Vedlegg 3 til

Bilag 1

Kundens tekniske plattform

og arkitekturprinsipper

Ullensaker kommune

Anskaffelse av velferdsteknologisk plattform

1. Innledning **3**

2. Arkitekturprinsipper **3**

2.1 Identitet og tilgangsstyring *3*

2.2 Nettverk og kommunikasjon *3*

2.3 Dataforvaltning og informasjonsflyt *3*

2.4 Sikkerhetsprinsipper *4*

3. Teknisk plattform **4**

3.1 Identitetsplattform *4*

3.2 Nettverk og kommunikasjon *4*

Velferdsteknologisk og medisinsk utstyr 5

Mobilkommunikasjon og APN 5

Microsoft Azure 5

Norsk Helsenett 5

3.3 Klienter og applikasjonsforvaltning *5*

Mobile enheter og apper 6

1. Innledning

Dette bilaget beskriver systemlandskapet som er relevant for leverandørens ytelse og som den samlede løsningen skal samvirke og integreres med.

2. Arkitekturprinsipper

Ullensaker kommune har et sammensatt og gradvis modernisert systemlandskap med både skybaserte tjenester, kommunespesifikke løsninger og lokal infrastruktur. Systemlandskapet omfatter IaaS/PaaS- og SaaS-baserte tjenester samt moderne og mer tradisjonelle arbeidsflater. Kommunens arkitektur utvikles gradvis i retning av mer skybaserte og fleksible tjenester, samtidig som eksisterende løsninger og behov for lokal infrastruktur ivaretas.

Arkitekturen bygger på prinsipper om sikkerhet, standardisering, gjenbruk, tydelige systemgrenser og helhetlig identitets- og tilgangsstyring. Felles tjenester benyttes på tvers av systemlandskapet der dette er hensiktsmessig.

Velferdsteknologien inngår som en del av dette landskapet sammen med kommunens identitetsplattform, arbeidsflater, nettverk, fagsystemer, integrasjoner og øvrige fellestjenester.

2.1 Identitet og tilgangsstyring

Kommunens arkitektur bygger på at **identitet er et sentralt utgangspunkt for tilgang til systemer, tjenester og informasjon**. Autentisering og tilgangsstyring håndteres i størst mulig grad gjennom kommunens sentrale identitets- og tilgangsløsninger. Dette gir en helhetlig forvaltning av identiteter og tilganger gjennom hele livsløpet, blant annet ved endring av rolle eller arbeidsforhold.

Tilgangsstyringen bygger på **tjenstlig behov, minste privilegium og en risikobasert tilnærming**. Tilgang og autentisering vurderes blant annet ut fra rolle, informasjonens beskyttelsesbehov og konteksten tilgangen skjer fra. Brukere og administratorer har som utgangspunkt bare tilgang til den funksjonaliteten og informasjonen som er nødvendig for å ivareta sine oppgaver. Administrative rettigheter begrenses både i omfang og tid.

Teknisk drift og forvaltning søkes så langt som mulig gjennomført uten unødvendig innsyn i tjeneste- og personopplysninger.

2.2 Nettverk og kommunikasjon

Kommunens nettverksarkitektur bygger på **segmentering og kontrollert kommunikasjon** mellom ulike deler av systemlandskapet. Tjenester og tekniske miljøer holdes adskilt der dette er hensiktsmessig, og kommunikasjon begrenses til nødvendige forbindelser.

Kommunikasjon mellom klienter, tjenester og systemer beskyttes mot uautorisert innsyn og manipulering. Data beskyttes tilsvarende ved lagring gjennom kryptering og andre relevante sikkerhetsmekanismer.

2.3 Dataforvaltning og informasjonsflyt

Kommunens arkitektur bygger på at **data er en viktig ressurs som forvaltes på en kontrollert og ansvarlig måte gjennom hele livsløpet**. Data og datasett har et tydelig eierskap i virksomheten, slik at ansvar for hvordan data oppstår, forvaltes, brukes og deles er kjent.

For personopplysninger legges det til grunn at opplysninger ikke oppbevares lenger enn det som er nødvendig for formålet, samtidig som krav til bevaring etter annet relevant regelverk ivaretas. Sletting, anonymisering og bevaring inngår som en del av informasjonens livsløp.

Kommunens arkitektur legger også vekt på **åpne og dokumenterte grensesnitt** som gjør det mulig å tilgjengeliggjøre og utveksle data mellom systemer på en kontrollert måte. Dette understøtter integrasjon og gjenbruk av informasjon og reduserer unødvendige tekniske bindinger mellom enkeltløsninger.

2.4 Sikkerhetsprinsipper

Kommunens sikkerhetsarkitektur bygger på at sikkerhet ivaretas gjennom hele livsløpet til systemer og tjenester, fra etablering og konfigurasjon til drift, endring og avvikling. Dokumentasjon inngår som en del av dette, slik at tekniske avhengigheter, konfigurasjon og sikkerhetstiltak kan forvaltes over tid.

Identiteter skal være **entydige og sporbare**. Personlige tilganger knyttes til den enkelte bruker, mens maskin- og tjenesteidentiteter knyttes til den aktuelle tjenesten og formålet de benyttes til.

For tjenester som er tilgjengelige fra internett, bygger sikkerhetsarkitekturen på **sterk autentisering og flere uavhengige autentiseringsfaktorer** for personlige tilganger. Maskin- og tjenesteidentiteter beskyttes gjennom egnede mekanismer for sterk autentisering. Geografiske tilgangsbegrensninger betraktes som et supplerende sikkerhetstiltak og ikke som en autentiseringsfaktor.

Kommunen legger videre vekt på **sikker konfigurasjon og reduksjon av angrepsflaten**. Funksjoner, tjenester og protokoller som ikke er nødvendige, holdes deaktivert eller begrenset. Sikkerhetskopiering og gjenoppretting inngår som en del av kommunens arbeid med robusthet og kontinuitet.

3. Teknisk plattform

Kommunens tekniske plattform består av **skybaserte og lokalt etablerte tjenester, klienter og mobile enheter, nettverk, integrasjoner og sentrale fellestjenester**.

De følgende kapitlene beskriver de delene av plattformen som er særlig relevante for velferdsteknologi, herunder identitetsplattform, nettverk og kommunikasjon, klienter og applikasjonsforvaltning samt tilkobling mot kommunale, eksterne og nasjonale tjenester.

3.1 Identitetsplattform

Kommunens HR-system er kilde til opplysninger om ansatte og arbeidsforhold. Kommunens system for identitets- og tilgangsstyring (IAM) bruker disse opplysningene som grunnlag for å opprette, oppdatere og deaktivere brukerkontoer. Når en ansatt tiltrer, bytter stilling eller slutter, danner endringen i arbeidsforholdet grunnlag for å tildele, justere eller fjerne relevante tilganger i tilknyttede tjenester.

Microsoft Entra ID er kommunens sentrale identitetsleverandør for autentisering mot skybaserte tjenester. Gjennom føderert pålogging og Single Sign-On (SSO) kan ansatte benytte sin kommunale identitet på tvers av tilknyttede tjenester og fagsystemer. Autentiseringen inngår i kommunens sentrale mekanismer for flerfaktorautentisering og betinget tilgang.

Active Directory (AD) benyttes som katalogtjeneste for deler av kommunens lokale server- og driftsmiljø.

3.2 Nettverk og kommunikasjon

Ullensaker kommunes nettverksplattform omfatter **kablede lokalnett (LAN), trådløse nettverk (Wi-Fi), WAN og mobilkommunikasjon** ved kommunens tjenestesteder. Lokasjonene er knyttet sammen gjennom et sentralt forvaltet SD-WAN, og Microsoft Azure inngår som en integrert del av nettverksplattformen.

Nettverksinfrastrukturen består av utstyr og teknologi fra blant annet **Cisco, HPE Aruba og Extreme Networks**. Nettverket er delt i separate logiske segmenter for ulike tjenester, klienttyper og teknisk utstyr.

For deler av infrastrukturen benyttes en **hub-and-spoke-arkitektur**, der lokasjoner og tekniske nett kommuniserer med sentrale tjenester fremfor direkte med hverandre. Kommunikasjon mellom nettverkssegmenter, lokasjoner, Azure og eksterne tjenester håndteres gjennom sentrale nettverks- og brannmurfunksjoner.

Velferdsteknologisk og medisinsk utstyr

Dagens helse- og velferdsteknologiske miljø omfatter blant annet lokale systemkomponenter, sensorer, posisjoneringsutstyr, mobile enheter, medisindispensere og annet medisinsk-teknisk utstyr.

Utstyret kan være tilkoblet gjennom **kablet Ethernet, Wi-Fi eller mobilnett**. Enkelte løsninger har lokale serverkomponenter ved tjenestestedet, mens andre kommuniserer med sentrale eller skybaserte tjenester gjennom kommunens WAN eller eksterne nettverk.

Enkelte eksisterende velferdsteknologiske løsninger er etablert i egne segmenterte nettverksmiljøer ved tjenestestedene. Lokale serverkomponenter og teknisk utstyr kan være kablet til kommunens nettverksinfrastruktur, mens mobile klienter kommuniserer over Wi-Fi. Annet teknisk og medisinsk utstyr kan være plassert i separate nett ved den enkelte lokasjon med forbindelse mot nødvendige sentrale eller eksterne tjenester.

Mobilkommunikasjon og APN

Kommunen benytter mobilnett for enkelte mobile arbeidsflater, tekniske enheter og velferdsteknologiske tjenester. For enkelte tjenester benyttes **privat APN (Access Point Name)** som en avgrenset kommunikasjonsvei over mobilnettet.

APN inngår som en del av kommunens eksisterende nettverksmiljø og benyttes blant annet for mobile enheter som kommuniserer med tjenester med begrenset tilgjengelighet. Mobile løsninger kan dermed benytte Wi-Fi, ordinær mobilkommunikasjon eller privat APN, avhengig av tjenestens oppbygning.

Microsoft Azure

Microsoft Azure inngår som en del av kommunens nettverks- og applikasjonsmiljø. Skybaserte applikasjonsmiljøer er nettverksmessig segmentert, og sentrale nettverksfunksjoner håndterer kommunikasjon mellom applikasjonsmiljøer, kommunens øvrige infrastruktur og eksterne tjenester.

Deler av kommunens helse- og fagsystemlandskap er etablert i eller kommuniserer gjennom dette miljøet. Andre løsninger er lokalt etablert og kommuniserer gjennom kommunens LAN og WAN.

Norsk Helsenett

Kommunen er tilknyttet **Norsk Helsenett (NHN)** for kommunikasjon med nasjonale helse- og samhandlingstjenester. Arkitekturen omfatter kommunikasjon mot NHN både fra skybaserte tjenester i Azure og fra tjenester etablert i kommunens lokale infrastruktur.

Helse- og velferdsteknologiske tjenester kan derfor bestå av en kombinasjon av lokale komponenter, kommunens LAN/WAN, Azure og tjenester tilgjengelig gjennom Norsk Helsenett. Enkelte eksisterende lokale helse- og velferdsteknologiske miljøer er etablert som separate nettverk ved tjenestestedene med forbindelse videre mot NHN.

Velferdsteknologisk knutepunkt (VKP) inngår i kommunens arkitekturbilde som en viktig samhandlingskomponent mellom velferdsteknologiske løsninger og relevante helse- og fagsystemer.

3.3 Klienter og applikasjonsforvaltning

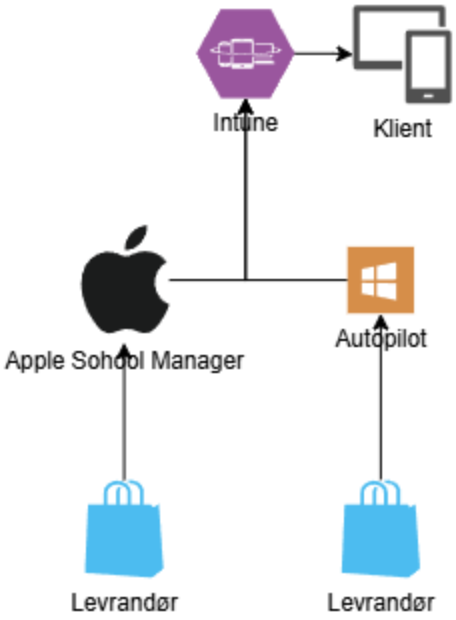
Kommunens PC-er benytter **Windows 11** og forvaltes primært gjennom **Microsoft Intune**. Programvare distribueres sentralt, blant annet gjennom Firmaportalen. Utvalgte interne fagsystemer tilgjengeliggjøres gjennom **Azure Virtual Desktop (AVD)**.

Klientmiljøet omfatter både nettleserbaserte løsninger og applikasjoner med lokale komponenter. Installasjon, oppdatering og avinstallasjon håndteres gjennom kommunens sentrale klientforvaltning.

Mobile enheter og apper

Kommunens mobile enheter og applikasjoner forvaltes gjennom **Microsoft Intune**. Mobile applikasjoner distribueres og administreres sentralt og benytter normalt de offisielle distribusjonskanalene **Apple App Store og Google Play**.

Intune benyttes til administrasjon og konfigurasjon av enheter og applikasjoner, herunder distribusjon av apper og relevante innstillinger. Kommunens mobile klientmiljø omfatter både personlige arbeidsenheter og delte enheter der flere ansatte kan benytte samme enhet med personlig pålogging.


Intune
Klient
Apple School Manager
Autopilot
Levrandør
Levrandør