

Pasientvarsling med tilhørende tjenester for Trondheim Kommune

2020 PAVA SSA-V Bilag 3

Beskrivelse av miljøet løsningen skal driftes i

1. ARKITEKTUR	2
2. UNDERBYGGENDE TJENESTER - KUNDENS ANDRE AVTALER	2
2.1. TELEFONI	2
2.1.1. MX-One	2
2.1.2. Alarmserver	2
2.2. DIGITALE ARBEIDSFLATER	2
2.2.1. Mobilt utstyr	2
2.2.2. PC/CB/Arbeidsstasjoner	3
3. RELEVANTE AVTALER OG SAMARBEIDSPARTNERE	3
4. KUNDENS AKTØRER/FUNKSJONER I AVTALEN	4
5. KUNDENS PROSESS FOR ENDRINGSHÅNDTERING	5
5.1 STANDARDENDRINGER	5
5.2 HASTEENDRINGER (EMERGENCY CHANGE)	5

1. ARKITEKTUR

Kunden har utarbeidet en overordnet arkitektur for de viktigste applikasjoner i *2020 PAVA SSA-V Bilag 3 Vedlegg 2 Referansearkitektur Trondheim*. Arkitekturprinsipper er beskrevet i *2020 PAVA SSA-V Bilag 3 Vedlegg 1 Arkitekturprinsipper for Trondheim*.

Kunden har etablert et permanent arkitekturarbeid for å vedlikeholde og realisere målbildet og beskrivelser, samt kjøre fortløpende arkitektur-prosesser i forbindelse med prosjekter og aktuelle problemstillinger. I arkitektur-arbeidet ønsker Kunden å benytte TOGAF 9-rammeverket, som Kunden håper kan bidra til å øke modenheten i virksomheten på dette området.

2. UNDERBYGGENDE TJENESTER - KUNDENS ANDRE AVTALER

2.1. TELEFONI

2.1.1. MX-One

Sentralisert Helseserver Mitel X-ONE v6.3

Mitel ASU plattform i 19" rack lokalt på hver enkelt helsehus/helse- og velferdssenter. ASU servere til Trondheim Kommune er bestykket med 2 stk. harddisker og Linux Software RAID for redundans. Alle servere har en media gateway tilknyttet via LAN/WAN

2.1.2. Alarmserver

Mitel Alarmserver benyttes for å integrere brannvarsling med telefoniløsningen på Elpas-anlegg.

2.2. DIGITALE ARBEIDSFLATER

Alle digitale arbeidsflater som benyttes hos Kunden, anskaffes i avtalen Digitale arbeidsflater. Produkter som tilbys/tilgjengeliggjøres for anskaffelse er vurdert i et produktråd med Kunden, hvor utvikling i markedet, behov, kvalitet, brukbarhet og tilgang til utstyr vurderes.

2.2.1. Mobilt utstyr

Alt eid mobilt utstyr er lagt under administrasjon og sikret gjennom to forskjellige Mobile Device Management-løsninger etter hvilke tjenester, og bruksområde for utstyret:

1. Google Mobile Management; SaaS-tjeneste, levert fra Google sitt datasenter.
2. WSONE; SaaS-tjeneste, levert fra VMware sitt datasenter.

MDM-løsningene sikrer at mobilt utstyr underlegges Trondheim kommunes krav til sikring av mobilt utstyr, herunder krav til kryptering, skjermlåsing, mulighet for fjernsletting mv.

2.2.2. PC/CB/Arbeidsstasjoner

Alle windowsbaserte maskiner administreres i Microsoft SCCM.

Windowsbaserte maskiner underlegges herdingsstandarder for informasjonssikkerhet som sikrer at konfigurasjon ivaretar krav til informasjonssikkerhet, og benytter endepunktssikkerhetsverktøy som sikrer at lagringsmedier er kryptert, beskyttet mot ondsinnet kode, og med lokal brannmur og styring av tillatte applikasjoner som kan kjøre (applikasjonshvitlisting).

Utstyr med Chrome OS administreres i Google løsning for enhetsadministrasjon.

3. RELEVANTE AVTALER OG SAMARBEIDSPARTNERE

Leverandør må aktivt samarbeide med dagens- og fremtidige leverandører og samarbeidspartnere innenfor relevante tjenesteområder:

- ATEA
 - Digitale arbeidsflater, eksempelvis PC, Chromebooks, nettbrett, mobil
 - Telefoni
 - AV

- Evry
 - Sikker infrastruktur kommunikasjon Trondheim kommune (SIKT)- nettverk
 - Mobil og fasttelefoniabonnement og løsninger

- Trondheim eiendom
 - Utbygging
 - Bygningstekniske feil
 - Bygningstekniske endringer
 - Testing

4. KUNDENS AKTØRER/FUNKSJONER I AVTALEN

Kundens aktører/funksjoner som har tilknytning til feilhåndtering:

Helsepersonell på lokasjonene: Helsepersonell er sammen med beboerne brukerne av PAVA. Helsepersonell driver i all hovedsak med pasientbehandling og har relativt liten kapasitet til å drive feilretting. Det må forutsettes at kunnskapen om de tekniske sidene av PAVA er begrenset.

Merkantilt personale på lokasjonene: Merkantilt personale på lokasjonene er tilstede på dagtid og kan ivareta administrative oppgaver med PAVA, eksempelvis konfigurasjon og batteribytter, samt foreta nødvendige bestillinger.

Driftsoperatører på lokasjonene og på døgnvakt: På dagtid er det driftsoperatører på lokasjonene som driver vedlikehold av bygningsmassen og tildels noen tekniske anlegg. Utenfor normal arbeidstid er det en driftsoperatør på vakt i hele kommunen som kan rykke ut ved behov. Det kan ikke forutsettes at driftsoperatør har formell teknisk kompetanse.

IT-brukerhjelp: IT-brukerhjelp har som oppgave å motta brukerhenvendelser fra ansatte i kommunen og rute disse videre til riktig instans. De mottar ikke systemgenererte feilmeldinger/varsel. IT-brukerhjelp kan kategorisere feil og fungere som førstelinje feilretting. Graden av feilretting vil avhenge av hvilken informasjon Leverandørene kan utstyre IT-brukerhjelp med.

Incident Manager: Rolle i IT-tjenesten med ansvar for å håndtere større/mer komplekse hendelser (incidents). Koordinerer aktivitetene på tvers av Kunde/Leverandør/kontrakter og er bindeleddet opp mot kommunens ledelse.

Leverandør av server- og applikasjonsdrift: Kommunen har outsourcet server- og applikasjonsdrift til en ekstern leverandør. Der det er formålstjenlig kan applikasjoner installeres og driftes i dette servermiljøet. Denne leverandøren overvåker og drifter normalt server, operativsystem (OS) og applikasjonene som er installert.

ESIKT: ESIKT innehar rollen som tjenesteforvalter for PAVA og vil kunne fungere som et bindeledd mellom brukerne og PAVA-leverandøren. ESIKT kan også ivareta administrative oppgaver i PAVA om dette er formålstjenlig, herunder oppgaver som konfigurasjon, brukerautorisering, analyse av logg, opplæring og andrelinje feilretting.

5. KUNDENS PROSESS FOR ENDRINGSHÅNDTERING

Kunden har etablert en prosess for håndtering av endringer. Leverandøren har ansvar for melde endringer relatert til avtalen til Kundens endringsråd. Prosessen har til hensikt å kontrollere endringers livssyklus slik at endringen gjennomføres uten at IKT-tjenesten avbrytes. Prosessen omfatter alle endringer initiert av Kunden eller av Leverandøren, herunder også endringer på prosesser og organisasjonsendringer.

5.1 STANDARDENDRINGER

Det er Leverandøren sitt ansvar å definere standardendringer (endringer som medfører lav risiko og følger dokumentert rutine) i samhandling med Kunden, slik at prosessen blir så effektiv som mulig og bidra til at flest mulige endringer defineres som standardendringer.

Leverandøren skal registrere endringer som ikke er standardendringer i Kundens Service Management verktøy (Service Now).

5.2 HASTEENDRINGER (EMERGENCY CHANGE)

Hasteendringer skal benyttes i de tilfeller der det er strengt nødvendig for å unngå eller løse en kritisk feil, eller fjerne et potensielt sikkerhetsproblem.

Hasteendringer (Emergency Changes) skal varsles som ordinært planlagt arbeid, men uten varslingsfristen.

Hasteendringer skal så langt som mulig utføres i angitte tidspunkter for vedlikeholdsvindu og fortrinnsvis på gunstigste tidspunkt for Kunden.

Hasteendringer skal utføres så fort som mulig for å løse en Major Incident eller implementere en sikkerhetspatch. Hasteendringer skal varsles brukerne øyeblikkelig via Kundens Service Desk.