KRAVSPESIFIKASJON

Larvik
kommune

Standarder og krav til IT-systemer

1 Generelt

1.1 Innledning

Dette dokumentet er utarbeidet for bruk ved:

- anskaffelse av IT-systemer.
- vesentlige endringer av eksisterende IT-systemer.
- nybygg, bygningsmessige utvidelser eller større restaureringsarbeider som berører IKT-områder.

1.2 Anbud/leveranse

Når leverandører skal legge inn anbud etter forespørsel fra Larvik kommune, skal alle forhold stemme med krav og spesifikasjoner i dette dokumentet - avvik må avklares med IT-avdelingen / Digitalisering. Dersom leverandøren mangler informasjon kan dette fås på forespørsel til IT-avdelingen / Digitalisering.

2 Systemtekniske krav

2.1 Plattform servere

Det stilles følgende systemtekniske krav:

- Windows-basert applikasjon
- 64 bit for serverapplikasjoner.
- Alle applikasjoner skal være kjørbare på Microsoft terminalserver 2016 (Citrix PVS (provisjonerte servere)).
- Serverne er basert på Win 2016 eller nyere. Alle løsninger skal støtte dette.
- Programmer og databaser som tilbys kommunen skal kunne kjøres på Virtuelle servermiljøer – VMware v. 7.
- Flerbrukersystem – i praksis ingen begrensning på antall samtidige brukere.
- Ved bruk av containerteknologi, må det kunne kjøres på kubernetes (Tanzu Basic i VMware).

2.2 Plattform klient

Windows-basert applikasjon må kunne kjøres på følgende plattform:

- Windows 10 Professional 64-bit og nyere.

iOS/iPadOS-basert applikasjon må kunne kjøres på følgende plattform:

- Til enhver tid nyeste iOS/iPadOS-versjon.
- Apper må kunne tildeles via kommunens MDM (jf. “7 MDM-miljø), og handles/hentes fra Apple School/Business Manager (tidl. VPP).

Chromebook-basert applikasjon må kunne kjøres på følgende plattform:

- Til enhver tid nyeste ChromeOS-versjon.
- Apper må kunne hentes fra Marketplace, ev. leveres i form av Android-app som er støttet av Chromebook. Android-app må kunne hentes fra Play Store.

2.3 Databasestandarder

- Microsoft SQL 2016 – eller høyere.

Eventuelt unntak fra denne standarden må godkjennes av IT.

IT-avdelingen godtar leveranser på Linux-VMer/-appliance, men vet at løsninger leveres på svært ulike måter. IT ønsker derfor å bli enige med leverandør om OS, databasetype mm.

2.4 Standard Web-server system

System	**Applikasjon**
Operativsystem	Windows 2019 server
Web-server system	MS Internet information server

Eventuelt unntak fra denne standarden må godkjennes av IT.

IT-avdelingen godtar leveranser på Linux-VMer/-appliance, men vet at løsninger leveres på svært ulike måter. IT ønsker derfor å bli enige med leverandør om OS, databasetype mm.

2.5 Publisering av applikasjoner

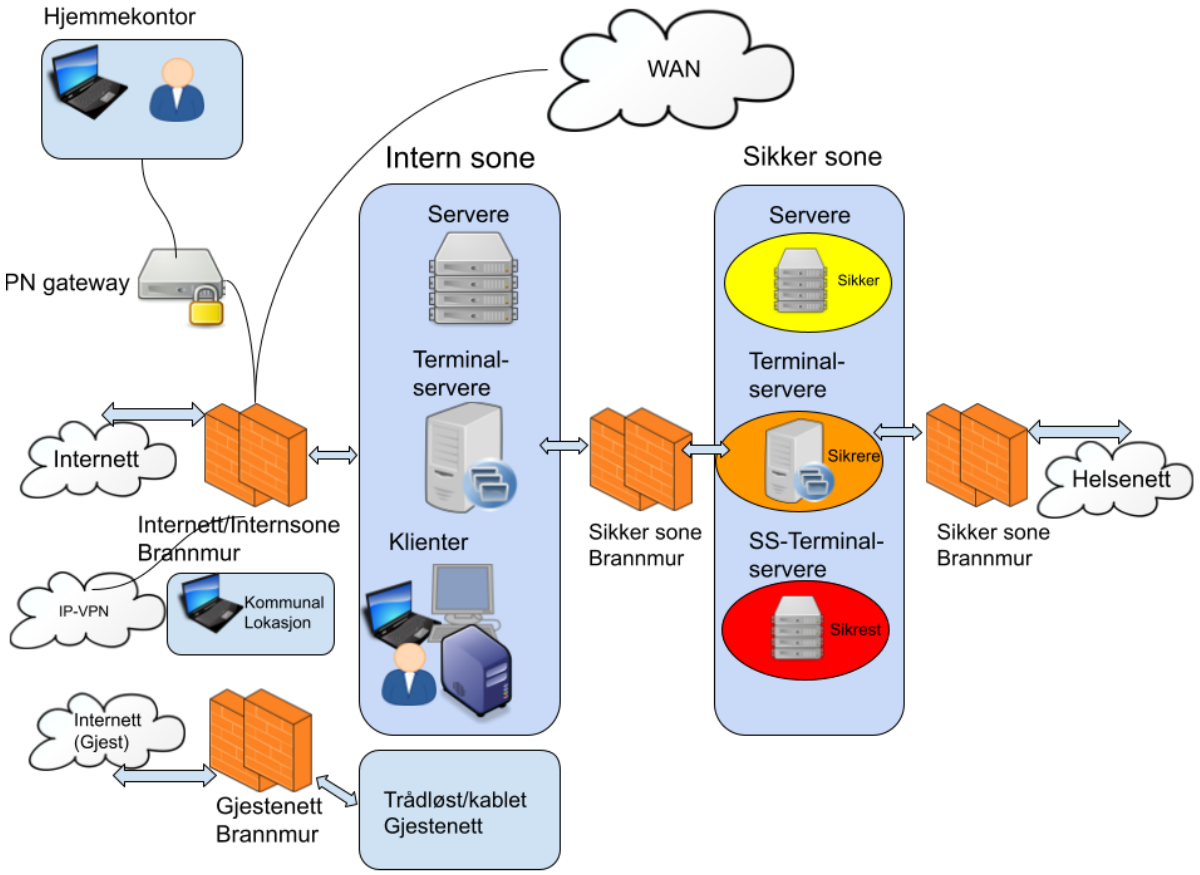
Applikasjonene må støtte installasjon på Citrix terminalservere. I sikker sone støttes kun applikasjoner som kan kjøre i et Citrix terminalservermiljø (PVS). Alle applikasjoner bør komme i MSI-format.

2.6 Nettverk

2.6.1 Brannmur

Løsningen består av ytre og indre brannmur. Det er etablert inline-filtre for all internett trafikk. Datatilsynets krav og regler blir overholdt. Det forutsettes at leverandører av programvare holder seg innenfor de samme rammer. Dette gjelder all form for kommunikasjon. Leverandør må levere dokumentasjon på trafikkflyt, slik at dette kan implementeres i brannmur.

Overordnet design / grovskisse:



2.6.2 Kablet nettverk

Larvik kommune eier og drifter egen fiber mellom sine lokasjoner. Fiber termineres inn i våre sentrale datarom. Et fåtall lokasjoner har ikke fiber, disse kobles mot kommunens nettverk over IP-VPN. Larvik kommune har redundante internettlinjer og har i utstrakt grad redundans i egne fiberlinjer ved bruk av ringstrukturer.

2.6.2.1 Kabling i bygg

https://kvalitet.larvik.kommune.no/felleslarvikkommune/Publishing/Document/LoadLocalContent/6946?forOL1=felleslarvikkommune

2.6.3 Trådløst nettverk

Larvik kommune har et kontroller basert WiFi-system, hvor all trafikk tunneleres til sentralt datarom. I hovedsak består trådløst nett av to SSID'er:

LK - Kryptert nett med autentisering via 802.1X. Dette nettet krever enheter registrert som objekter i Active Directory.

LK_Gjest - Åpent nett med autentisering via portal (captiveportal). Klientens mac adresse kan registreres slik at enheten kan kobles direkte mot LK_Gjest uten interaksjon mot portal. Nettet har klient isolasjon og gir kun tilgang til internett.

2.6.5 VPN-løsninger

Ansatte i Larvik kommune som disponerer bærbare Windows-klienter benytter GlobalProtect-VPN for fjerntilgang til kommunens nettverk. Øvrige aksesserer kommunens interne tjenester via Citrix når de befinner seg utenfor kommunens nettverk.

2.7 E-post

Larvik kommune benytter Google GMail som e-postløsning. DMARC, DKIM, SPF mm. er satt opp. Systemer kan sende e-post med @larvik.kommune.no-adresse via f.eks. SMTP og Googles APIer. Tjenester som ikke er installert on-prem hos Larvik kommune ønskes primært å sende fra andre adresser enn @larvik.kommune.no - annet må avklares med IT. All konfigurering av e-postutsending må settes opp i samarbeid med IT-avdelingen.

2.8 Utskrift og skanning

Larvik kommune benytter Uniflow som sentral utskrifts-/skanningsystem. Printere/scannere leveres fra Canon, og er satt opp med PIN-autentisering mot Uniflow. Alt kjøp av printere/scannere må godkjennes av IT-avdelingen.

3 Krav til programmer/applikasjoner

3.1 Installasjon

All programvare som skal installeres bør leveres på MSI. Programinstallasjon skal kunne automatiseres og installeres "silent".

All programvare skal leveres med installasjonsveiledning og dokumentasjon på teknisk oppsett.

3.2 Oppdatering - ”Nye versjoner”

Enhver ny versjon av et program skal være grundig testet før det settes i produksjon i vårt miljø.

Når programvaren oppgraderes for kommende versjoner skal den nye oppgraderingen bestå av en fullverdig installasjon. Dette innebærer at den nye oppgraderingen skal kunne installeres uten å ha den gamle tilgjengelig, enten installert eller på annet lagringsmedium.

All programvare skal leveres med installasjonsveiledning og dokumentasjon på teknisk oppsett.

3.3 Standardapplikasjoner

Larvik kommune benytter Google Workspace som kontorpakkesystem, men har også lokalt installert MS Office 2016 STD.

Ved tilbud av systemer som krever integrasjon mot øvrige standardapplikasjoner skal nedenforstående liste legges til grunn:

Type	**Produkt**
Kontorstøtte	Generelt: Google Workspace. For systemer i f.eks. Sikker sone: MS Office 2016 STD.
Nettleser	Chromium-baserte nettlesere.
Dokumentvisning	Adobe Acrobat Reader (nyeste versjon).

3.4 Programvarelås

Det tillates ikke leveranser av programvare med noen form for fysisk programvarelås, dongler, USB-brikke etc.

3.5 Fjerndrift/-leveranse

Alle dataprogrammer hvor sensitive opplysninger behandles, skal som hovedregel kjøres på servere lokalisert i kommunens datarom. Alle programmer skal installeres og oppdateres av leverandør i samarbeid med IT-personell i Larvik kommune.

Unntak kan gjøres der det ikke finnes alternativer for lokal drift, eller der det er hensiktsmessig for Larvik kommune å ikke ha systemet on-prem. Dette stiller imidlertid strenge krav til behandling av data og eventuelt personopplysninger (GDPR etc). Slike tjenester må leveres over Norsk Helsenett eller tilsvarende sikker løsning. Design må avklares med IT-avdelingen i Larvik kommune.

Programmer med sensitive opplysninger bør “by-design” ha mekanismer som hindrer utilsiktet lekkasje av data, eksempelvis copy/paste, nedlasting av datasett til lokal maskin mm.

3.6 Arkivering og deponering

Fagsystemer som avleverer til arkiv, skal primært integreres med Larvik kommunes eksisterende arkivkjerner. Journalføring og arkivering skal fortrinnsvis være løpende og automatisk.

Fagsystemet skal ha funksjonalitet som oppfyller de grunnleggende kravene i arkivregelverket. I dette ligger funksjonalitet til dokumentfangst, metadata og logger, sikkerhet og tilgangsstyring, tilgjengelighet og anvendbarhet og kassasjon.

3.7 Integrasjoner

Larvik kommune ønsker at data skal flyte sikkert og sømløst mellom ulike applikasjoner. Systemer/applikasjoner som leveres til Larvik kommune skal kunne avlevere/motta data på slik det er beskrevet i dette dokumentet.

3.7.1 SFTP & IP-filtrering

SFTP med IP-filtrering er krav ved filoverføringer (der API-integrasjoner e.l. ikke er mulig). Dokumentasjon av hvor filer lagres og hvor lenge må fremkomme, og intervall for filuthenting/avlevering må avtales.

3.7.2 APIer

Ved innkjøp av nye applikasjoner er det viktig å sikre tilgang til egne data. Tradisjonelt har vi kunnet koble oss direkte til databaser når systemene driftes hos oss. Når man går på skyleveranser og/eller sikrede systemer forsvinner ofte denne muligheten.

Det er et krav at vi har tilgang til egne data, slik at vi kan benytte den til de formål vi måtte ønske. Dette gjøres i dag ved bruk av Application Programming Interface (API).

Tilgang til egne data bør være en del av leveransen og inkludert i prisen. Trafikkbaserte kostnader for bruk aksepteres når det anses nødvendig. Pris og vilkår skal da være rimelige, transparente og ikke-diskriminerende. Tilgang til test/utvikling bør gis uten ekstra kostnad.

Dokumentasjon bør tilbys iht “OpenAPI Specification” eller tilsvarende åpne og maskinlesbare formater. Dokumentasjonen skal være så komplett at en erfaren utvikler kan bruke API’et uten mer informasjon og skal inneholde:

- Hvordan man bruker API-et, inkludert eksempelkode.
- Hvilke og hvordan feilsituasjoner håndteres
- Hvilke bruksområder API-et har.
- Hvilken funksjonalitet/ressurser som det tilbyr.
- Krav til identiteten til brukere og beskrivelse av tilgangsstyring. Må inneholde beskrivelse av sikkerhetsmekanismene som beskytter API-et.
- Beskrivelser av test muligheter og bruk av testfasiliteter inkludert kontaktinformasjon.
- Beskrivelse av tilgjengelighet for API-et, og hvordan planlagt vedlikehold gjennomføres
- Beskrivelse av begrensninger og andre driftsmessige egenskaper
- Lisensiering og eventuelle kostnader knyttet til bruk av API-et i produksjon.
- Bruksvilkår på data mottatt fra API-et. Må inkludere krav og vilkår for sikkerhet, lagring, behandling, videreformidling og sletting.
- Forventet levetid for API-et og hvordan versjonering av API-et håndteres.

Andre løsninger må avtales med IT/Digitalisering.

3.7.2.1 Sikkerhet API

API’et bør sikres med token-basert autentisering basert på OAuth 2.0.

Applikasjoner som ikke trygt kan lagre klientid/passord eller har andre svakheter bør sikres med Proof Key for Code Exchange (PKCE), definert i OAuth 2.0 RFC 7636.

Dette gjelder feks følgende typer:

Native Apps
Typisk de som er laget for et spesifikt økosystem (Android, iOS). Disse kan ikke lagre en klientId/passord trygt da de kan dekompileres. De kan også benytte andre URL-skjema som fanger redirigeringer (feks minapplikasjon://) som gjør at token kan komme på avveie.

SPA (single page apps)
Kan ikke lagre klientId/passord trygt da all kildekoden ligger i nettleseren

3.7.3 ERP

Larvik kommune benytter Unit 4 ERP (Agresso) installert on-prem. Modulene som benyttes er blant annet Økonomi, Lønn, HR, Innkjøp, Regnskap, Fakturering og Parkering.

Vi drifter også løsningen for foretaket Kulturhuset Bølgen og Larvik kirkelige fellesråd.

Avlevering fra Agresso til eksterne fagsystem skal som hovedregel gå over SOAP.

Innhenting av data til Agresso gjøre pr. nå primært med fil på standard Agresso filformat som hentes av oss fra leverandørens SFTP-tjeneste.

Prinsippet er færrest mulig inngående åpninger til kommunen, utgående og inngående trafikk settes i gang (initieres) fra oss og til leverandør.

3.8 Universell utforming

Nettsider og applikasjoner som omfattes av regelverk for universell utforming skal følge de minimumskrav som er definert i lovverket. Mer informasjon om gjeldende regelverk er beskrevet på https://www.uutilsynet.no/. Eventuelle krav utover de minimumskrav som er definert i lovverket vil fremgå av konkurransedokumentene.

4 Leverandørtilgang

Leverandørtilgang skal reguleres i kontrakts form, også inkludert taushetserklæring. Denne opprettes mellom leverandør og systemeier ved fagenheten. For fjerntilgang kontakter leverandøren IT for tidsbegrenset tilgang.

5 Brukeradministrasjon og autentisering

5.1 Brukeradministrasjon

Det stilles krav til administrasjon av brukere. Brukere må kunne opprettes og avsluttes automatisert ved integrasjon mot lokalt AD, Azure AD, Google Workspace eller kommunens BAS (Life Cycle Server), slik at man ikke må definere brukere manuelt inne i applikasjonen. Et sikkerhetsgruppemedlemskap bør ligge til grunn - ledere i Larvik kommune kan melde inn/ut medlemmer via kommunens ID-portal.

Systemet må ha mulighet for mer detaljert/granulert rettighetsstyring internt i systemet.

5.2 Autentisering

Larvik kommune ønsker at all autentisering integreres mot sine egne løsninger, alternativt mot nasjonal felles innloggingsløsning for offentlige tjenester.

- Protokoller: SAML2.x eller OAUTH / OpenIDConnect.
    - Larvik kommunes endepunkter for disse autentiseringsmåtene er on-prem ADFS, Azure eller Google WS.
    - Disse løsningene gir SSO for Larvik kommunes brukere når de arbeider i kommunens nettverk, og avkrever kommunens to-faktor-løsning (Citrix ADC) ved pålogging over eksterne nett (eks. Internett).
- Active Directory-integrasjon kan benyttes ved on-prem-løsninger (eks. sikker sone-applikasjoner).
- ID-porten.
- Feide for skolesystemer.

Sikring av native apps og SPA-nettsider bør gjøres med Proof Key for Code Exchange (PKCE), definert i OAuth 2.0 RFC 7636.

All autentisering over eksterne nett (eks. Internett), som ikke benytter en av de ovennevnte autentiseringsmetoder, må være sikret med to-faktor/MFA. Alternative sikringsmekanismer kan være IP-godkjenning, device-godkjenning mm. Avvik fra dette må gjøres i dialog med IT.

6 Krav til systemadministrasjon

Systemer skal kunne benyttes av flere virksomheter. Hver virksomhet har egne driftsmidler og ressurser og må derfor ha definert egen avdeling/brukerområde i systemet. Brukere skal defineres og ha ulike tilgangsrettigheter. Kontroll av brukeridentitet må skje ved pålogging.

7 MDM-miljø

Larvik kommune bruker ulike måter for utrulling/vedlikehold av sine klienter;

- Lightspeed: iOS-enheter i skole og administrasjon
- AirWatch: iOS og Android-enheter i helse
- Google Workspace: Chromebooks
- Interne/egenutviklede løsninger for Windows-klienter

8 Kontaktinformasjon

8.1 IT-avdelingen

Magnus Dahl Mortensen
+47 95818507
magnus.dahl.mortensen@larvik.kommune.no

8.2 Digitalisering

Vilhelm Einen
+47 98231283
vilhelm.einen@larvik.kommune.no