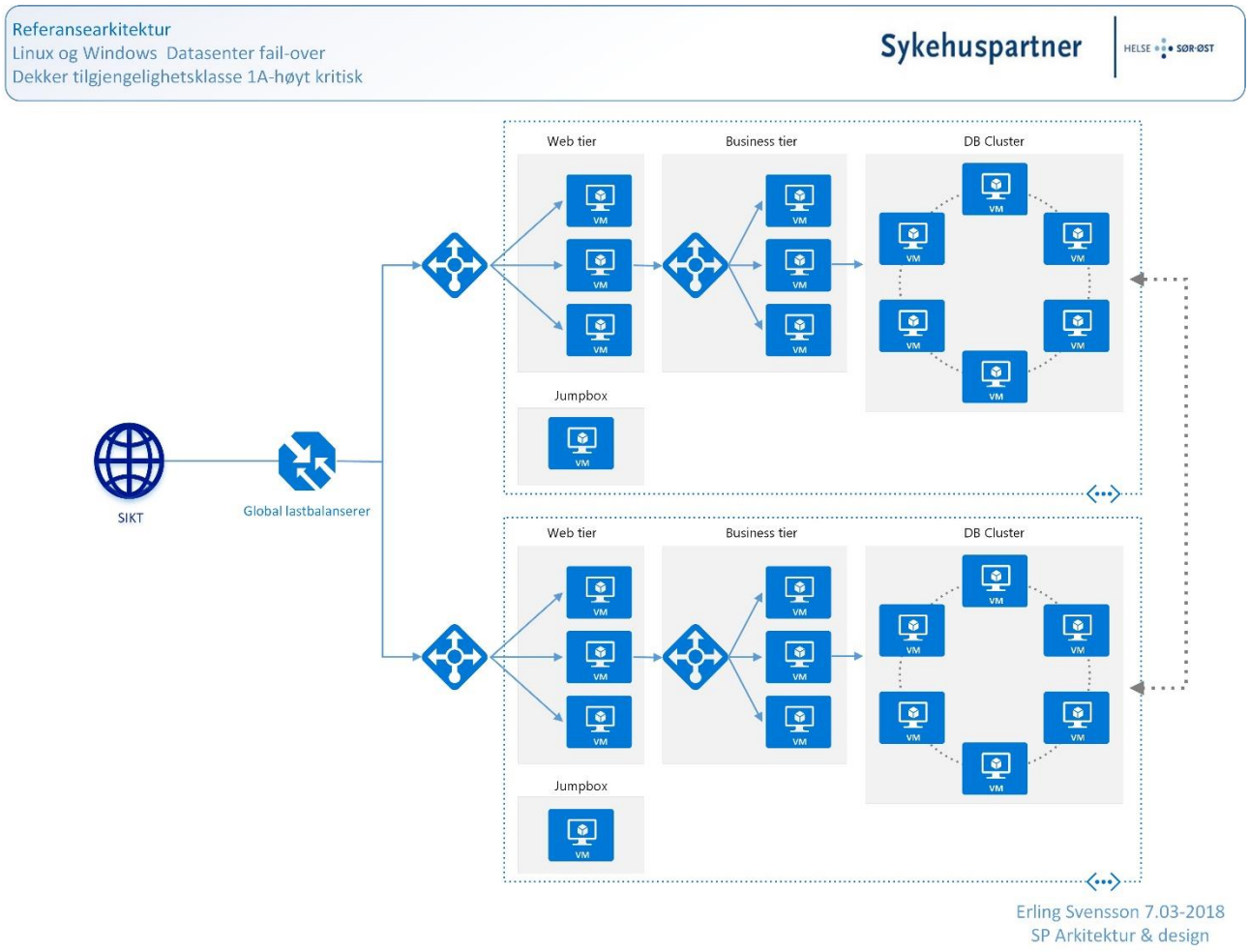
3.1.2 Datasenter fail-over

Denne referansen tilfredsstiller følgende kriterier:

Kritikalitet = 1-Høyt kritisk

RPO = 0

RTO = 60 minutter



3.1.3 Databaseplattform

Det benyttes enten Microsoft SQL server eller Oracle som databaseplattform standard edition eller Enterprise.

Det må benyttes den til enhver tid høyeste versjon eller n-1.

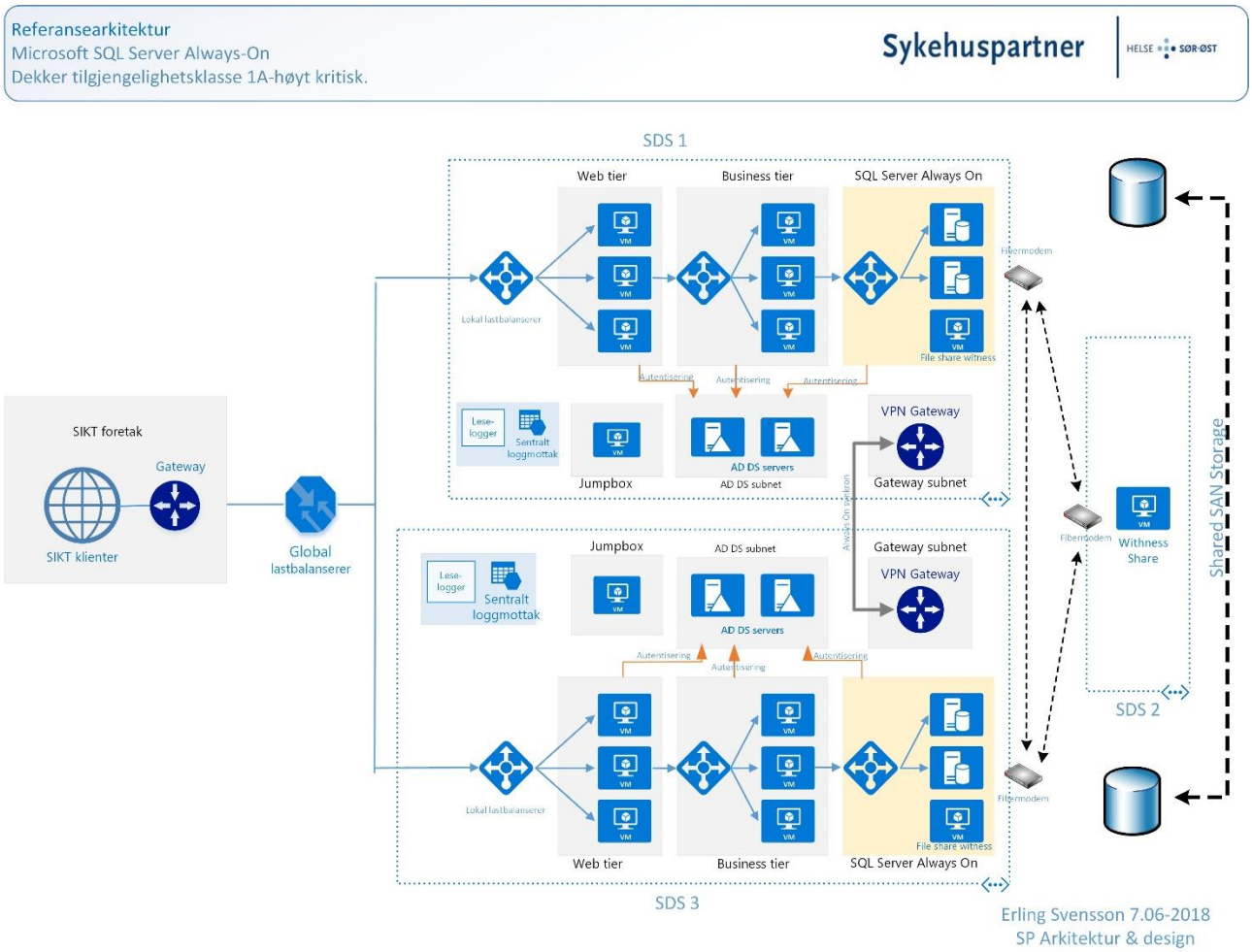
Lavere versjoner må begrunnes.

For 1-høyt kritiske løsninger er det følgende krav:

Microsoft SQL server skal være Enterprise Edition og med Always-on funksjonalitet.

Oracle skal kjøres på fysiske RAC og ikke virtuelt. Det skal kunne benyttes MMA.

3.1.3.1 Microsoft SQL Server Always On



Løsningen fordrer spesial dedikerte konfigurasjoner:

Collation: DA-NO

Disk konfigurasjon

1. Disk oppsett: C=OS, D=SQL Bin,E=UserDB,F=UserLog/TempDB Log, G=Backup, T=TempDB,P=PageFile

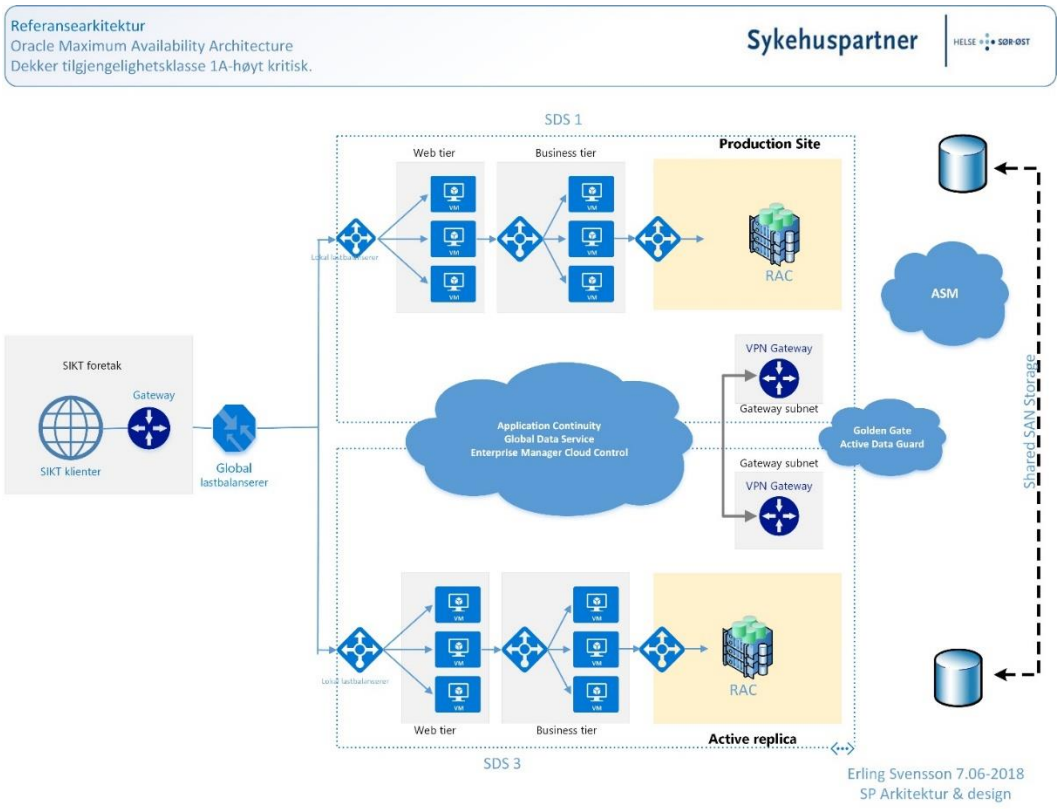
2. Alle disker unntatt C, G og P settes opp med 10GB hvis ikke noe annet er spesifisert. Bestiller av server bestemmer størrelse. C settes opp standard med 40GB, G settes opp med (E*3)GB og P settes opp (minne*1,5)GB.
Systemdisk kommer i tillegg.
Konfigurasjon

Disk stasjon	Label/Katalog	Funksjon	Størrelse(standard)	Årlig vekst %
C:	OS	OS bin filer	40GB	
D:	MSSQLBin	SQL bin filer	10GB	
E:	MSSQLUserDB	Database filer	10GB	
F:	MSSQLUserLog	Database Log filer	10GB	
G:	MSSQLBackup	SQL Backup dump filer	30GB	
P:	PageFile	PageFile	12GB	
T:	MSSQLTempDB	TempDB database fil	10GB	

3.1.3.2 Oracle Maximum Availability Architecture (MAA)

Denne modellen avviker fra HSØ Sør-Østs standard om foretrukket virtuell plattformetablering.

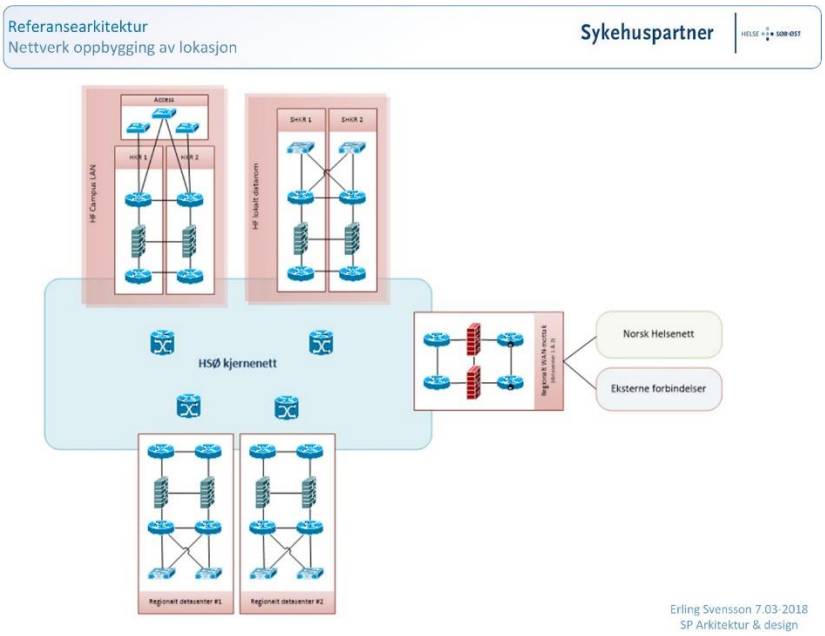
Bruk av Oracle RAC krever fysiske noder.



3.1.4 Datasenterlokasjoner

Datasentre i HSØ er bygget opp rundt 2 regionale datasentre (SDS1/SDS3), med enkeltstående lokale datasentre (SHKR xx) tilknyttet det enkelt HF.

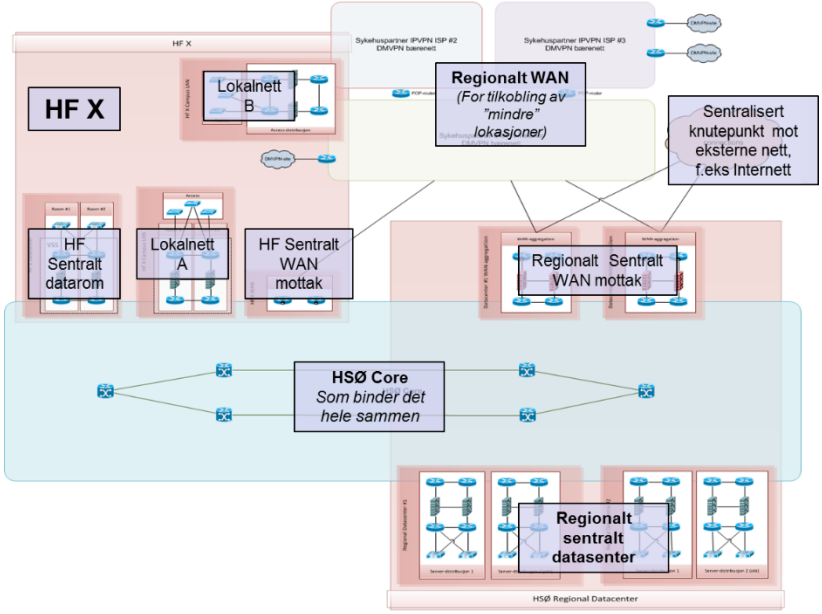
Det er i tillegg etablert ett regionalt datasentre for backup/restore lokalisert på Ahus (SDS3). Her plasseres det også Withness share for MS SQL Always On løsninger definert som 1-høyt kritisk. Ahus har i tillegg også lokalt datarom (SHKR1)



3.1.5 HSØs kjernenett

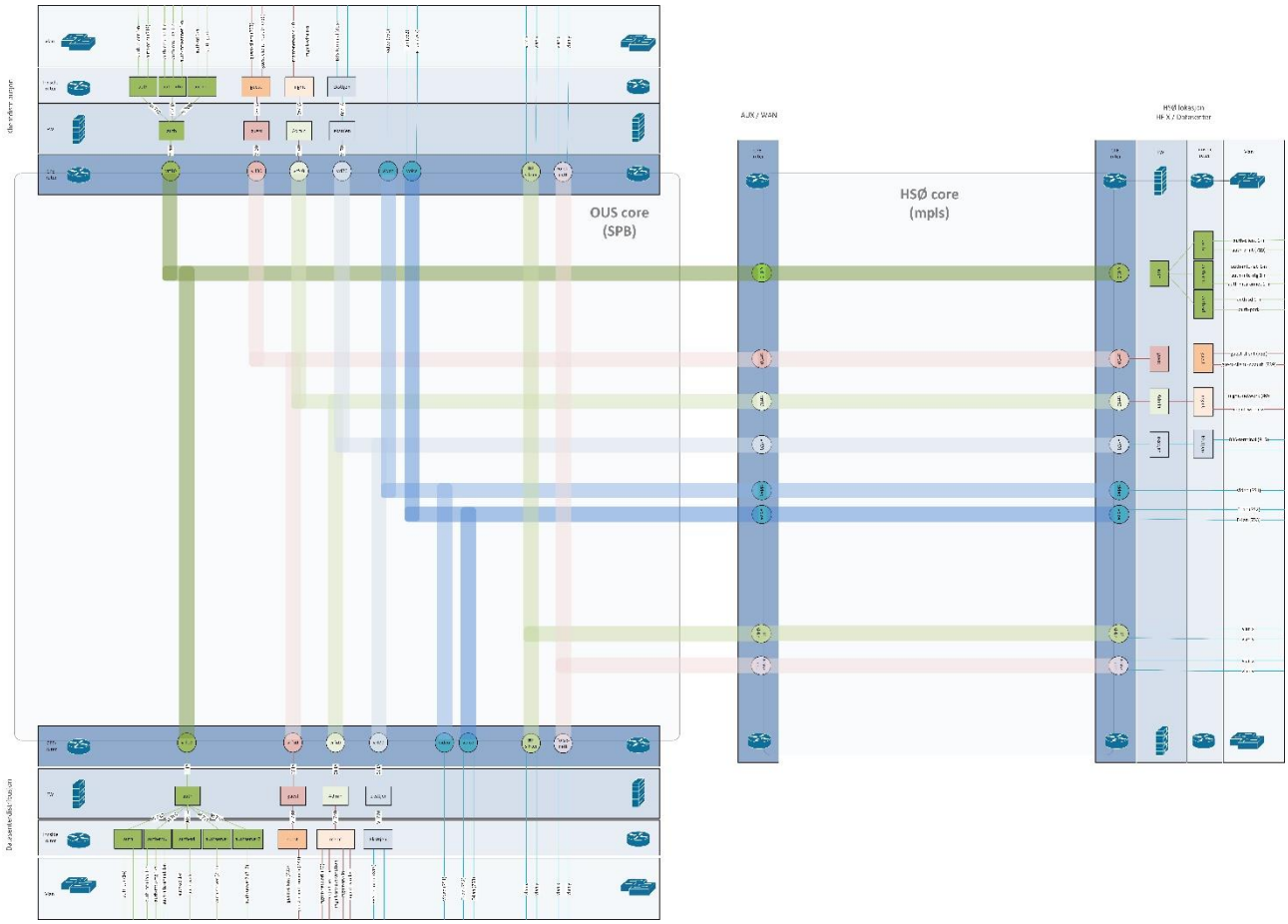
Kjernettet er bygget opp som MPLS ringkjerne med det enkelte HF etablert som fjernlokasjon tilkoblet MPLS over dedikerte WAN mottak. Regionale datasentre er håndtert på samme måte.

OUS benytter SBP lokalt, men er etablert med WAN mottak på samme måte.



3.1.6 MPLS ruting (VRF)

Det er satt opp standardisert ruting med VRF dedikert ulike typer trafikk (Data, video, Telecom, SAN etc.). VRF datatrafikk er etablert med VRF 10 regionalt.
OUS er satt opp med eget VRF for datatrafikk, VRF 110 dette på grunn av avvik fra MPLS standarden. Det er imidlertid ingen forskjell på konfigurasjoner, ettersom VRF 110 er en kopi av VRF 10. Alle andre VRF'er er imidlertid standard for alle HF og regionale datasentre.
Skisse vist under.

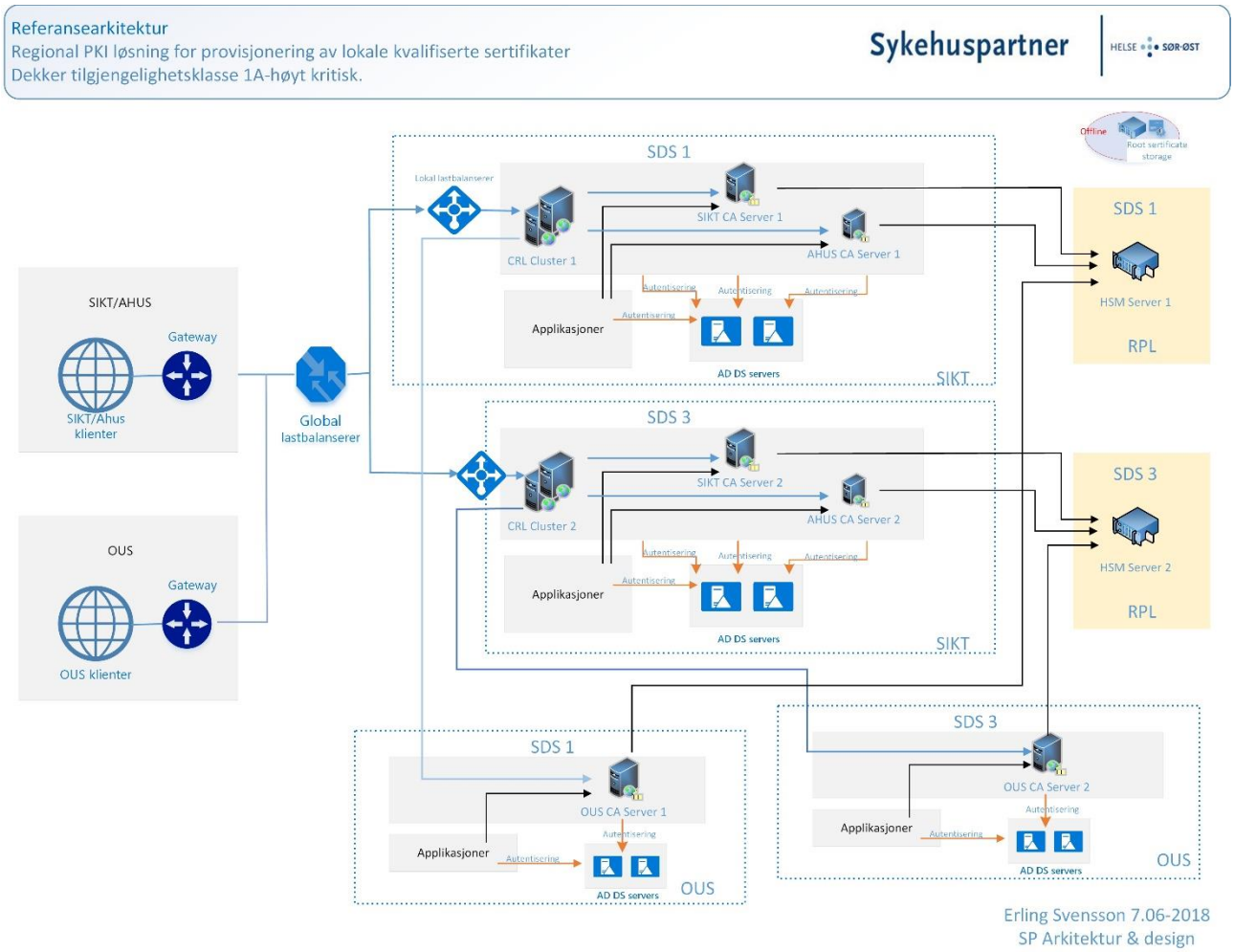


3.2 Sertifikatbasert kryptering, Public Key Infrastructure (PKI)

HSØ har under etablering en Regional Sentralisert løsning for distribusjon av lokale kvalifiserte sertifikater. Det forutsettes at alle applikasjoner gjør bruk av denne krypteringsmekanismen for all samtrafikk.

Det henvises til følgende publikasjoner for mer detaljer rundt protokoller og krypteringsmekanismer: SP-S-INSTRUKS-06 - Kryptografi i Sykehuspartner

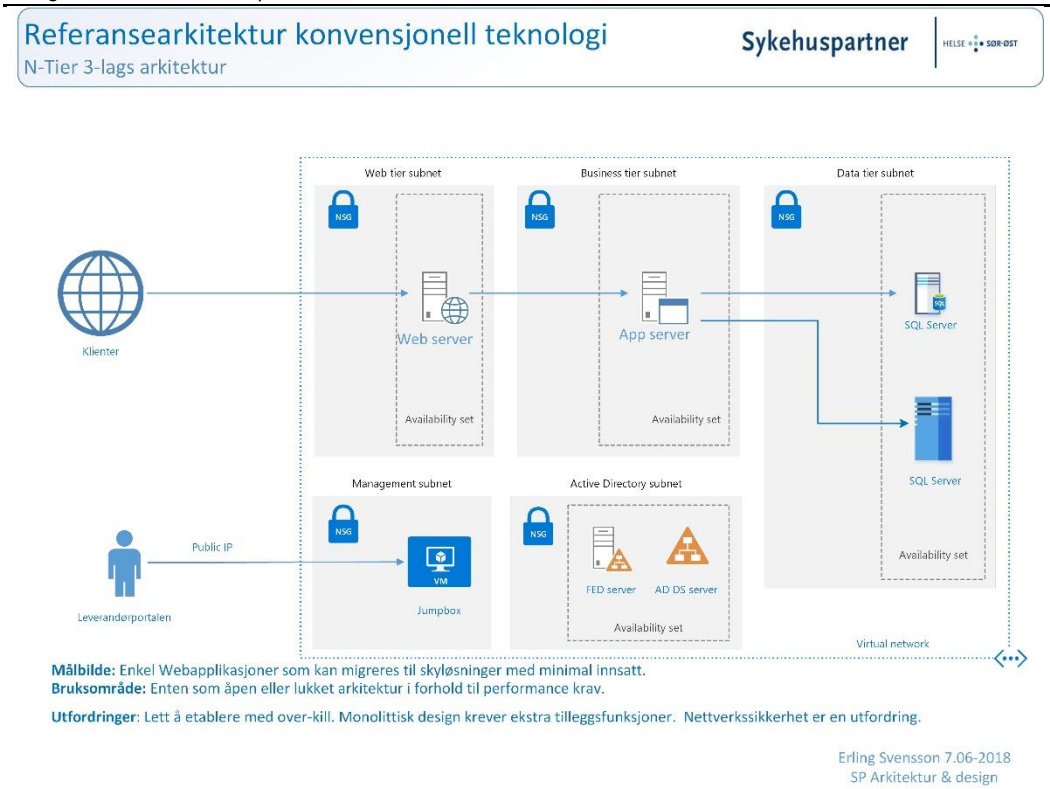
Skisse viser prinsipp for PKI



3.2.1 Applikasjonsarkitektur.

Det er ett krav at applikasjoner skal bygges opp som 3-lagsarkitektiur. Klienter skal ikke ha tilgang til filområder på generell basis og det gis ikke klient tilgang til database eller RDP.

Det vises til skisse nedenfor rundt prinsipp:



3.2.2 Lagring, backup og arkivering

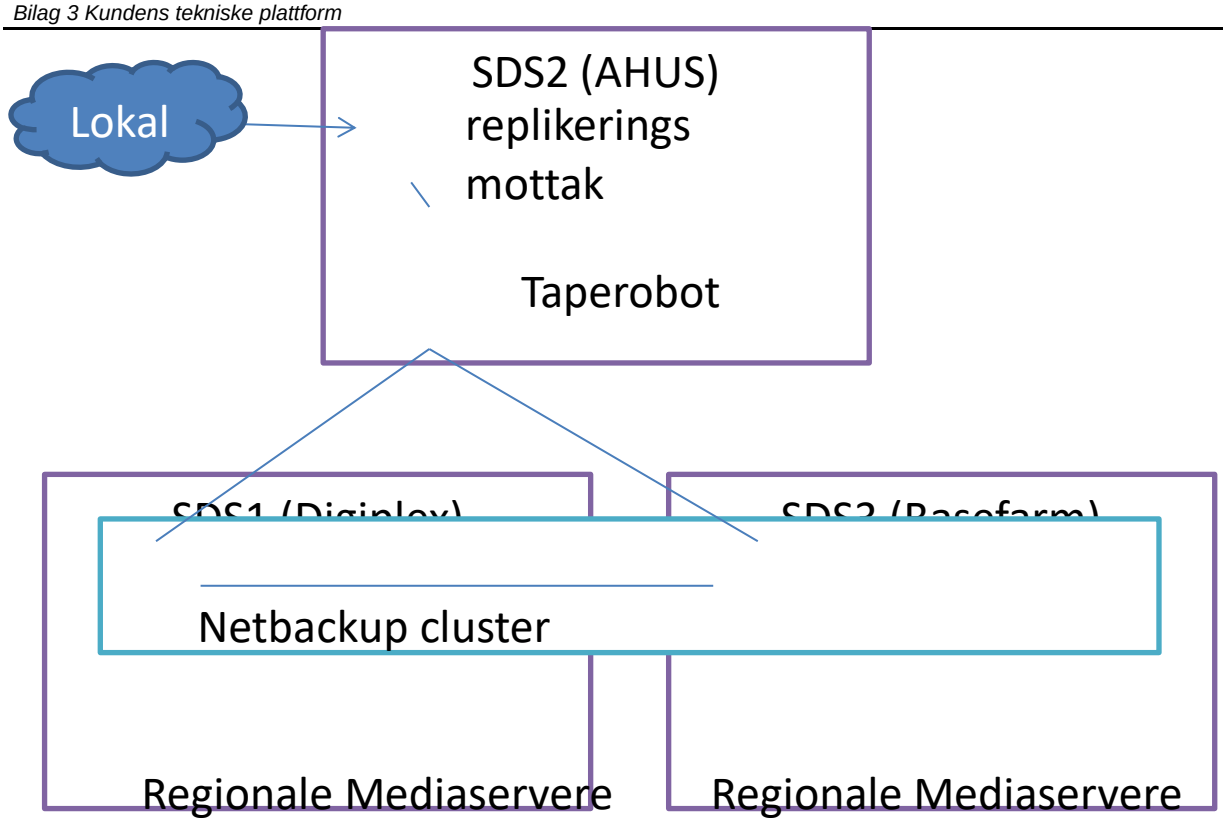
3.2.2.1 Backup

Applikasjonen som benyttes for all backup i Sykehuspartner er Symantec NetBackup. De aller fleste sykehusene har historisk benyttet denne applikasjonen lokalt ettersom den har bred støtte for applikasjoner og operativsystem - Inkludert gamle legacy plattformer som AIX, Solaris, HPUX og NetWare. Nye tjenester etableres så langt det er mulig kun på Windows og Linux. Sykehuspartner har tre sentrale datarom (datasentere) i Osloregionen, hvor to kjører aktiv produksjon:

- SDS1 på Digiplex
- SDS3 på Basefarm

Det tredje er tiltenkt backupdata og katastrofeløsninger

- SDS2 på AHUS



Det eksisterer to regionale backupmiljø.

Følgende sykehus har lokal backup infrastruktur:

Foretak	Lokasjon	Masterserver	Taperobot
OUS	Ullevål Aker Rikshospitalet	nbma.ullevaal.uus.no sds-bckaker-01.akersykehus.no rhs-backup-01.ous-hf.no	Ullevål
SØHF	Fredrikstad Kalnes	soback01.so.hf.no spg-backup-01.sikt.sykehuspartner.no	Fredrikstad (lokal) Repl. til SDS2
SIHF	Gjøvik	bcksi01.sihf.no	Fjellhallen (lokal)
Sunnås		sun-backup-01.sunnaas.no	
SIV	Tønsberg	tbgnb1	Tønsberg
SSHF	Arendal	are-backup-01.sikt.sykehuspartner.no	Arendal
VVHF	Drammen Ringerike Bærum	sb-backup.sb-hf.no penny nbumaster	Drammen (lokal robot) Lokal robot Lokal robot
STHF	Skien	nbhsm	Lokal robot
AHUS	Ahus	Mrhat.ahus.no	Taperobot I SDS1

Standard SLA på backup

Da backup er en tung belastning for nettverk og disksystem er de aller fleste backupjobbene satt opp til å kjøre utenom vanlig arbeidstid, 17:00 til 05:00, med hovedtyngden av jobber etter midnatt. Jobber kan unntaksvis settes opp til å gå på dagtid, hvis det er spesielle grunner til det.

Vi har definert forskjellige nivåer på backup. Ikke alle nivåene kan leveres på alle lokasjoner. Her vil skjønn bli benyttet slik at man oppnår tilfredsstillende beskyttelse i henhold til bestilling. Vi tenker at de forskjellige nivåene (gull, sølv, bronse) skal gjenspeile kritikaliteten til tjenesten.

Teknologien endres hele tiden. Hvordan man tar backup kan derfor endres uten forvarsel, så fremt dette er innenfor SLA.

Ved store hendelser for mange tjenester er berørt, kan det bli fravik fra SLA siden restorehastighet begrenses av infrastruktur. Nettverk er som ett eks strupet til 15gbit/s inn og ut fra backupnett.

Nivå Gull

Backup finnes alltid på disk for rask restore. Disse jobbene vil få førsteprioritet i vårt backupsystem. Dette styres automatisk. Inkrementell backup hver natt. Full backup en gang pr. uke.

Eldre backuper ligger på tape. Leveres på regionale tjenester fra SDS1 og SDS3.
Recovery Point Objective: mindre enn 24 timer
Recovery Time Objective: inntil 500MB/s

- Daglig backup man-tir-on-tor-lør-søn, inkrementell (må kombineres med siste fulle backup)
- Ukentlig backup fredager
- Månedlig backup første fredag i måneden

Standard holdetider (oppbevaring):

- Daglig backup: 1 måned, eller 3 måned
- Ukentlig Backup: 3 måneder, 6 måneder eller 12 måneder
- Månedlig backup: 12 måneder

Årlig backup som lagres i 10 år kan bestilles som ekstra opsjon.

Typiske tjenester hvor dette nivået er aktuellt er: EPJ, LAB, PACS/RIS

Restore av nivå gull har høyeste prioritet i henhold til SLA. Ved en restoresak påbegynnes arbeidet så fort som mulig. Vaktavtalen styrer responstider utenfor vanlig arbeidstid.

Nivå Sølv

Inntil 4 TB per klient. Inkrementell backup hver natt. Full backup en gang pr. uke. Leveres på alle lokasjoner.
RPO: mindre enn 24 timer
RTO: inntil 150MB/s

- Daglig backup man-tir-on-tor-lør-søn, inkrementell
- Ukentlig backup fredager
- Månedlig backup, første fredag i måneden

Standard Holdetider(oppbevaring)::

- Daglig backup: 1 måned, eller 3 måned
- Ukentlig Backup: 3 måneder
- Månedlig backup: 3 måneder

Årlig backup som lagres i 10 år kan bestilles som ekstra opsjon.

Sølv prioriteres foran bronsejobber ved restore. SLA-brudd om restorejobb ikke er påbegynt i løpet av 24 timer.

Nivå Bronse

Backup til disk, kopi til tape. Inntil 4 TB per klient. Inkrementell backup hver natt. Full backup en gang pr. uke. Leveres på alle lokasjoner.
RPO: mindre enn 24 timer
RTO: inntil 100MB/s

Daglig backup man-tir-on-tor-lør-søn
Ukentlig backup fredager
Månedlig backup, første fredag i måneden

Standard Holdetider(oppbevaring)::

- Daglig backup: 1 måned, eller 3 måned
- Ukentlig Backup: 3 måneder
- Månedlig backup: 3 måneder

SLA-brudd om restorejobb ikke er påbegynt i løpet av 72 timer

Nivå Arkiv

Backup til tape. Inntil 100 TB per klient. Daglig eller ukentlig kumulativ backup. Full backup en gang pr kvartal. Leveres på alle lokasjoner. Benyttes primært til å ha ekstra historiske kopier av store billedarkiver. *Kombinasjonen av store datamengder og moderat RTO gjør at en full restore av alle data er tidkrevende, og dataene bør ha en annen primærbeskyttelse..*

RPO: mindre enn 7 dager
RTO: inntil 100MB/s

Ukentlig kumulativ backup fredager: lagres i 6 måneder
Kvartalsvis full backup fredager: lagres i 12 måneder.

Årlig backup som lagres i 10 år kan bestilles som ekstra opsjon.

SAN lagring

Isilnenyttes der man har krav om god ytelse/mange samtidige brukere. Gode kandidater er:

- Fellesområder (Gull)
- Hjemmeområder
- Arkivdisk (Bronse)

Passer ikke til alt. Eksempelvis: Databaser, transaksjonsintensive applikasjoner, eller applikasjonsområder, mye småfiler. Her benyttes det GAD

For fellesområder, hjemmeområder:

- Daglig snapshot: kl0900, kl1100, kl1300, kl1500
- Ukentlig snapshot: Fredager kl1800
- Månedlige snapshot: 1. fredag i måneden kl1800

Standard holdetider (oppbevaring):

- Daglige snapshot: 20 kopier – dvs 5 dager
- Ukentlige snapshot: 8 – dvs 8 uker
- Månedlige snapshot: 12 – dvs 12 måneder.

For arkivtjenester:

Arkiv er mer statisk. Det er dessuten færre som har direkte tilgang til dataene. Vi vurderer derfor behovet for snapshot på denne tjenesten som mindre

- Daglig snapshot i 14 dager
- Ukentlig snapshot i 10 uker

Leveres på regionale tjenester fra SDS1 og SDS3.

Ved store arkiv som er plassert regionalt har vi speilet data mellom 2 datarom. I slike tilfeller kjøres full backup til tape en gang i kvartalet.

3.2.2.2 Restore

Som hovedregel påbegynnes restore så raskt som mulig uavhengig av valgt kritikalitet, men ved stort påtrykk av saker vil man måtte kunne prioritere. Backup og restore er komplekst for å få en raskest mulig restore er det viktig at man ved en restore situasjon inkluderer mest mulig riktig informasjon om det som skal restores.

Som ett minimum må man ha følgende informasjon for restore av filer:

- Tjenestenavn
- EKSAKT server- og filnavn (så godt det lar seg gjøre). Netbackup forholder seg til server navn og logiske diskbokstaver. Det er viktig at vi får informasjon som er så presis så mulig. Gjerne en «UNC-path»
- Når ble filen/katalogen opprettet eller endret sist
- Skal det restores og overskrives til samme lokasjon
- Hvis ikke, hvor skal det restores til:

Ved restore av hele servere og tjenester så er backup og lagring avhengig av god og riktig informasjon om hva man ønsker å oppnå. Man må i slike tilfeller snakke på tvers av fagrupper. Eksempelvis brukerstøtte, serverdrift, database og tjenesteansvarlig.

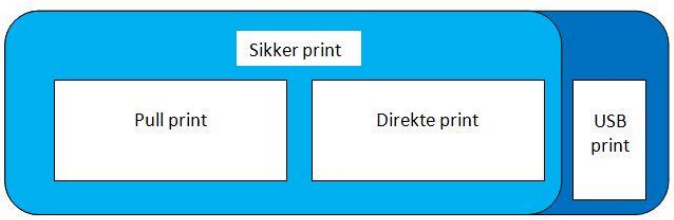
3.2.2.3 Overvåking

Backupstatus blir overvåket daglig via NetBackup OpsCenter for både regionale og lokale miljø. Her vil man kun se status på backup som allerede er etablert, altså vil en server som backupsystemet ikke allerede har et forhold til være usynlig for denne overvåkingen. Eventuelle feil blir rettet fortløpende. Hvis backup har feilet vurderes det i hvert enkelt tilfelle om backup skal kjøres på nytt på dagtid eller om man venter til neste dags backupjobb skal kjøres på natten.

3.2.3 Utskrift

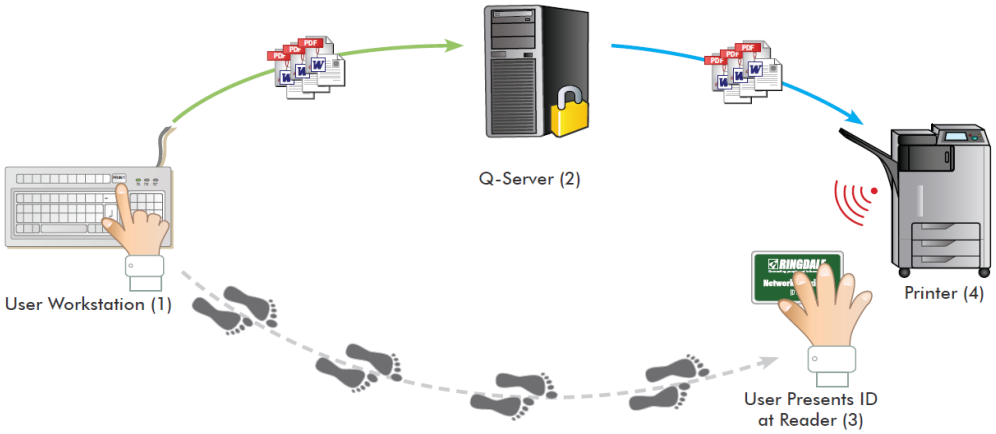
Det foresettes at alle applikasjoner kan benytte HSØs Sikker print løsning.

Sikker Print er utskriftstjenesten i Helse Sør-Øst. Sikker print har to alternative måter å skrive ut på, Pull print eller direkte print. USB-print vil fortsatt være mulig for spesielle funksjoner som f.eks. labprintere, labelprint og andre spesialskrivere. Prosjektet ser for seg at USB-print på vanlige klienter utfases og erstattes med enten Pull print eller direkte print.
Prosjektet har gått til anskaffelse av programvaren uniFLOW som leveres av Canon Norge AS.



Illustrasjon Sikker Print: Nivå 1 – Pull Print, Nivå 2 – Direkte print, USB-print.

Pull print vil være hovedalternativet for brukerne i oppsettet og den vil fungere på følgende måte:



1. Brukere skriver ut et dokument fra en PC eller annen enhet. Pull-printkøen er installert som standard på klienten, så selv om brukeren er på en ny lokasjon trenger han ikke lete fram til hvilken printer han skal bruke.
2. Utskriftsjobben sendes til en sentral utskrifts kø på pull-print serveren. Utskriften lagres her til brukeren identifiserer seg på en utskriftsenhet. Hvis brukeren ikke identifiserer seg ved en utskriftsenhet eller sletter jobben selv, vil dokumentet slettes fra serveren automatisk etter 24 timer.
3. Brukeren kan forflytte seg til en hvilken som helst utskriftsenhet med pull-print på foretaket og identifisere seg med adgangskortet eller brukernavn/passord.
4. Dokumentet vil så skrives ut på utskriftsenheten og bruker kan plukke opp dokumentet.

Pull-print køen vil blir distribuert automatisk til alle klienter hvor brukere logger seg på. Selv om denne utskriftskøen er tilgjengelig overalt så vil det være tilfeller hvor det er mer hensiktsmessig med en direkte printkø til en skriver som står i nærheten av klienten.
Direkte print er en alternativ utskriftsmåte der pull print ikke er hensiktsmessig. Direkte print fungerer på samme måte som i dag der brukeren velgere en utskriftskø direkte til en spesifikk printer i Windows. Dette utskriftsalternativet er primært ment for ekspedisjoner der printere er i umiddelbar nærhet av datamaskinen og ved behandlingsrom der det vil være upraktisk å måtte forlate pasienten for å hente en utskrift. I tillegg vil direkte print være en løsning for å sikre at klienter som er pålogget med fellesbrukere får en effektiv utskriftsløsning.
Klienter som skal ha direkte print avtales med helseforetaket når prosjektet har gjennomgang av de enkelte helseforetak før implementering av løsningen.

Ahus benytter for øvrig ikke UniFlow, men SafeCom.

3.2.4 Driftsovervåking

Det er definert følgende standard tjenester innen driftsovervåking:

	Drifte overvåking & måling

Tjenestens kritikalitet	**Basis overvåking med oppetidsmåling** • Overvåking med knytning mellom servere og tjeneste • Rutine for håndtering av alarmer • Viser oppetid for tjenesten • Målested: Datasenteret	**Full overvåking med datasentermålinger** • Overvåking med knytning mellom infrastruktur, systemer, applikasjoner og tjenester • Rutine for håndtering av alarmer • Viser oppetid og responstider for tjenesten • Simulerer brukeraktiviteter • Målested: Datasenteret	**Full overvåking med brukermålinger** • Overvåking med knytning mellom infrastruktur, systemer, applikasjoner og tjenester • Rutine for håndtering av alarmer • Viser oppetid og responstider for tjenesten • Simulerer brukeraktiviteter • Muliggjør detaljerte analyser for å identifisere forbedringstiltak • Målested: Utvalgte lokasjoner
Kritikalitet-1		X	X
Kritikalitet-2		X	
Kritikalitet-3	X		

4 Sikkerhet

Sikkerhet omfatter konfidensialitet, integritet og tilgjengelighet. Gitt at løsninger som anskaffes til bruk i helseforetakene i de fleste tilfeller vil behandle sensitiv informasjon så har Helse Sør-Øst over tid gjennomført tiltak og etablert standarder for hvordan behov for sikker tilgjengeliggjøring av informasjon dynamisk kan balanseres opp mot risiko for pasientsikkerheten.

4.1 Tilgangsstyring

Helse Sør-Øst har etablert en IAM løsning som tilbyr rolle- og attributtbasert tilgangsstyring. Tilgang til informasjon styres gjennom Helse Sør-Øst sin IAM løsning. Det betyr at en applikasjon må forholde seg til en eksternalisert identitet for både autentisering og autorisering.

Tjenester for tilgangsstyring beskrives i eget vedlegg (Bilag 3a – Identitet og tilgangsstyring)

4.2 Tilgangslogging

Helse Sør-Øst er pålagt å følge opp tilgang til pasientinformasjon. Dette gjøres ved at tilganger logges og at slike logger analyseres gjennom Helse Sør-Øst sin Logganalyseløsning. All tilgang gis basert på personlig identitet.

Splunk benyttes i Sykehuspartners som sentralt loggmottak. Det importeres data fra eksisterende loggkilder/applikasjoner og det forutsettes at nye loggkilder/applikasjoner benytter det sentrale loggmottaket. Splunk benyttes også for bearbeiding av metadata til tidsbaserte rapporter både for analyseplattform og andre applikasjoner.
Splunk kan ta imot logger på flere format, og mest vanlige er Syslog og strukturerte tekstbaserte filer.
Det er dedikerte krav til systemer som skal håndtere pasient og personsensitiv informasjon. Det vises til lov om helseregistre i den forbindelse.

4.3 Integritet

Løsningens integritet omfatter evnen til å sikre at feil ikke påvirker datagrunnlaget i løsningen. Bruker- og systemendringer på data som er kritisk for eks. pasientbehandling skal logges og kunne avleveres til Helse Sør-Øst sin Logganalyseløsning.

4.4 Tilgjengelighet

Tilgjengelighet er viktig for alle løsninger og Helse Sør-Øst benytter et system for klassifikasjon av tilgjengelighet som bygger på følgende nivåer av kritikalitet:

Kritikalitet	Sikres mot	RPO område	RTO område
1-Høyt kritisk	Utfall av datasenter, hardware feil, logiske feil, overlast	0-60 minutter	0-60 minutter
2-Kritisk	Hardware feil, overlast	1-24 timer	1-48 timer
3-Ikke kritisk	-	1-7 dager	2-7 dager

5 Integrasjon

5.1 Tjenesteorientering

Helse Sør-Øst har en tjenesteorientert integrasjonsarkitektur der ulike fagsystemer tilbyr og konsumerer tjenester på integrasjonsplattformen gjennom synkrone tjenester.
Tjenesteorienteringen skal bidra til å forbedre samhandling mellom systemer og gi en lavere terskel for nye systemer til å tilby funksjonalitet. Det er ikke ønskelig at fagsystemer har egne integrasjonsløsninger som overlapper med Helse Sør-Øst integrasjonsplattform.

Integrasjonstjenester er beskrevet i bilag 3b - integrasjon

5.2 Autoritative kilder

Helse Sør-Øst har etablert prinsipper for autoritative kilder som nye løsninger må forholde seg til. Dette betyr at leverandørens løsning må forholde seg til at sentrale dataelementer i egen løsning oppdateres utenfor løsningen og at løsningen må håndtere og **hente** slike dataelementer fra kilden samt at eventuelle oppdateringer skal gjøres via kilden.

5.3 Identitet og tilgangsstyring

Integrasjoner er gjenstand for de samme sikkerhetskrav som brukertilganger generelt. Det betyr at fagsystemers bruk av integrasjoner må autentiseres, autoriseres og loggføres samt at overføring av informasjon mellom fagsystemer og integrasjonsplattform må krypteres.

6 Grunnleggende infrastrukturtjenester og vedlikeholdbarhet

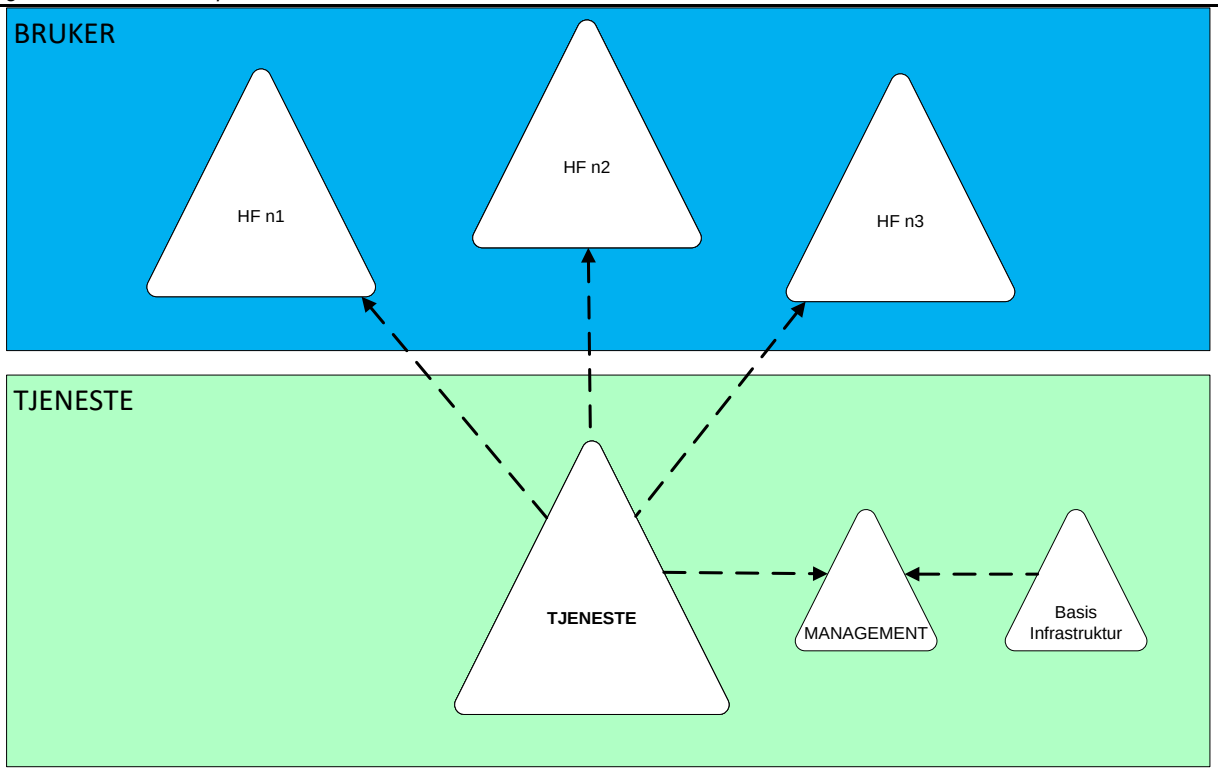
6.1 Standardisering

Sykehuspartner leverer et sett med infrastrukturtjenester. Disse tjenestene utgjør de grunnleggende byggesteinene som benyttes for å sette sammen applikasjonstjenester for helseforetakene. Tjenestene leveres fra regionale datasentre til avtalte enhetspriser per tjenestenivå.

Infrastrukturtjenester er beskrevet i bilag 3a – Standard infrastruktur.

6.2 Domenestruktur

Helse Sør-Øst har definert en domenestruktur som alle løsninger som skal etableres plasseres inn i. Grunnleggende for denne strukturen er at tjenestebærende elementer som at servere plasseres inn i et eget tjenestedomene. Dette domenet er separat fra sluttbrukerdomenene og også fra administratordomene. Klientutstyret ligger også i et separat domene. Skissen under illustrerer dette på overordnet nivå:



Figur 1 Helse Sør-Øst domenestruktur

6.3 Leverandørtilgang

En leverandør som skal levere en løsning basert på Helse Sør-Øst sine infrastrukturtjenester vil få tilgang til administrasjonsgrensesnitt for løsningen gjennom en standard Leverandørtilgangs-tjeneste. Grunnleggende for denne tjenesten er at leverandørens brukere skal ha personlig identitet og at autentisering og autorisering følger Helse Sør-Øst IAM retningslinjer. Federering av leverandørens IAM løsning med Helse Sør-Øst's IAM løsning vil foretrekkes.
Leverandørens tilganger vil logges da det kan være sensitiv informasjon i løsningen.

6.4 Virtualisering

Helse Sør-Øst har som strategi å virtualisere sine løsninger, og applikasjoner som kan virtualiseres både på server og klient vil bli preferert.

6.5 Applikasjonsdistribusjon

Helse Sør-Øst har en strategi for virtualisering av brukergrensesnittet. Helse Sør-Øst tilbyr distribusjon av applikasjoner tilpasset brukerens og applikasjonens behov samt den situasjon tilgang ønskes i. Det prefererte grensesnittet er web basert. Skal en applikasjon installeres på klientutstyr så må denne kunne pakkes og distribueres automatisk, og tykke[1] og tynne[2] klienter samt strømming av installasjonen må støttes.

[1] 'Tykk' betyr her tradisjonell applikasjonsdistribusjon i form av lokal installasjon av applikasjonen på brukerens utstyr.
[2] 'Tynn' betyr her applikasjonsdistribusjon i form av tynnklientløsninger så som RDP eller ICA.