Kundens tekniske plattform

BÆRUM KOMMUNE

Innhold

1 Endringslogg 2
2 Innledning 2
3 Arkitektur – behov og føringer 2
4 Fokusområder 3
4.1 Informasjonssikkerhet 4
4.2 Dokumentasjonsforvaltning 4
4.3 Identitetsstyring og tilgangsadministrasjon 5
4.4 Integrasjoner 6
5 Teknologistandarder hos kunden 7

1 Endringslogg

Dato	Innhold som er endret
Juni 2018	Dokument opprettet
August 2019	Dokument revidert
November 2021	Dokument revidert

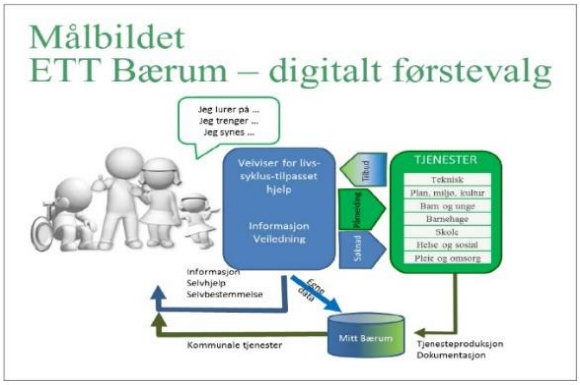
2 Innledning

Bærum kommune har fire fokusområder innen teknologiarkitektur; informasjonssikkerhet, dokumentasjonsforvaltning, identitetsstyring og integrasjon. Formålet med dette dokumentet er at leverandører og andre interessenter skal se hvor Bærum kommune har sitt fokus og bedre forstå krav knyttet til arkitektur og teknologi som settes i anskaffelsesprosjektene.

3 Arkitektur – behov og føringer

Bærum kommune har behov for en arkitektur som understøtter Difis arkitekturprinsipper[1], med spesiell vekt på tjenesteorientering, der komponenter tilbyr og konsumerer informasjon via standardiserte grensesnitt. Krav til arkitektur og teknologi har til hensikt å sørge for at ny løsning er i tråd med arkitekturprinsippene og legge til rette for effektiv integrasjon og gjenbruk av data. Data som forvaltes skal gjøres så åpne som mulig for innsyn for innbygger/næringsliv, samt for integrasjon i andre system for effektiv gjenbruk i andre delprosesser.

Figuren til høyre viser hovedmålbildet som Bærum har lagt til grunn for kommunens arkitektur. Tanken er at innbyggere og næringsliv får nødvendig innsyn i egne data, og at kommunen kan tilby tjenester på bakgrunn av tilgjengelig informasjon. Bærebjelken i målbildet er at kommunen har en enhetlig strategi for kommunikasjon med



[1] https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/nasjonal-arkitektur

innbyggerne. Det kan bety at Leverandør skal ha/har løsninger som er mulige å bygge inn i Bærums nåværende og fremtidige kommunikasjonskanal med innbyggeren.
Bærum kommune vektlegger nasjonale føringer i sine løsninger og prosjekter. Av disse vektlegges særskilt prinsippet om tjenesteorientering for å sikre en fremtidsrettet og fleksibel arkitektur, samt sikkerhet for å sikre bl.a. trygghet for ivaretakelse av personvern som spesielt sentralt.
I tillegg har Bærum kommune følgende prinsipper/føringer som skal legges til grunn ved valg av nye løsninger:

- **Brukeren i sentrum** - All virksomhetsendring fokuserer på enkelhet for brukerne med størst mulig grad av automatisering, oppgaveforenkling og intuitive grensesnitt.
- **Informasjon som sentral ressurs** - Informasjon er en ressurs som skal forvaltes og i størst mulig grad gjøres tilgjengelig for effektiv bruk på tvers av prosesser og tjenesteområder.
- **Størst mulig verdi for virksomheten som helhet** - Valg og prioriteringer må baseres på hvilke alternativ som gir størst verdi for virksomheten som helhet.
- **Helhetlig livssyklus** - Valg av teknologi og løsninger må ta utgangspunkt i totaleffektivitet og totalkostnad gjennom hele livssyklusen til teknologien og løsningen.
- **Følger standarder** - Tjenester som realiseres skal følge relevante standarder, retningslinjer; både internasjonale, nasjonale, sektorspesifikke og lokale.
- **Benytter anerkjent og velprøvd teknologi** - Virksomhetskritiske tjenester og sentral infrastruktur er basert på anerkjent og velprøvd teknologi med god tilgang på kompetanse og support.

4 Fokusområder

Bærum kommune ønsker å sette fokus på de områdene vi mener det behøves ekstra oppmerksomhet på, både fra eget hold og fra eksterne virksomheter. Vi ser blant annet at identitetsstyring og tilgangsadministrasjon er et område som mange leverandører av programvare har utfordringer med. Ved å beskrive med enkle ord behovene vi som kommune har, er målet at kravene som er satt i en anskaffelse blir tydeligere.

4.1 Informasjonssikkerhet

Informasjonssikkerhet er svært viktig for Bærum kommune. Kommunen benytter et rammeverk basert på ISO 2700X, og må i tillegg overholde kravene i Norm for informasjonssikkerhet[2] (Normen) der det behandles personsensitive data.
Informasjonssikkerhet betyr i korthet at vi må ha systemer og rutiner som ivaretar tre viktige hensyn: konfidensialitet, integritet og tilgjengelighet.

- **Konfidensialitet** betyr at informasjonen vi lagrer kun skal kunne leses av de som er autoriserte og har behov for informasjonen i sitt arbeid.
- **Integritet** betyr at informasjonen vi lagrer alltid skal være korrekt og fullstendig. Det er svært viktig at ingen andre enn de som er autorisert har mulighet til å endre eller slette data.
- **Tilgjengelighet** betyr at informasjonen alltid må være tilgjengelig for autoriserte brukere når de har behov for dataene.

Det er svært viktig at tilbudt løsning opprettholder kommunens håndtering av personopplysninger, og oppfyller kravene til GDPR.

4.2 Dokumentasjonsforvaltning

Bærum kommune stiller krav til at fagsystemene som anskaffes understøtter en helhetlig dokumentasjonsforvaltning. Kommunen har flere lovkrav som skal dekkes, deriblant arkivloven, offentleglova, forvaltningsloven og flere særlover og forskrifter.
God informasjons- og dokumentasjonsforvaltning handler om å kunne legge frem bevis på saksbehandling og annen oppgaveløsing i form av gjennomførte transaksjoner, aktiviteter og prosesser. Dokumentasjon skal **forvaltes og bevares på en måte som sikrer dens autentisitet, pålitelighet, integritet og anvendelighet.**

Det handler om rask og enkel tilgang til informasjonen som ansatte trenger for å kunne utføre sine arbeidsoppgaver på en effektiv måte, samt ivareta innsyn i kommunens virksomhet for innbyggere og offentligheten generelt.
Kommunen jobber aktivt med digitalisering på flere nivåer, og en god forvaltning av dokumentasjon er helt nødvendig for å understøtte digitaliseringstiltakene.

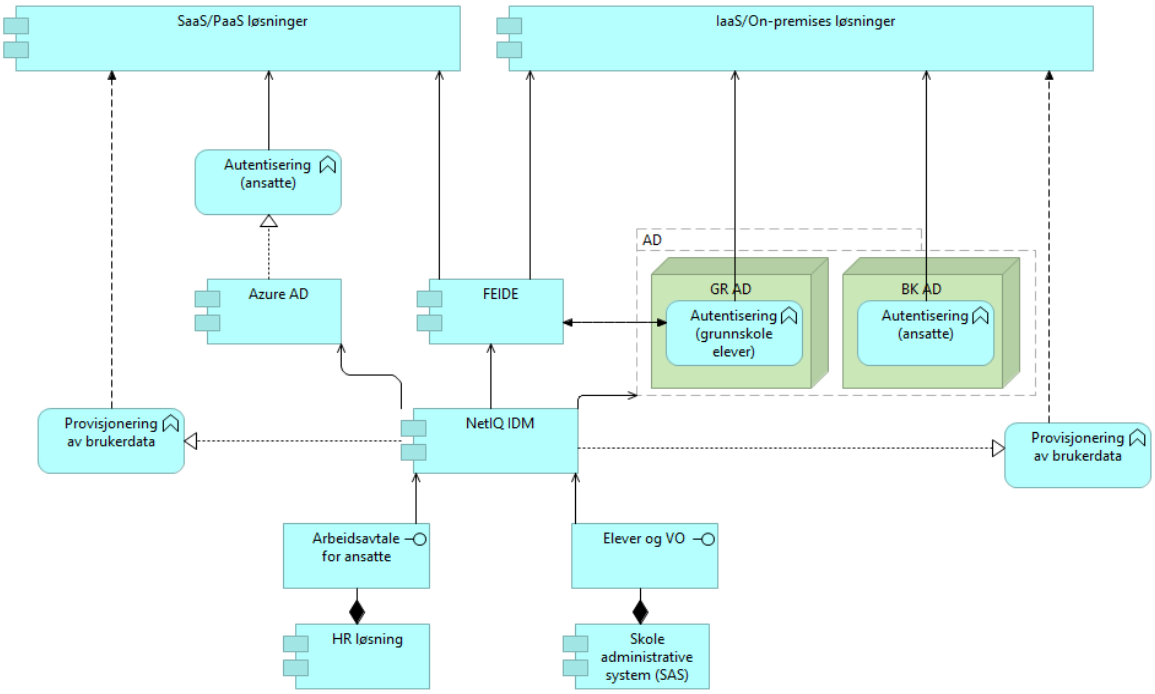
[2] https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

4.3 Identitetsstyring og tilgangsadministrasjon

Bærum kommune bruker NetIQ Identity Manager (IDM) for å styre og administrere tilganger og identiteter. Løsningen består av en selvbetjeningsplattform hvor brukerne selv kan nullstille sitt eget passord, få oversikt over tilgangene de har og be om nye tilganger. Tilgangsstyringen er basert på rolles. Dette forenkler prosessen med å oppdatere tilganger, slik at en leder ikke trenger å være usikker på hva hver ansatt kommer til å trenge, og slipper å bruke tid på å avklare de grunnleggende behovene for tilganger. Ansatte i kommunen kan ha mer enn én aktiv arbeidsavtale samtidig, på samme databruker.

- Når en **nyansatt** kommer første dag på jobb vil alle basistilganger for rollen være klare. Det eneste den nyansatte trenger å gjøre er å sette passordet sitt for så å logge inn og begynne å jobbe.
- Når en ansatt **bytter tjenesteområde** vil løsningen automatisk gi den ansatte nye tilganger og fjerne de gamle iht. de rollene vedkommende har fått.
- Når en **ansatt slutter** blir alle tilgangene i kommunens systemer automatisk fjernet

IDM er hovedkilde/nav for alle brukertilganger, og skal eie integrasjoner mot systemer som har egen intern database for brukere med tilhørende styring av interne tilganger. Disse integrasjonene skal være basert på åpne standarder (API) og skal ha støtte for sikring av autentisering og datautveksling. Alle nye systemer eller applikasjoner skal ha grensesnitt (API) for provisjonering av brukere og autorisasjon av tilganger. Dette sikrer at kommunen har kontroll på brukerkontoer og sørger for at tilganger styres etter arbeidsforhold og rydding/deaktivering skjer automatisk. Dette understøtter sporbarhet og informasjonssikkerhet.



4.4 Integrasjoner

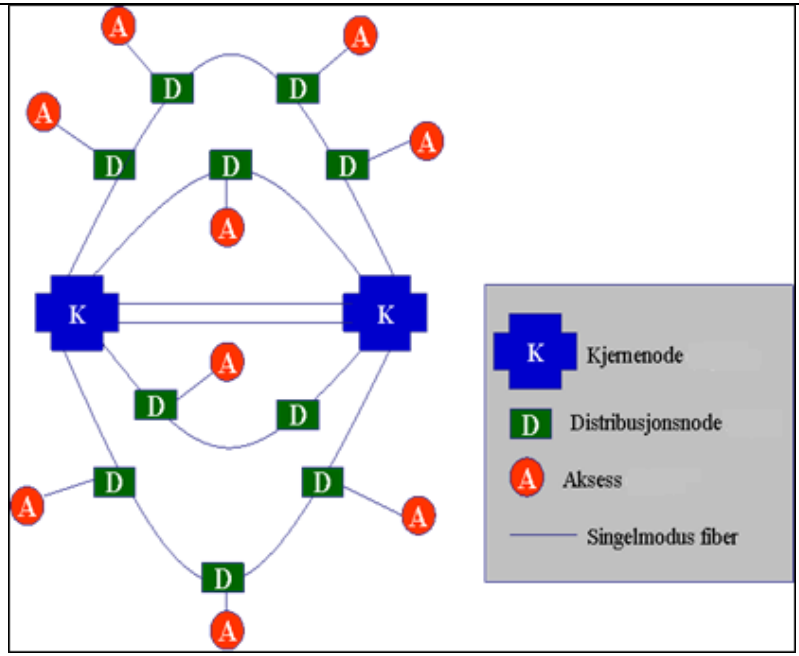
I Bærum kommune regnes all informasjon om innbyggere, saksbehandling og tjenesteproduksjon som sentrale ressurser. Det er derfor viktig for kommunen å ha kontroll over og tilgang til all slik informasjon.

For å kunne støtte målbildet «ETT Bærum – digitalt førstevalg», beskrevet ovenfor, skal alle løsninger tilby grensesnitt (API) som gir tilgang til all informasjon som er lagret i løsningen. Grensesnittet skal være basert på åpne standarder og skal ha støtte for sikkerhet som er tilstrekkelig for den informasjonen som er lagret i løsningen. Hvis det finnes nasjonale standarder, og/eller føringer, skal disse benyttes.

API skal både gi mulighet for søk og oppslag av informasjon som for eksempel er egnet for bruk til å visualisere og analysere data på tvers av våre fagsystemer, og for å kunne hente ut komplette datasett for eksempel for å kunne konvertere data over til annen løsning.

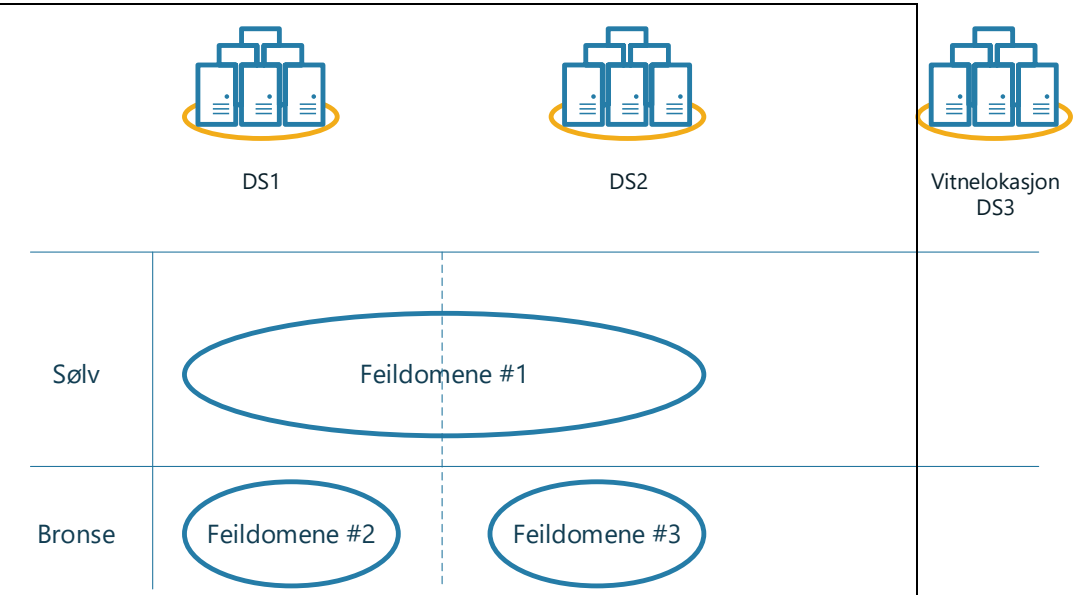
5 Teknologistandarder hos kunden

Område	Standard	Kommentar/beskrivelse
1.0 Nettverkskommunikasjon		
1.1 Hardware	Produsent: Cisco Modeller: Catalyst og Nexus-serien	
1.2 BK-MAN	Nettverket har følgende nøkkelegenskaper: • 40 Gbit/s i kjernen • 10 Gbit/s i distribusjonsnettet • 1/10 Gbits til aksesslokasjoner avhengig av behov. • Soneinndelt med dedikerte soner for PC-klienter, byggautomasjon, IP-telefoni, gjestenett, IPTV m.m. • Klargjort for prioriteringsmekanismer. • Full redundans i distribusjonsnettet • Mulighet for redundant aksess (benyttes for større kontorer)	Kunden har etablert et MPLS-basert fibernett med forbindelse til de fleste lokasjoner i kommunen. Det er mer enn 250 lokasjoner tilknyttet BK-MAN. Fibernettet benytter leid mørk fiber der Kunden eier og drifter teknisk utstyr. Kapasitet og stabilitet tilstrekkelig til at Kunden kan sentralisere alle sine dataressurser (servere, lagring, Internett etc.). Løsningen er bygget opp med tre nivåer og vises i figuren under: Nivå 1, kjernenett. Bestående av to noder plassert i hvert sitt datasenter i kommune. Nivå 2, distribusjonsnett: Distribusjonsnoder bygget opp i en ringstruktur med hovedformål å etablere redundans og redusere fiberlengdene i aksessnettet. Nivå 3, aksessnett: Aksess fra det enkelte tjenestested til den nærmeste distribusjonsnoden. For all intern ruting benyttes det private IP-adresser basert på RFC1918. All IP-kommunikasjonen mot eksterne partnere skal skje via offisielle IP-adresser.

		 **Figur 5 – Skisse over nettverksstruktur**
1.3 WIFI	Produsent: Fortinet De fleste større lokasjonene har full WIFI dekning med minimum 802.11n eller bedre.	Det finnes dedikerte WIFI nett for forskjellige formål. Autentisering av klienter må støtte minst WPA2 Enterprise. Hvis en løsningen kun støtter andre autentiseringsmekanismer må dette avklares med kommunen. Det samme gjelder dersom løsningen kun støtter 2,4 GHz båndet.
1.4 BK-WAN (VPN)	Løsningen har følgende nøkkelegenskaper: • VPN-forbindelse, kan benytte private IP-adresser • 1-20 Mbit kommunikasjonskapasitet for hver enkelt tilkoblet aksess. • Alle soner tilgjengelig i BK-MAN er tilgjengelig.	Tjenestesteder som ikke har fibertilknytning kan benytte Site to Site VPN. Dette gjelder et fåtall av tjenestestedene i kommunen. På disse lokasjonene settes det opp en ruter som tilbyr de samme sonene som er tilgjengelige i MAN. All kommunikasjon mellom tjenestestedet og Kundens sentrale nettverk kjøres i en VPN-tunnel.

		Det tillates ikke at det etableres andre Site to Site løsninger enn kommunens standardløsning.
1.5 Sikkerhetsløsninger	Sonebasert segmentering av datanett med følgende overordnede sonebegreper: • Ekstern • Intern • Sikker	Kunden har flere separate sikkerhetsbarrierer som virker uavhengig av hverandre. Sikkerhetsbarrierene skiller datanettets hovedsoner og undersoner. Mot enkelte soner benyttes to separate sikkerhetsbarrierer i kombinasjon. I tillegg er det etablert filtreringstjenester basert på innhold. Sikker sone eksisterer kun i kommunens datasentere.
1.6 Eksterne leverandører		Kunden har etablert egne kommunikasjonsforbindelser med enkelte eksterne leverandører av datatjenester. Denne kommunikasjonen er regulert av forskjellige sikkerhetsbarrierer. Ved utveksling av sensitive data, passord og lignende, benyttes krypterte forbindelser. Kunden benytter også i stor grad VPN-klienter som eksterne leverandører må installere på sine PCer for å kunne jobbe på løsninger hos Kunden. VPN-autentiseringen er primært 2-faktor (SMS i tillegg til brukerID og passord). Bærum kommune er tilkoblet «kommuneversjonen» av Norsk Helsenett for kommunikasjon med tjenester.
1.7 Datasenterkommunikasjon	BKDC kjører en NSX infrastruktur med ACI som underlay nettverk: https://nsx.techzone.vmware.com/resource/deploying-nsx-data-center-cisco-aci-underlay-design-guide-20	ACI brukes kun før å transportere VXLAN headers fra en VM i en ESX host til andre deler av infrastrukturen. All mikrosegmentering skjer i NSX, med unntak før ett par hardware appliance bokser. ACI infrastrukturen består av 2 «pods» (RHDC og RUDC) som er sammenknytte med et IPN = Inter-Pod Network. eBGP naboskap er etablert mellom Sentral distribusjon og ACI infrastrukturen (Eksterne nett fra ACIs perspektiv). BGP peeringen

		skjer i VRF connect, som er legacy serversone og hub før alle FW soner. Hastigheter er 80Gb/s mellom poddene, 40Gb/s mellom switcher i en pod, 40Gb/s til eksterne nett og 1/10Gb/s til enkelte hosts.
1.8 Internett	Leverandør: Telenor	Kunden leier internettforbindelse med maksimalt 2 x 10 Gbit kapasitet terminert i to forskjellige datasentere. Løsningen er fullredundant
1.9 Mobil datakommunikasjon	Leverandør: Phonero	
2.0 Serverløsninger		
2.1 IaaS – Infrastructure as a Service	Hyperconverged infrastruktur basert på HPE og VMware	Alle VM'er kjøres i Bærum kommunes on-premise IaaS. Den bygger på VMware stack med VMware NSX, VMware vSAN og vCloud. All lagring er på SSD. Miljøet er delt opp i 3 feil-domener over 2 fysiske lokasjoner som muliggjør en høy SLA, 99.5% på enkle VM'er og 99.95% på 1 av 2 like VM'er ved bruk av lastbalanserer eller annen teknologi for feilhåndtering. Det brukes en vitnelokasjon for å bestemme hvilket datasenter som vinner hvis det er split-brain problemer i Feildomene #1.



Gull nivå:

- Bestemmes i samråd med DigIT, avhenger av arkitekturen til applikasjonen.
- SLA på 99.95%

Sølv:

- For viktige systemer som ikke kan være nede mer enn en arbeidsdag ved større feil på ett av datasentrene.
- SLA på 99.5%

Bronse:

- For vanlig produksjonslast.
- SLA på 99.5%

		- Ved langvarige feil blir virtuelle maskiner fra ett datasenter restaurert via sikkerhetskopi til det andre.
2 PaaS – Platform as a Service	Skytjenester i Azure	Bærum kommune har flere subscriptions i Microsoft Azure som separerer DTAP miljøer.
2.3 SaaS – Software as a Service	Skytjenester levert av tredjepart	Skybaserte tjenester skal tilby API for provisjonering og autorisering av brukere. Autentisering skal støtte kommunens IDP enten via Azure eller NetIQ Access Manager.
2.2 Lokal lagring på server	Virtuelle disker i VMware	Lokalt lager på servere benyttes i hovedsak for OS og Applikasjonsinstallasjon. Applikasjoner installeres ikke på systemdisk. Data lagres ikke på systemdisk.
2.3 Backup	Commvault Vmware snapshot	Det benyttes en policybasert backupschedule. Det tas inkrementell backup av fildata daglig, samt full backup en gang i uken. I tillegg har BK filarkivfunksjonalitet. Det gjennomføres backup av logg hver time, inkrementell backup daglig, samt full backup en gang i uken av SQL-databaser . Det gjennomføres backup av arkivlogger to ganger i døgnet, inkrementell backup daglig, og full backup hver uke av Oracledatabaser. Det foretas Vmware snapshot ved arbeid på server Det foretas full backup av VMer daglig
2.5 Identitetshåndtering og katalogtjenester	NetIQ Identity Manager Microsoft AD Microsoft AzureAD	NetIQ Identity Manager (IDM) er master for identitet i Bærum kommune. Dette er navet i all utveksling av brukerinformasjon og rettigheter til katalogtjenester og andre interne løsninger i fagsystemer.

		Tjenester som kun er knyttet mot katalogtjeneste er avhengig av gruppetilganger. Tjenester som mottar data fra IDM får brukerdata og tilganger direkte i det formatet tjenesten støtter. .
2.6 Operativsystemer	Microsoft Windows Server 2019 Suse Linux Enterprise Server 15 Oracle Linux 7 Ubuntu LTS 20.04	
2.7 Filtjenester	NTFS volum på Microsoft server. SharePoint	SharePoint Online der det er hensiktsmessig.
2.8 Utskriftstjenester	Follow me Print	PaperCut
2.9 Databasetjenester	Microsoft SQL Server 2019 Oracle 12	Oracle og MySQL benyttes kun på spesifikke tjenester. Hvis ønsket brukt må det dokumenteres at Microsoft SQL ikke er støttet.
2.10 Applikasjons-tjenester	Microsoft Windows Server Microsoft IIS Linux Apache/Tomcat	
2.11 Antivirus	Trend Deep Security på serversiden Defender på klientsiden	
2.11 TerminalServer	Windows 2012 R2 Citrix XenApp 7 Office 2010	
2.12 Aksess-løsninger	Citrix NetScalerADC NetIQ Access Manager	
2.13 Overvåkning	Icinga2, CiscoPrime HP SIM EZRF Mule MMC Splunk	

	CeeView SQL Monitor m.fl.	
3.0 Mobile enheter		
Administrasjonsverktøy	VMWare Airwatch	VMWare Airwatch
Operativsystem mobiltelefon	iOS	Siste gjeldende versjon er til enhver tid standard.
Operativsystem nettbrett	iOS	Siste gjeldende versjon er til enhver tid standard.
App-distribusjon	Apple AppStore	Hvis det leveres app i tilbudt løsning skal denne være tilgjengelig gjennom Apple App store. Applikasjon skal være utviklet etter beste praksis fra AppConfig Community
Innkjøpsmetode	Volume Purchase Program	
3.1 Klientprogramvare – Windows 10		

Generelt	Alle klienter som skal benyttes i Bærum kommunes nett skal leveres, konfigurers og administreres av Bærum kommune.	Applikasjoner og andre funksjoner/løsninger som krever avvik fra noe av det nedenfor stående må avklares separat og gjennomgå egen prosess for godkjenning.
		• Avvik kan være
		  ○ Behov for egne klienter
		  ○ Behov for andre kontorstøtteprodukter

Operativsystem arbeidsstasjon	Microsoft Windows 10 Enterprise	Oppdateringsfrekvens på Windows 10 versjon er ca hver 6 måned. Standard oppsett for klientene inkluderer: • Applocker ○ RunOnce applikasjoner må være digitalt signert • Bitlocker • Microsoft Baseline Security Policy • MS LAPS (Microsoft Local Administrator Password Solution)

		○ Ingen sluttbrukere har administrator rettigheter • Standard print policy Avvik kan forekomme
Klientadministrasjon	- Microsoft System Center Configuration Manager - Active Directory	- Benyttes til installasjon av klienter, Microsoft oppdateringer og installasjon av applikasjoner - Benyttes til GPO (Group Policy Objects)
Kontorstøtteprodukter	Microsoft Office 2016 Pro Plus/Standard, Microsoft Office 365 E3/E1/F3	Avhengig av brukerlisens.
E-post klient	Microsoft Outlook 2016 Pro Plus/Standard Microsoft Outlook M365 Microsoft Outlook Online	Avhengig av brukerlisens
Nettleser	Microsoft Edge	Oppdateres ved oppstart
Antivirus	Microsoft Windows Defender	
PDF-leser	Adobe Reader	
4.0 Fagsystemer Administrasjon		
Sak- og arkivløsning	Acos WebSak Focus	NOARK 5 kjerne Tilgjengelige grensesnitt: NOARK 4 WS, Autoarkiver WS
Integrasjon	BPM Intalio BPMS ESB Mulesoft Anyplatform	
5.0 Testmiljø		
Testmiljø etableres i henhold til spesifikasjoner ved behov.		