RINGERIKE KOMMUNE

# Operative føringer for IKT

# Strategi for Informasjon-, kommunikasjon- og telefonsystemer i Ringerike kommune.

**Dato 15. januar 2019**

**Utarbeidet av:**
**IT-enheten**

# Innholdsfortegnelse

## Dokumenthistorikk

| Dato | Versjon | Laget av | Godkjent av | Beskrivelse av endring |
|---|---|---|---|---|
| 07.01.15 | 1.0 | TD | | Gjennomgått i IT-enheten. |
| 06.09.18 | 1.1 | TD | | Oppdatert |
| 19.09.18 | 1.11 | TD | | Merkesystem for spredenett |
| 08.10.18 | 1.12 | TD | | Informasjonssikkerhet og databehandleravtale |
| 30.11.18 | 1.13 | KN | | Kabling og adgangskontroll |
| 15.01.19 | 1.14 | TD | | Soner og klienter |
| | | | | |

# 1. Dokumentets mål og hensikt

Ringerike kommune utarbeidet høsten 2017 en digitaliseringsstrategi, denne setter innbyggeren i sentrum for kommunens digitale satsning.

«**Vi skal fornye og forenkle Ringerike inn i en ny tid**».

Ringerike kommune er inne i en spennende tid for digitalisering, som krever en stabil og robust IKT-plattform for etablering av de nye digitale løsningene. Kommunen bygger derfor en enhetlig virksomhetsarkitektur som legger til rette for gode og innovative innbyggertjenester og effektiv forvaltning. Samtidig vil kommunen velge teknologier og driftsmodeller som utnytter kommunens ressurser optimalt, som gir god økonomi og gir stabilitet og sikkerhet.

Dette dokumentet gir operative føringer for anskaffelse av nye installasjoner, systemer og løsninger slik at det etableres i en helhetlig virksomhetsarkitektur. I tillegg gir dokumentet et innblikk i det strategiske arkitekturmålbildet for IKT som Ringerike kommune ser for seg de kommende årene.

# 2. Innledning

Ringerike kommune strategi for IKT skal understøtte digitaliseringsstrategien og etablering av drift for fagsystemer og andre støttesystemer. Et hovedmål for IKT-plattformen er å kunne understøtte både tradisjonelle installerte løsninger og skyløsninger (SaaS) på en god måte.

## 2.1. *Tall og omfang*

Kommunens tjenesteproduksjon er avhengig av en rekke fagsystemer og andre IKT-løsninger.

IKT i kommunen består av et stort antall brukere og omfatter alt fra helse, omsorg, undervisning, administrasjon, samfunnstjenester til publikumstjenester og tilstedeværelse på sosiale medier. Ansatte har varierende behov, avhengig av organisasjonstilhørighet, rolle og kompetanse. Noen ansatte har faste kontorplasser, mens andre har høy mobilitet. Enketle må være tilgjengelige hele tiden, mens andre kan styre tiden sin mer selv. Mange ansatte er avhengig av IT-utstyr for å få jobben gjort, mens andre kan utføre den uten tilgang til egen PC. Noen arbeider både innen- og utendørs.

Nøkkeltall:

- I administrativt nett er det 3200 brukerkontoer for ansatte, og i skolenett 3500 brukerkontoer for elevbrukere, 3800 arbeidsstasjoner (PC/Tynnklienter), 150 skrivere
- 71 lokasjoner med 350 switcher og brannmurer, som er koblet sammen med fiber, radio og leide linjer.

## 2.2. *Organisering og driftsmodell*

I Ringerike kommune driftes IKT-plattformen av egne ansatte. IT-enheten har bred kompetanse innen de fagområdene som trengs, samt moderne og effektiv IKT-drift som er smidig og tilpasset kommunale tjenester.

Kort avstand fra bruker til support / driftsapparat er et viktig element for å oppnå høy kvalitet og effektivitet i håndtering av både driftsoppgaver og utviklingsoppgaver. Dette gi god forutsigbar drift og god oppetid på IKT-plattformen.

# 3. Arkitektur og digitaltøkosystem

Krav til fysisk arkitektur som må følges som er nærmere spesifisert utover i dette dokumentet. Men målbilde, prinsipper og sikkerhet rundt arkitekter må legges som en føring i alt arbeid rundt teknologi, herunder utskiftning, anskaffelser, installasjoner, oppgraderinger mm.

## 3.1. *Arkitektur målbilde*

For at Ringerike kommune skal sette innbygger og digitale løsninger i sentrum, må det bygges videre på en arkitektur som gir mulighet til å levere gode og proaktive innbyggertjenester gjennom de digitale flater som innbyggerne benytter.

Kommunen benytter en rekke fagsystemer med hver sine datasett. Noen av disse inneholder løsninger for innbyggerdialog, mens andre kan være interne fagapplikasjoner eller saksbehandlingsløsninger.

Ringerike kommune har ambisjoner om å møte innbyggerne på en enhetlig og konsistent måte. En del av dette handler om å tilby innbyggeren et personalisert grensesnitt hvor data og prosesser er tilgjengelig på digitale flater. Dette kan eksempelvis omfatte informasjon om bolig, barn, barnehage, skole, søknader og ulike prosesser innenfor helse og omsorgssektoren.

Kommunen har også ambisjoner om å bygge innsikt gjennom analyse av de data som produseres og håndteres i de ulike fagapplikasjonene. Dette vil kunne gi kommunen innsikt i utviklingstrekk og trender som ellers ikke ville være lette å oppdage.

For å kunne nå disse målene, vil Ringerike kommune legge vekt på at de løsninger som anskaffes tilbyr åpne og strukturerte grensesnitt for tilgang til data. I noen tilfeller vil det også være ønskelig med åpne grensesnitt for oppdatering av data.

Med åpne og strukturerte grensesnitt menes det som omtales som «åpne APIer». Ringerike kommune foretrekker at disse leveres enten som WebServices over SOAP protokoll eller som REST API'er over standard http protokoll. Som innholds format kreves det enten XML eller JSON.

Videre må API'er leveres med autentisering basert på moderne standarder som "OpenID Connect" eller OAuth 2.0. For å håndtere sikkerhet må all kommunikasjon kunne gå over HTTPS for ende til ende kryptering.

Med bakgrunn i et ønske om høy datakvalitet ønsker Ringerike kommune seg løsninger som er modulbasert på den måten at de er laget med en tjenesteorientert arkitektur i bunn. Dette gir mer autonome tjenester som leverer data med stor grad av uavhengighet til andre dataentiteter. Dette gir igjen Ringerike kommune større mulighet til å kunne sette sammen data fra mange API'er til gode innbyggertjenester.

Se avsnittet «Definisjoner og forklaringer» for en utdypende forklaring på hva som menes med åpne API'er.

## 3.2. *Arkitekturprinsipper*

For å underbygge samt stille krav til en helhetlig virksomhetsarkitektur vil Ringerike kommune bruke de samme arkitekturprinsipper for alle løsninger.
Arkitekturprinsippene følger Difi sine anbefalinger rundt nasjonal arkitektur (https://www.difi.no/).

- **Helhetlig tilnærming** – Ringerike kommune ønsker å kunne se de enkelte fag- og støttesystemer i en større sammenheng for å unngå silo-tenking og heller skape gevinster på tvers av sektorer og avdelinger.

- **Prosessorientering** – Det er viktig at IT-løsningene er gode verktøy som understøtter kommunens prosesser for å levere tjenester.

- **Brukskvalitet** – Kommunens IT-løsninger skal utformes på en måte som sikrer effektivitet og en god brukeropplevelse.

- **Tjenesteorientering** - er en tilnærming og en fremgangsmåte der informasjon og funksjoner defineres og leveres gjennom tjenester. Tjenester åpner for effektivisering gjennom gjenbruk i stedet for å utføre de samme eller lignende tjenester flere steder av flere tjenesteytere eller IKT-løsninger.

- **Interoperabilitet** (evne til samhandling) – Det er viktig at fag- og støttesystemer ved behov kan utveksle informasjon med andre virksomheter og systemer, slik at to eller flere løsninger kan benyttes for å understøtte andre prosesser.

- **Tilgjengelighet** - Alle aktuelle brukergrupper skal ha tilgang til nødvendig funksjonalitet og informasjon i rett form til rett tid og på rett sted, brukervennlig og universelt utformet.

- **Sikkerhet** – Alle IT-løsninger som blir innført skal etableres og driftes på en sikkerhetsmessig god måte, samtidig som informasjon og tjenester er elektronisk tilgjengelig for de som har behov for og/eller rettigheter til disse. Alle krav til sikkerhet som følger av regelverk, instrukser og planer må følges. Følgende konsekvenser skal gjennomgås og beskrives:
    - Kartlegge hvilket informasjonsinnhold løsningen skal omfatte.
    - Ha definert et nivå for hvilken risiko som aksepteres.
    - Gjennomføre en risikoanalyse av løsningen, basert på virksomhetens behov og egenart.
    - Tilordne løsningen et passende sikkerhetsnivå.
    - Implementere sikkerhetstiltak for IT-løsningen, som tilfredsstiller det sikkerhetsnivået som er besluttet.

    - Teste at sikkerhetstiltakene fungerer som forventet IT-løsningens sikkerhetsnivå må kunne endres ved behov.

- **Informasjonssikkerhet** – Kommunens IT-løsninger i seg og informasjonen i den, skal med utgangspunkt i formelle og risikobaserte krav beskyttes mote brudd på konfidensialitet, integritet og tilgjengelighet.

- **Åpenhet** – Kommunens IKT-løsninger skal understøtte rettssikkerheten ved at det skal være kjent hvilke premisser som ligger til grunn for avgjørelser. Dette betyr at IKT-løsninger skal utvikles på en måte som gjør at avgjørelser er dokumenterbare og sporbare. Dette innebærer at forvalteren av IKT-løsningen må kunne redegjøre for datagrunnlag og regelanvendelse ved behov (revisjon).

- **Fleksibilitet** - Virksomhetenes organisering, prosesser, IT-løsninger, informasjon og teknologi skal utformes på en slik måte at de kan understøtte endringer, og ikke virke som begrensninger for endringer.

- **Skalerbarhet** – Kommunens IKT-løsninger skal fortsatt kunne benyttes selv om graden av utnyttelse endrer seg. Endring kan være knyttet til antall brukere, data-volum, responstider, eller IKT-løsningens livsløp.

- **Samhandling** – Følge Norsk arkitekturrammeverk for samhandling. Det skal tas høyde for å gjøre de riktige løsningsvalgene når man skal forenkle, forbedre og effektivisere samhandlingen i offentlig sektor.

- **Nasjonale felleskomponenter** – der det finnes nasjonale felleskomponenter skal disse benyttes.

## 3.3. *Sikkerhetsarkitektur*

Ringerike kommune ønsker å bygge sikkerhetsarkitekturen på moderne sikkerhetsprinsipper, og bruker NSMs «grunnprinsipper for IKT-Sikkerhet» som et utgangspunkt for å få til dette.

Disse grunnprinsippene bygger på internasjonale standarder som ISO27002:2017, NIST Cyber Security Framework og CIS CSC Top 20.

Viktige prinsipp er «Defense-in-depth» og «Trust-no-one», det vil si at det skal være mange lag med sikkerhet og at sikkerhet ikke skal baseres på at maskiner eller nettverk defineres som sikre. Alle systemer skal konfigureres etter beste praksis for sikkerhet og sikre baselines skal benyttes når klienter og servere settes opp.

Nettverket er segmentert i soner og trafikk mellom soner er sperret så lenge det ikke er eksplisitt åpnet for. Systemer som inneholder sensitive data er plassert i sikre soner som er

beskyttet av egne dedikerte brannmurer. Servere, utstyr og klienter er skilt i egne soner og adskilt av brannmur.

# 4. Identitets- og tilgangsstyring

Med alle ansatte og elever i Ringerike kommune er det meget viktig å kunne styre tilganger til alle IT-systemer, utstyr, bygninger mm. på en effektiv måte. Det å ha kontroll på autentisering, autorisering, roller og rettigheter er avgjørende for å kunne tilby ansatte en sømløs opplevelse i sin arbeidshverdag. I tillegg er det viktig å kunne dokumentere hvem som har hvilke tilganger fra et revisjonsperspektiv.

Single sign-on (SSO) er en klar forventning til alle løsninger og fagapplikasjoner.

## 4.1. *Intern Identitets- og tilgangsstyring*

Ringerike kommune vil benytte sine løsninger for identitets- og tilgangshåndtering (IDM&IAM). Løsning som benyttes er LCS (LifeCycle Server fra DotNet Internals), for å opprette og synkronisere identiteter, grupper, roller og organisasjonsstruktur mellom kataloger, databaser og applikasjoner.

HRM, økonomi, oppvekstadministrativt system (IST Hypernett) og Visma Voksenopplæring er viktige grunndatasystemer og blir «master-data» for identiteter, grupper, roller og organisasjons-strukturer. Kommunens katalog (AD/ADFS) er bygget basert på data fra disse grunndatasystemene. Ved å bruke disse systemene sikrer kommunen kontroll på tilganger og ikke minst vil administrasjon av tilganger bli automatisert. En annen viktig gevinst er at data oppdateres et sted og gjenbrukes.

IT-enheten samarbeider med «fagmiljøene/sektorene» og fagapplikasjonsleverandører og integrere deres systemer med IDM- og IAM-plattformen for tilordning av tilganger med brukere og roller.

Der det ikke lar seg gjøre å integrere alle tilganger er det en intern webtjeneste ved navn «mine tilganger» som skal benyttes for administrering av tilganger.

## 4.2. *Ekstern identitets- og tilgangsstyring*

### *4.2.1. ID-porten*

Ringerike kommune vil bruke ID-porten for autentisering der eksterne brukere/tjenestemottakere skal ha tilgang til løsninger som krever pålogging.

### *4.2.2. Feide*

Feide - Felles Elektronisk IDEntitet - er Kunnskapsdepartementets valgte løsning for sikker identifisering i utdanningssektoren. Ringerike kommune vil bruke dette for autentisering mot tjenester som skal brukes av utdanningssektoren.

### *4.2.3. G-suite*

G-suite er etablert for utdanningssektoren, så alle lærere og elever har Google konto som er tilgangsstyrt med Feide pålogging.

### *4.2.4. Single Sign On (SSO)*

Det er en forventning til at alle nye løsninger, også fagsystemer, både som SAAS og lokalt installert, skal støtte SSO med AD eller ADFS. Eventuelt Feide eller G-suite for systemer kun knyttet til lærere og/eller elever.

# 5. Systemteknisk informasjon

## 5.1. *Infrastruktur beskrivelse*

### *5.1.1. Kommunikasjon*

Ringerike kommune har et datanettverk som dekker alle tjenestene i kommunen, 70+ lokasjoner. Disse er koblet sammen via både eide og leide samband (xdsl, fiber og radio). Båndbredden verier mellom 4 mbit til 10 gbit.

### *5.1.2. Utstyrspark*

Kommunens klientpark er pr. 1.1.2018: 3642 stk. fordelt mellom PC, Tynnklient og Chromebooks. Antallet stiger. Det er i overkant av 700 pads og mobiltelefoner.

### *5.1.3. Plattformer for virtualisering, tynnklienter og windows*

Det stilles følgende systemtekniske krav og forutsetninger:

- Windows-basert applikasjon
- Fortrinnsvis 64 bit for både klient og serverapplikasjoner. Minimum 32 bits kode.
- Alle applikasjoner skal være kjørbare på VMware Horizon 7 og nyere.
- Horizon applikasjonsteknologi er Windows 10 64bit Enterprise med vdi persona management (roaming profiles).
- Servere kjører Windows 2016, 2012, 2012 R2, 2008 og 2008R2 (Standard og Datacenter Edition) 64bit. Nye servere installeres utelukkende med Windows Server 2016.
- Tykke klienter kjører Windows 10 Enterprise 64-bit eller nyere.
- Programmer som tilbys kommunen skal kunne kjøres i et virtuelt servermiljø. Kommunen benytter VMware som plattform.
- Flerbrukersystem – i praksis ingen begrensning på antall samtidige brukere
- Det er fordel om systemet er web-basert (plattform spesifisert nedenfor).

### *5.1.4. Katalogtjeneste*

Ringerike kommune bruker Microsoft Active Directory som katalogtjeneste.

### *5.1.5. Databasestandarder*

- Oracle database, ver 11g
- MS-SQL 2016
- MySQL V5.7/8.0

Oracle er vedtatt nedlagt, så nyinstallasjoner må kjøre på annen databaseplattform.

### *5.1.6. Overvåknig*

Ringerike kommune benytter PRTG fra Paessler til overvåkning av applikasjoner og infrastruktur.

### *5.1.7. Kommunikasjonsprotokoller*

Det er kun TCP/IP som tillates, systemer må ikke kreve eller generere andre protokoller. De fysiske standardene er beskrevet nedenfor.

### 5.1.8. Utskriftstjenester

Systemet skal benytte kommunens utskrift-servere for all utskrift. Eventuelle drivere skal leveres både for 32-bit og 64-bit Windows systemer. Kommunen benytter følg-meg-utskrift med Canon MFP og Uniflow, dette må støttes.

### 5.1.9. Elektronisk post

Standard system for elektronisk post er MS-Outlook 2016 på klientsiden og MS- Exchange 2016 på serversiden. Utover Outlook tillates det kun SMTP og IMAP i kommunikasjon mot Exchange som må avtales spesielt i hvert enkelt tilfelle.

### 5.1.10. Serverstruktur

Strukturen på serverne som inngår i den totale løsningen er delt inn i soner. Kommunens serverfarm er i hovedsak delt i 4 soner.

- DMZ (Sone for kommunikasjon med omverdenen, web tjenester til innbyggere, næring og brukere)
- Intern sone (Sone for saksbehandling, e-post og kontorstøtte)
- Intern DMZ (for transport av transaksjoner og andre data mellom intern og sikker sone)
- Sikker sone (sone for behandling av helseinformasjon mm.)

Alle nye løsninger skal dekke Datatilsynets krav, se mer på http://www.datatilsynet.no/.

### 5.1.11. Sone sikkerhet

Sonene er en del av kommunens sikkerhetsarkitektur, og er basert på følgende prinsipper:

- Servernettverket er delt i fire soner (DMZ, Intern, intern DMZ og sikker).
- Klienter og utstyr ligger ikke i samme sone som servere.
- Soner for utstyr (f.eks. SD-bygg styring og velferdsteknologi) har ikke direkte tilgang til internett.
- Det er ikke lov at utstyr og klienter kan benyttes som broer, dvs. flere tilkoblinger til forskjellige soner (f.eks. utstyr kan ikke være kablet til SD-nett og tilknyttet 3G/4G).
- Det er klart skille mellom tjenester og klienttyper inndelt i relevant sikkerhetspolicy.
- Tilgang til tjenester reguleres gjennom bruk av sikkerhetsbarrierer (brannmurer, VLAN, pakkefilter, applikasjonsfilter, innholds filter, autentiseringsløsninger, VPN/SSL-GW, krav til klienter og tjenere, m.m.
- En sone har ikke tilgang til en sone med høyere sikkerhetsnivå med mindre det er eksplisitt tillatt, og regulert i en brannmur.
- En sone med høyere sikkerhetsnivå har ikke tilgang til en sone med lavere sikkerhetsnivå med mindre det er eksplisitt tillatt, og regulert i en brannmur.
- Kommunikasjon/brannmuråpninger mellom soner skal risiko vurderes og det er ikke mulig å forsere mer enn en sone av gangen.

- Hver sone inneholder ett eller flere nettverkssegmenter.

Soner:

| DMZ | Intern | Intern-DMZ | Sikker |
|---|---|---|---|
| Internettrelaterte systemer | Administrative og fagorienterte nett | Transportnett sikker og intern | Behandling av sensitive personopplysninger |
| Transportnett for internett og intern | Driftsnett | | Helse- og omsorgssystemer |
| | Tekniske tjenester | | Virksomhetskritiske løsninger |
| | Elevnett | | SD og velferdsteknologi |

Datatilsynets krav og retningslinjer blir overholdt av kommunen. Det forutsettes at leverandører av programvare holder seg innenfor de samme rammer. Dette gjelder all form for kommunikasjon, slik som:

- Tradisjonelle filoverføringssystemer
- Applikasjonsbaserte datastrømmer
- Låsesystemer
- Talesystemer
- Andre signalbaserte systemer

### *5.1.12. DMZ soner*

Kommunen benytter en kompleks sammensatt Demilitarisert Sone(er) mellom LAN og Internett og mellom sikker og intern sone. Alle systemer som skal kommunisere fra Internett til LAN eller omvendt må kommunisere igjennom en sikkerhets-Gateway dersom to soner passeres. Ytterligere informasjon får man ved beskrivelse av hva som ønskes i en egen henvendelse til IT-enheten.

Følgende tjenester er organisert i DMZ bak F5:

- Termineringspunkt for alle eksterne nettverk
- Eksterne navnetjenester, DNS (autorativ og publiserende)
- Eksterne nettsider, innbyggerportaler etc.
- E-post sending- og mottakspunkt
- Webmail og ActiveSync
- Tilgangspunkt mot intranett
- VPN-tjenester for ansatte og andre
- Kommunikasjon med tjenestetilbydere
- Lync federering mot eksterne

Alle nye tjenester i DMZ skal plasseres bak sikkerhet til F5 fra BigIP. For mer informasjon se https://f5.com/

### *5.1.13. Intern sone*

Følgende tjenester lagt til intern sone: Systemadministrative og fagorienterte nett, tekniske tjenester, administrative systemer og driftsnett, administrasjon av fjerntilgang samt klienter med mulighet for aksess til tjenester i lukket sone.

### *5.1.14. Sikker sone*

Alle tjenester og systemer som inneholder sensitive personopplysninger ref. personopplysningsloven § 2-8 og alle virksomhetskritiske systemer plasseres i en lukket sone.

### *5.1.15. SD og velferdsteknologi sone*

Alt utstyr som benyttes til velferdsteknologi og SD bygg styring legges i denne sonen, sonen håndteres som en sikker sone og har ikke direkte tilgang til Internett. Det kan etableres kontakt til NHN (Norsk Helsenett).

Tilgang til å knytte utstyr i denne sonen til trådløst (WLAN) eller mobilt bredbånd må vurderes særskilt med IT-enheten.

### *5.1.16. Elevnett*

Elevnett er der alle elever får tilgang til læringsressurser på lokalnett og internett.

### *5.1.17. Nettverksprinsipper*

Alle løsninger skal benytte eksisterende nettverk. Det er etablert kommunalt nettverk som knytter sammen alle kommunale lokaliteter. Hver lokasjon har egen lokalnett med minimum CAT-5 standard sprede nett. All aksess og tilknytning til lokalnettet avtales med IT-enheten. Bærende protokoll for all kommunikasjon skal være TCP/IP.

- Ethernet 10/100/1000BaseT
- Power over Ethernet (802.3af og 802.3at)
- WiFi 802.11 b/g/a/n/ac med 802.1x sikkerhet
- Fortrinnsvis faste IP-adresser for alt permanent tilknyttet utstyr

For all navngiving finnes det interne konvensjoner, tilsvarende også for adressering (eks. IP). Tilbyder skal konferere med IT-enheten for få tildelt navn og IP adresser for løsningene ved implementering. All navngivning eller adressering skal tildeles av IT-enheten. Det skal ikke tilbys løsninger som krever spesielle navngitte servere/hoster.

## 5.2. *Krav til programmer/applikasjoner*

### *5.2.1. Installasjon*

Alle programmer som skal installeres på Windows klienter skal leveres på MSI-fil format. Alternativt kunne settes opp til å installeres ”unattended”. Når en ny applikasjon installeres kan IT kreve at den først installeres på en testserver og testes for å hindre at den påvirker annen programvare i produksjon. Deretter skal den legges på serveren som programmet skal kjøres i produksjon på. Programmene skal kunne installeres/rulles ut ved hjelp av MS System Center Configuration Manager (SCCM).

Programmer som skal distribueres til mobiltelefoner og/eller pads må støtte utrulling via MDM verktøyet Airwarch fra VMware.

### *5.2.2. Oppdatering -” Nye versjoner”*

Tilsvarende rutine og krav som under pkt. 3.2.1. Enhver ny versjon av et program skal leveres IT-enheten slik at den kan testes før den settes i produksjon. Alle oppgraderinger skal leveres som en komplett installasjon av programvaren.

### *5.2.3. Publisering av applikasjoner*

Applikasjoner distribueres og pakkes, til tykke klienter med SCCM 2016 og til tynnklienter via VMware Horizon. VMware Airwatch for pads og mobiler. Alle nye applikasjoner må støtte alle disse måtene å distribueres på.

### *5.2.4. Adresseringer*

Program skal kunne kjøres i et stormiljø. Dette innebærer at alle ressurser skal kunne adresseres internt fra programmet. Eksempler på dette kan være:

- At filområder applikasjonen benytter skal kunne styres til perifere disker, normalt også andre servere.
- At databaser legges på felles databaseservere.
- Ikke annet enn selve den eksekverende delen av programmet finnes på applikasjonsserveren og/eller klienten.

Dette innebærer blant annet at all internadressering aksepterer bruk av UNC-bane.

### *5.2.5. Programvarelås*

Det tillates ikke leveranser av programvare med noen form for fysisk programvarelås, dongler, USB brikker etc. All kontroll av lisensnummer skal skje mot fil baserte løsninger lokalisert på den samme serveren som applikasjonen ligger.

### *5.2.6. Fjerndrift/-leveranse*

Alle dataprogrammer som krever installasjon og kommunikasjon i kommunens nettverk skal som hovedregel kjøres på server lokalisert ved kommunens datasenter. Alle programmer

skal installeres av personell fra kommunenes IT-enhet, eller i samarbeid med leverandør – hvis det er formålstjenlig. Datasenter er tilknyttet internett og fungerer som skyløsning (Private Cloud), så alle lokalt installerte systemer kan tilgjengelig gjøres i skyen. Datasenteret har ferdig 2 faktor autentisering og mulighet for ytterligere sikkerhet der det kreves.

Ved lokal installasjon er det normalt IT-enheten som har ansvar for drift og oppgraderinger av løsningen, hvis ikke annet er avtalt særskilt.

Der det er gunstig er det åpning for at programmer installeres om SAAS (Software As A Service) i skyen. Der det velges ekstern skyløsning, stilles det strenge krav til behandling av data. Data av sensitiv art skal ikke behandles i fjern driftede løsninger. Løsningene kan heller ikke inneholde elementer av integrasjon med våre øvrige IT-løsninger internt. Kommunens mal for databehandleravtale skal benyttes. Systemeier har ansvar for avtaler og risikovurderinger ifht. ekstern lagring av informasjon.

Ved SAAS løsning er det leverandøren som har ansvar for drift og oppgraderinger av løsningen.

## 5.3. *Database regler*

Følgende regler gjelder for implementasjon av relasjonsdatabaser med relasjoner mot eksisterende systemer i kommune samarbeidet. Når en leverandør skal implementere databasesystemer som skal ha relasjoner, views, triggere eller annen kontakt med eksisterende databaser gjelder alle hovedreglene herunder.

### *5.3.1. Data skal kun finnes ett sted*

Normaliseringsnormene for databaser skal følges, dette innebærer at når systemet har behov for data som finnes i et eksisterende system, skal disse registrene/tabellene ikke dupliseres. Systemet skal hente data fra det eksisterende systemet. Dette gjelder selv om det vil medføre omskrivninger av systemet. Disse data skal hentes i et API eller et View mot de eksisterende tabellene. Det tillates ikke at tabeller kopieres over til systemet.

### *5.3.2. Opprettelse av ”sysposter”*

Når det ikke er mulig å opprette relasjoner kun ved bruk av Views tillates det å kopiere over systempost(er), felter med innhold, som muliggjør opprettelse av relasjoner mot systemets datastruktur. Minst mulig datamengde skal kopieres over. Kopiering av ”sysposter” anses ikke som duplisering av data.

### *5.3.3. Handlinger mot eksisterende systemer*

All programkode (Triggere, SQL-statement, prosedyrer) som utfører oppslag mot Views eller Snapshot og som sørger for oppdatering av ”systemposter” må ligge i systemet. Det er ikke tillatt å skrive kode inn i de eksisterende systemene.

### *5.3.4. Oppgradering av databaseserver*

Leverandøren bærer selv ansvaret for at systemet lar seg oppgradere i takt med kommende oppgraderinger av de eksisterende systemene. Når en eksisterende systemtabell får nytt navn og relasjonen forsvinner må leverandøren oppgradere sin egen kode.

## 5.4. *Krav til integrasjon med andre systemer*

Utover de ovenstående reglene for databaserelasjoner gjelder også;

- Alle utvekslingsprosedyrer skal ligge i systemet.
- Utveksling av data mellom systemet og eksisterende løsninger skal gå automatisk

Tilbys en annen løsning/modell enn dette, må den begrunnes og beskrives spesielt.

Tilbys det eksempelvis en form for mellomlagring av eksportdata fra eksisterende system må tilbyderen beskrive hvorledes rutinene for import til nytt system skal foregå. Benyttes det flatfil (ev. et utvekslingsformat) for mellomlagring må både utvekslingen fra eksporterende og importerende system løses og beskrives.

## 5.5. *Forhold til eksisterende løsninger*

Ved integrasjon av systemet skal ikke eksisterende systemer endres. Trengs eksport/import fra eksisterende systemer skal dette skje fra systemet. Disse eksportprosedyrene skal lagres i systemet og brukeren skal kunne nå disse fra det systemets brukergrensesnitt.

Tilbyder er ansvarlig for integrering mot eksisterende systemer. Dette innebærer at tilbyder for eksempel må skaffe databasedefinisjon(er) direkte fra leverandørene av eksisterende systemer. Kommunen kan være behjelpelig med å etablere kontakt med kommunens IT leverandører.

Følgende garantier må gis i tilbudet:

- Dersom løsningen det skal integreres mot tilbyr et ferdig integrasjonslag skal dette benyttes i størst mulig grad.
- Leverandøren skal gi garantier for at innlesningsprosedyre(er) fra eksisterende system fungerer tilfredsstillende.
- Leverandøren skal gi garantier for at eksport fra systemet fungerer tilfredsstillende.
- Leverandøren skal gi garantier for at ved endringer av eller i eksisterende system må leverandøren oppgradere systemet slik at det fortsatt fungerer (eksport/import) optimalt. Leverandøren skal kun gjøre dette etter skriftlig avtale med IT-enheten og kommunen.

- Leverandøren skal legge alle Views, Triggere, Prosedyrer, etc. internt i det nye systemet. Ingen kode må legges i eksisterende systemer.

I motsatt fall, at en annen leverandør trenger opplysninger om det innkjøpte systemet forplikter leverandøren å tilrettelegge slik at en av samarbeidets andre underleverandører for tilgang på nødvendig informasjon. Herunder eksempelvis databasestrukturer, kildekode

etc. Likeledes forplikter leverandøren seg til å etablere et gjensidig samarbeid med kommunens andre aktuelle leverandører.

## 5.6. *Leverandørtilgang*

Leverandørtilgangen er regulert i kontrakts form, mellom IT-enheten og den enkelte leverandørs konsulent. Leverandøren kontakter IT-enheten for å få opprettet en slik samarbeidsform.

Det er utarbeidet en egen rutine/instruks for denne ordningen som skal følges, dette blir opplyst ved inngåelse av en slik kontrakt.

Leverandøren er ansvarlig for installasjon, oppsett og feilsøking av tilgangsløsning på sine ansattes maskiner.

## 5.7. *Krav til systemadministrasjon*

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

## 5.8. *Krav til brukergrensesnitt*

Systemet skal være brukervennlig og Windows-basert. Systemet skal benytte grafisk brukergrensesnitt (GUI), og følge standard for universell utforming, ELMER og andre offentlige konvensjoner for GUI. Systemet skal ha en lettforståelig struktur av skjermbilder og menyer.

Systemet skal også kunne håndteres av brukere som tilbringer liten del av sin arbeidsdag foran en dataskjerm.

## 5.9. *Krav til oppgraderinger*

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.

Ved hver programvareleveranse skal det medfølge en installasjonsveiledning.

## 5.10. *Virtuelle server-miljøer*

IT-enheten benytter VMware for å kjøre virtuelle servermiljøer. Standarder i dag er VMware med Vcenter 6.5. På hostene er ESXi 6.5 installert. Dette kjøres over flere fysiske maskiner i HA-cluster.

# 6. Standard applikasjoner

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

| Type | Produkt |
|---|---|
| Kontorstøtte | Microsoft Office 2016, 32bit |
| Internett «Browser» | Internet Explorer 11, 64 bit, Google Chrome siste versjon |
| Bildebehandling | MS-Paint og Paint.Net |
| Verktøy | Til enhver tid siste versjon av Java, Adobe produkter og .Net. Støtte for Silverlight og Flash legges ned. |
| Dørlåssystem/adgangslkontroll | Tidomat |
| CallSenter | TRIO |
| ERP | Visma Enterprise |
| Sak/arkiv-system | ESA 8 |

Skal tilbudt system integreres mot andre standardapplikasjoner må tilbyder ta kontakt med IT-enheten for å få rede på hvilke øvrige applikasjoner som er standard. Tilsvarende gjelder også for spesielle applikasjoner/fagapplikasjoner, der det finnes en lang liste godkjente programmer.

# 7. Krav til opplæring

Leverandøren må kunne stå for opplæring av brukere og/eller av løsningsansvarlige for systemet, når dette kreves av kommunen. Prosjekteier/systemansvarlig beslutter endelig omfang av opplæringen.

Forslag til opplæring skal være beskrevet i tilbudet.

Opplæringen må tilpasses de enkelte brukeres behov, og derfor deles opp i grupper, som f.eks.:

- Brukere som kun skal ha spørre tilgang
- Brukere som skal registrere/bruke systemet

Kompleksiteten til systemet vil være avgjørende for valg av løsning for opplæring. Det må utarbeides en milepælsplan og ansvarskart for opplæring. Denne må redegjøre for metode, tidsplan, ressursbruk samt kostnader.

- Leverandører skal stille et forhåndsavtalt antall konsulenttimer til rådighet for kommunen til bruk i opplæringsøyemed.
- Leverandøren skal utarbeide komplett opplæringsmateriell som kommunen kan distribuere til sine brukere.
- Leverandøren har ansvar for at sine konsulenters maskiner er satt opp slik at de fungerer i kommunens nettverk. Ressursbruk på dette er ikke fakturerbart.

Kommunen vil kunne kreve opplæring av interne superbrukere som igjen står for videre intern opplæring.

Eventuelle krav til opplæring fra leverandør før funksjoner og system kan tas i bruk, skal informeres om i tilbudet.

# 8. Krav til dokumentasjon

Dokumentasjonen skal omfatte alle deler av systemet og skal være på norsk. Dokumentasjonen/brukerhåndbøkene skal sikre at systemet brukes på en forsvarlig og korrekt måte.

Dokumentasjonen skal foreligge både i elektronisk redigerbart format og i form av hjelp-funksjon i systemet. Det er viktig at brukeren i et hvert skjermbilde skal kunne søke på aktuelle hjelpe-ord eller funksjoner.

## 8.1. *Systemdokumentasjon*

Systemdokumentasjonen skal vise hvordan systemet er bygd opp og hvordan kravene til funksjonalitet i regelverket er ivaretatt slik at brukere på en enkel måte kan sette seg inn i hvordan systemet fungerer.

Systemdokumentasjon, oppsettparametere, -regler, maskinelle kontroller og tilgangs-rettigheter som er nødvendig for etterprøving, skal fremgå på en oversiktlig måte.

Systemdokumentasjonen skal minimum inneholde en datadictionary med beskrivelse av hva de ulike tabeller/felt brukes til og angivelse av eventuelle maskinelle kontroller tilknyttet til de enkelte felt og hvordan system genererte feltverdier beregnes.

Komplett databasemodell skal leveres.

Applikasjonen skal inneholde historikk med entydig identifikasjon, produksjonsdato og periodeangivelse. Det skal være mulig å kontrollere at ingen historikk kan overstyres i ettertid. Historikken skal være implementert i løsningen og kunne leses til enhver tid.

## 8.2. *Brukerdokumentasjon*

Det skal være system for oppdatering av brukerhåndbøkene. Oppdatering kan skje ved overføring av filer med dokumentasjon, eller ved fysisk oversendelse av papirbaserte endringsdokumenter.

# 9. Telefoniløsninger

Nye virksomheter skal ikke ha telefonsentral lokalt.

Ringerike kommune benytter som hovedregel mobil telefoni og mobilt sentralbordløsning ved behov.

Alle tiltak, ønsker og tanker om løsninger innen telefoni og -sentraler skal IT-enheten involveres i før beslutninger tas. Alle løsninger skal ha en driftsavtale med leverandør for service, support og vedlikehold, slik avtale inngås av hver enkelt enhet.

# 10. Infrastruktur og kabling

Utover krav nevnt her, henviser vi for krav til byggstyring og SD-anlegg til Eiendom sin prosjekteringsanvisning for automatiseringsanlegg, et dokument ved navn «RK PA Automatisering».

## 10.1. *Nettverksprinsipper*

Hver lokasjon har eget lokalnett med minimum CAT-5/CAT-6 spredenett. All tilkobling av utstyr i lokalnettet skal avtales med IT-enheten. Det skal ikke etableres lokale trådløse nettverk. Alle switcher og annen nettverkselektronikk som skal benyttes skal leveres gjennom IT-enheten.  Alt permanent utstyr som tilkobles skal konfigureres med TCP/IP, og det lages reservasjoner på IP adresser. For alt utstyr som tilkobles nettet er det etablert interne konvensjoner for navngiving og IP adressering.

Tilbyder skal konferere med IT-enheten for å få tildelt navn og IP adresser for løsningene ved implementering. All navngivning eller adressering skal tildeles av Ringerike kommune med mindre noe annet er avtalt spesielt. Navngiving og adressering skal være enkelt å endre i løsningen.

## 10.2. *Ansattkort*

Alle ansatte i Ringerike kommune vil få utdelt et ansattkort med bilde og ansattinformasjon. Kortet har i tillegg teknologier for RFID basert på Mifare. Ved implementering av løsninger som benytter kort skal IT-enheten rådspørres for å i den grad det er mulig å benytte eksisterende kort.

## 10.3. *Adgangskontrollsystemer*

Kommunen vil ha sentraliserte adgangskontrollsystemer. Løsninger som finnes i dag er basert på Tidomat. Nye adgangskontrollsystemer må kunne administreres via dette systemet. Grunnen til kravet er at det automatisk blir opprettet og sperret brukere og kort gjennom en integrasjon med kommunens personalsystem.

Det er etablert Tidomat server plassert i kommunens datasenter. Det kreves at installatør av adgangssystemet har gjennomført opplæring hos importør.

- Adgangskontroll kommuniserer på eget nettverk for bygg styring, og IT-enheten utsteder faste ip adresser til alle enhetene i dette nettet.
- Ved valg av annet utstyr enn Tidomat, må det integreres med etablert serverløsning.
- Adgangskontroll er et adgangssystem og skal ikke brukes til brann og rømning.

Leveranser på Adgangskontroll skal være fullstendige, dvs. inkludere alle arbeider rundt dører, adgangssoner, tidsplaner, brukergrupper, kontroll/testing og opplæring til sluttbrukere.

Det skal leveres med en installasjon av Tidomat klient hos bruker av bygget for administrasjon av brukere og deres sone/gruppetilknytninger. Samt tilknytning mellom bruker og kommunens ID-kort.

Kommunens ID-kort som ansatte får utstedt skal benyttes.

Der det kreves egne kort for eksterne (f.eks. utleie), skal plan og opplæring for dette også leveres med.

## 10.4. *Kabling*

Denne instruksen gjelder for all kabling av svakstrøm og fiber i Ringerike kommune. Denne må legges til grunn ved prosjektering og etablering ved renovasjoner og nybygg, og må benyttes som norm for personell som gjennomfører arbeidet (elektriker).

Alt nettverksutstyr og overvåkning av dette skal avtales og bestilles gjennom IT-enheten. Spesielt utstyr som etter avtale med IT-enheten, må leveres av leverandør, må ha avtale med leverandør om daglig drift, overvåkning og vedlikehold.

| Termineringspanel | Kabler | Kontakter |
|---|---|---|
| **Generelt**<br>I alle termineringspunkter skal det benyttes RJ45 i 24 punkters paneler.<br><br>Utstyret skal være tilpasset 19” profiler.<br><br>Alt utstyr skal være i Category 6a | **Kabler til arbeidsplass**<br>Det skal benyttes category 6a kabler hele veien også dersom man skal tilfredsstille spesielle branntekniske krav. | **Datanett**<br>Alle kontakter skal være av type Cat6a og RJ45 med 568Bstandard<br>på pinneutlegget i kontaktene.<br><br>Alle par skal termineres selv om punktet er beregnet for andre tjenester. |
| **Fiber**<br>All terminering av fiberkabler skal foretas med SC-konnektorer og monteres i 19" fiberpaneler der hvor det finnes denne type rack. Ellers kan fibrene termineres i veggbokser. | **Fiber**<br>Fiber for intern bruk i bygg skal være multimodus. Utvendige kabler avtales før de legges. Lengde avgjør bruk av singel eller multimodus. | **Fiber**<br>Det skal leveres med patchekabel SC-LC i passende lengde for tilkobling av switch. |
| **Merking**<br>All merking skal følge eget merkesystem (se eget avsnitt nedenfor). | **Merking**<br>All merking skal følge eget merkesystem (se eget avsnitt nedenfor). | **Merking**<br>All merking skal følge eget merkesystem (se eget avsnitt nedenfor). |

**Alle kablingsarbeider skal utføres av sertifiserte installatører.**

- Hvis det finnes eksisterende kabling av dårligere kvalitet i bygget som ønskes benyttet, må det vurderes i en gjennomgang av bygg og planlagt bruk med IT-

enheten og Eiendom. Dette gjelder også ved uforutsette problemer som plassmangel o.l.

- Der det kables til flere funksjoner, skal punkter skilles ved egne paneler. For eksempel skal følgende funksjoner splittes i forskjellige paneler: punkter til trådløst nettverk, veggpunkter for brukere, adgangskontroll, SD-styring, talevarsling osv. Der utstyr krever PoE må dette også planlegges i egne paneler, og avtales med IT-enheten. Ved større installasjoner over 100 punkter, skal detalj plan for svakstrømskap, paneler, punkter og funksjoner være gjennomgått og godkjent med IT-enheten før termineringsarbeid starter.
- I skap med mer enn 3 paneler (72 punkter) skal det legges inn rom for switcher mellom panelene. Til vanlig tar en switch 48 punkter, men dette kan avvike pga. funksjon og skal derfor planlegges i samarbeid med IT-enheten før termineringsarbeid i skap starter.
- Alle kabler skal termineres på godkjente panel og med krone verktøy. Det er også nødvendig at kablene er lange nok til eventuell flytting senere (2-3 meter ekstra).
- Hvis kabellengde overstiger 90 meter på punkt mellom to skap/switcher skal fiber kabel benyttes. Ved kabling til punkt (vegg) kan denne lengen være 100 meter.
- Der det er behov for flere dataskap skal det kables og termineres 2 stk. cat 6a forbindelser mellom skapene. Eventuelt 2 stk. fiber der avstand krever det.
- All kabling som termineres over letthimling skal merkes ut under himling, slik at den lett skal kunne finnes igjen.

### *10.4.1. Kabelføringsveier*

Ved fremføring over himlinger og lignende skal det skal tas hensyn til avstander til annet elektrisk utstyr som kan påvirke signalering, for eksempel lysrørsarmaturer. Kanaler skal inneholde faste separate føringsveier for sterk- og svakstrøm. I videre føringsveier må separasjon opprettholdes.

Alle gjennomføringer skal legges i rør/løsninger som forenkler etter trekking av ny kabling eller utskiftning.

### *10.4.2. Punktplassering*

Plassering av og antall innvendige datapunkter skal gjøres i samråd med Eiendom, IT-enheten og brukere av bygget, sammen med avklaringer rundt funksjoner.

### *10.4.3. Testing og dokumentasjon*

Installatør skal være autorisert som teleinstallatør av Post- og Teletilsynet i henhold til gjeldende regler. All kabling av spredenett og fiber skal testes 100% og være godkjent i henhold til gjeldene standard. Testdokumentasjon skal leveres IT-enheten elektronisk på pdf- format.

### *10.4.4. Merkesystem i spredenett*

Termineringspunkter i dataskap/rack skal være merket i stigende nummerrekkefølge.

Eksempel: Det første skapet som monteres i 1. etasje, skal hete 1A. Punktene fra dette skap merkes hvert panel 1A1, 1A2 osv., punkter fra disse merkes da 1A1-01, 1A1-02 osv. Eventuelt et neste skap i 1. etasje skal få navnet 1B, punktene fra første panel i dette blir da 1B1-01, 1B1-02 osv. Samme måte om det er flere etasjer; F.eks. 2A tilsier at skapet er i 2. etasje, og punktene fra første panel skal da hete 2A1-1, 2A1-2 osv.

Skap i underetasje merkes med U; eks: UA – UB osv.

Døra til skapet skal ha en klar merking: F.eks. 1A,

XYZ-NN
X = Etasje (kan være U,1,2,3,4,5,6 osv)
Y = Skap nr. i etg. (1,2,3)
Z = Panel nr i skap
NN = løpenummer på punkt

Husk å skille funksjoner i hver sine paneler (dørkontroll, wifi, datapunkt, SD ol.).

### *10.4.5. Utvendige framføringsveier*

Ved nybygg eller ved endringer av eksisterende framføringsveier av signalkabler skal det avklares med IT-enheten og Eiendom/vaktmester.

### *10.4.6. Datarom*

Med datarom, menes et rom der kabling termineres og kommunikasjonslinjer kommer inn til bygget.

Det defineres/finnes 3 typer datarom:

- Sentrale/større rom
- Perifere/små rom
- Rom for ikke kommunal infrastruktur (privat).

Hvordan hvert enkelt rom skal defineres, avgjøres i samråd med IT-enheten.

### *10.4.7. Sentrale/større rom*

Design og utførelse av datarom skal foretas i samarbeide med IT-enheten. Det skal legges kabelbro i himling eller datagulv med minimum 15 cm effektiv plass for signalkabling. Videre skal alle sterkstrøms kabler og 220V anlegg plasseres i TEK 123 kanaler i taket på anvist plass over server og elektronikk racksystemer.

Hvis det er påkrevd med slokkeanlegg skal det benyttes Argonite gass slokkeanlegg dimensjonert med en minste konsentrasjonskoeffisient på 12.5, samt godkjent alarmsender. Hvorvidt slike anlegg skal etableres fremkommer av spesifiseringen av hver enkelt anskaffelse.

Kjøling skal monteres med fordampere i taket, og beregnes ut fra avgitt effekt fra det aktuelle utstyret som skal monteres i rommet. Det skal ikke overstige 20 grader Celsius i rommet. Minimumskrav på 4 kvadratmeter forbeholdt IT-utstyr. Rack (skap) skal være 19 tommer, med en minimums dybde på 55 cm fra monteringsskinnene i forkant til monteringsskinnene i bakkant av skapet.

Det skal minimum installeres 8 ledige stikk strømpunkt i hvert skap for kommunens nettverksutstyr.

Alle datarom skal til vanlig være låst for å hindre uautorisert adgang. Vanlige ansatte regnes ikke som autorisert personell for adgang til svakstrøm (sikkerhetsnorm).

Av sikkerhetsmessige årsaker er det slik at alle servere skal plasseres i kommunens Datacenter, ikke på datarom rundt i kommunen. Usikkerhet rundt dette, kontakt IT-enheten.

### *10.4.8. Perifere/små rom*

Minimumskrav på 4 kvadratmeter forbeholdt IT-utstyr. Rack (skap) skal være 19 tommer, med en minimums dybde på 55 cm fra monteringsskinnene i forkant til monteringsskinnene i bakkant av skapet. To hyller hører med til standard installasjon.

Det skal minimum installeres 4 ledige stikk strømpunkt i hvert skap for kommunens nettverksutstyr.

Alle datarom skal til vanlig være låst for å hindre uautorisert adgang. Vanlige ansatte regnes ikke som autorisert personell for adgang til svakstrøm (sikkerhetsnorm).

Av sikkerhetsmessige årsaker er det slik at alle servere skal plasseres i kommunens Datacenter, ikke på datarom rundt i kommunen. Usikkerhet rundt dette, kontakt IT-enheten.

### *10.4.9. Rom for ikke kommunal infrastruktur*

Der det planlegges kabling for privat infrastruktur, f.eks. TV-signaler, telefon, bredbånd til omsorgsboliger e.l. så må dette termineres i eget rom for å sikre mot uautorisert adgang til kommunens infrastruktur.

Det er viktig at merking av punkter til privat- og kommunal bruk skilles slik at det er enkelt å forstå i hvilket rom de termineres.

Enhet/beboer skal selv sørge for å gi adgang til dette når behov for installatør/reparasjon melder seg.

### *10.4.10. Undervisningsrom*

Etablering av undervisningsrom må avtales med IT-enheten og bruker i hvert enkelt tilfelle, for planlegging av trådløst nettverk, trådbasert nettverk, prosjektor, tavler mm. Utover dette gjelder alle spesifikasjoner gitt i dette dokumentet.

### *10.4.11. Møterom*

Etablering av møterom som skal inneholde IT-utstyr som prosjektor, elektroniske tavler o.l. avtales med IT-enheten. Utover dette gjelder alle spesifikasjoner gitt i dette dokumentet.

### *10.4.12. Kommunikasjon*

Etablering av IT-kommunikasjon til kommunens datacenter må planlegges. Der det er mulig skal mørk fiber planlegges. Avtales med IT-enheten.

### *10.4.13. Velferdsteknologi*

Ved prosjektering/planlegging av velferdsteknologi må IT-enheten og hjelpemiddellageret involveres.

Disse teknologiene er valgt som standard eller under utprøvning for bruk i Ringerike kommune:

- Sykesignalanlegg
- Multidose/automatisk medisin dispenser
- Digitalt tilsyn
- Teleslyngeanlegg
- Lokaliseringsteknologi
- Trygghetsalarm
- WLAN

Ved etablering av slik teknologi er det et krav at det fremføres med Cat. 6a kabling og at det inngås avtale om service, drift og vedlikehold med den enkelte leverandør.

Det forutsettes at det etterstrebes at velferdsteknologi integreres med fagsystem(er) for EPJ og andre relevante IT-systemer.

Bæretjenester for velferdsteknologi må avtales med IT-enheten og bruker. Overvåkning av slikt utstyr på mange forskjellige plattformer og forskjellig utstyr er ikke ønskelig. Derfor skal allerede etablerte løsninger for dette benyttes.

# 11. Skytjenester

Skytjenester (cloud computing) er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett.
Se mer på datatilsynet sine sider: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/skytjenester---cloud-computing/

## 11.1. *Datalagring*

Vi ønsker at en leverandør av skytjenester fortrinnsvis lagrer data i EU/EØS.
Ved lagring utenfor EU/EØS må leverandør dokumentere hvorfor dette er et behov, samt kunne fremvise at «eier» av skyen har en Privacy Shield avtale med EU.

## 11.2. *Sikkerhetskopiering/speiling*

Leverandører som vil overføre personopplysninger til utlandet må følge bestemmelsene i personopplysningsloven kapittel 5 og personopplysningsforskriften kapittel 6.

## 11.3. *Databehandleravtale*

Det er den behandlingsansvarlige som velger å ta i bruk skytjenesten. Hvis tjenesten gjennomfører en behandling på vegne av den behandlingsansvarlige, er leverandøren å anse som en databehandler. Datatilsynet anser derfor en leverandør av skytjenester som en databehandler, uavhengig av hvilken tjeneste som leveres.

Det skal dermed skrives en databehandleravtale når det tas i bruk skytjenester, uavhengig av tjenestens innhold.
Databehandleravtale skal v
eie tyngre enn leverandørens eventuelle personvernerklæring

## 11.4. *Bruk av underleverandører*

Underleverandører skal være kjent og godkjent av virksomheten. Dette relaterer til problemstillingen over om hvor data lagres og om det overføres data til tredjeland.

# 12. IKT Service og vedlikehold

Oppfølging av IKT-drift og forvaltning i Ringerike kommune vil gjenbruke eksisterende prosesser for tjenesteleveranse, hendelsesstyring, endringsstyring, konfigurasjonsstyring og kapasitetsstyring.

Fagapplikasjonsleverandører må bistå sammen med driftsleverandører ved feilsøking, kapasitetsvurderinger, risikovurderinger, kontinuitetsplanlegging m.m. i de tilfeller Ringerike kommune ikke sitter på denne kompetansen.

Det er et mål at leverandøren avleverer konfigurasjonsdata elektronisk til Ringeirke kommune.

Det er viktig for Ringerike kommune å være informert om oppdateringer som gjøres på både fag- og støttesystemer uavhengig av plattformen disse kjører på. Dette da man ønsker å informere brukere om både feil som er fikset og ny eller endret funksjonalitet.

# 13. Portaler og selvbetjening

Ringerike kommune benytter EPiServer som publiseringsløsning på web for intranett og internett.

Det er også en egenutviklet innbyggerportal med ID-port pålogging.

Dagens standard Web-server system:

| System | Applikasjon | Operativsystem |
|---|---|---|
| WEB-server system | MS-IIS 8.0 og nyere | Windows 2012R2 server |
| | .NET 4.5 og nyere | |
| Redigeringsverktøy | EPI-server | n/a |

## 13.1. *Brukskvalitet*

Ringeirke kommune prioriterer opplevd brukskvalitet høyt i løsninger laget for innbyggerne. Dette skal ivaretas gjennom målrettet arbeid med universell utforming, samt sikring av gode brukeropplevelser i alle kommunens tjenester, også de som leveres av eksterne leverandører. Ringerike kommune har egen kommunikasjonsenhet som skal involveres ved designvalg.

Ringerike kommune stiller krav til at leverandørene kan levere løsninger som oppfyller kommunens suksesskriterier for brukskvalitet. Følgende kriterier vektlegges:

- **Åpent for alle:** Alle kommunens tjenester som er tilgjengelige for innbyggere skal minst oppfylle og helst overgå kravene som er fremsatt i norsk lovgivning om universell utforming. Det anbefales at brukere med ulike funksjonsnedsettelser involveres i testing og utforming av tjenestene.
- **Mulig å tilpasse:** Alle kommunens tjenester som er tilgjengelige for innbyggere skal muliggjøre tilpasninger i grensesnittet, slik at kommunen selv kan ivareta at brukeropplevelsen blir best mulig.
- **Uavhengig av enhet:** Alle kommunens tjenester som er tilgjengelige for innbyggere skal være tilpasset bruk på alle typer enheter og skjermstørrelser, ikke sette bestemte krav til operativsystem eller programvare, og tilby samme funksjonalitet på tvers av ulike enhetstyper.
- **Involvering av brukere:** Alle kommunens tjenester som er tilgjengelige for innbyggere skal være grundig testet i samråd med brukere for å sikre at riktige tjeneste leveres på riktig måte. Brukertesting bør foregå fortløpende i utviklingsløpet av nye tjenester og ved videreutvikling av funksjonalitet.
- **Ringerike kommunes visuelle profil:** Alle kommunens tjenester som er tilgjengelige for innbyggere skal fremstå i Ringerike kommunes drakt og primært benytte Ringerike kommunes designsystem for å sikre at identitet og gjenkjennelighet er ivaretatt.
- **Robust:** Alle kommunens tjenester som er tilgjengelige for innbyggere skal være implementert på en måte som er teknologisk robust; all kode skal være validerbar og basert på moderne teknologier og rammeverk, tjenesten skal kunne tåle stor pågang

av brukere i perioder og over tid, og det skal være lett å gjøre oppgraderinger og nedgraderinger ved behov.

Disse kravene blir spesielt viktige i tiden fremover ettersom innbyggerne blir mer og mer selvbetjente og ønsker å kunne gjøre mer selv. Det er spesielt viktig å ivareta behovene til de som stiller svakere i den digitale hverdagen, som f.eks. eldre eller mennesker med funksjonshemninger og -nedsettelser. Kravene til brukskvalitet skal være med på å sikre at kommunen senker terskelen for disse brukerne. Det er også viktig å ivareta Ringerike kommunes identitet gjennom en tydelig "drakt" som alle kommunens tjenester skal benytte. Dette fører til økt gjenkjennelighet hos kommunens innbyggere.

Det er også et økende behov for brukerinvolvering i prosessene gjennom å utvikle og integrere nye tjenester. Det er dessverre en kjensgjerning at man ofte tester både for lite og for sent i prosessen, og derfor blir sittende med en tjeneste som brukerne har et dårlig forhold til. Tidlig og hyppig brukerinvolvering, særlig med brukere som har spesielle utfordringer knyttet til bruk av IKT-systemer, er derfor spesielt viktig slik at alle krav og behov avdekkes.

# 14. Norm for informasjonssikkerhet i helsetjenesten (Normen)

Alle fagsystemer som benyttes til behandling av helse- og personopplysninger i helse- og omsorgstjenesten, f.eks. elektronisk pasientjournal, pasientadministrasjon, laboratoriesystem, rekvisisjon og svar og elektromedisinsk utstyr som inneholder helse- og personopplysninger er underlagt kravene i «Norm for informasjonssikkerhet».
Se informasjon beskrevet i følgende dokument: Norm for informasjonssikkerhet

# 15. Personvern og GDPR

Alle norske virksomheter må forholde seg til de nye personvernreglene i EUs forordning om personvern (GDPR). Det nye regelverket gir virksomheter nye plikter og enkeltpersoner nye rettigheter. Det er derfor viktig at de fagsystemer kommunen anskaffer har godt innebygget personvern og således behandler sensitive personopplysninger i henhold til forordningen. Hvordan hvert enkelt system, både fagsystemer og støttesystemer behandler personopplysninger og hvilke, må dokumenteres.

***Prinsippene om ansvar, integritet og konfidensialitet***

Et av de viktige prinsippene for det nye personvernregelverket er at det er virksomheten som bruker personopplysningene som har ansvar for at personvernprinsippene overholdes. Dette innebærer at virksomheten skal kunne vise at de behandler personopplysninger i tråd med personvernprinsippene.

Behandlingsansvarlig skal blant annet å sørge for tilstrekkelig og forholdsmessig sikkerhet, at personopplysningene er sikret mot uautorisert eller ulovlig behandling eller utilsiktet tap, ødeleggelse eller skade.

Dette er nedfelt i artikkel 5 i det nye regelverket.

Forskjellen fra dagens regelverk er at det blir mindre forhåndskontroll ved at melde- og konsesjonspliktene forsvinner. Men det er også en viktig endring at ansvaret blir plassert hos virksomheten. Det kommer flere og til dels tydeligere rettigheter og plikter, og det blir krav om å iverksette risikobaserte tiltak. Mer etterkontroll kan medføre strengere sanksjoner om man ikke har «orden i eget hus».

Dette er regulert i artikkel 25 om innebygd personvern, artikkel 35 om vurdering av personvernkonsekvenser og artikkel 36 om forhåndsdrøftelse.

## 15.1. *Personvern og GDPR - Konsekvenser for kommunens leverandører*

Ringerike kommunes leverandører må kunne dokumentere hvordan personopplysninger brukes og lagres i hvert spesifikt fagsystem. Dette gjelder også hvordan personopplysninger blir kommunisert inn og ut av systemet.

Kravene til avviksbehandling, varsling av berørte skjerpes i det nye regelverket, og som en konsekvens må kommunens leverandører eksplisitt beskrive hvordan avvikshåndtering utføres.

En godt definert databehandleravtale vil bli påkrevd i et hvert leverandørforhold for systemer som behandler personopplysninger.

# 16. Definisjoner og forklaringer

**Referansekatalog for IT-standarder i offentlig sektor**
http://standard.difi.no/forvaltningsstandarder/referansekatalogen-html-versjon/

Referansekatalogen er en liste over standarder som er vedtatt anbefalt eller obligatorisk å benytte i offentlig sektor. Regjeringen vedtar de obligatoriske standardene gjennom Forskrift om IT-standarder i forvaltningen og Difi vedtar de anbefalte standardene.
De obligatoriske kravene skal benyttes for anvist område, med mindre den offentlige virksomheten faller innenfor en spesifikk unntaksordning i forskriften. Anbefalte krav skal følges med mindre virksomheten har en god grunn til å handle annerledes, og dette ikke skader fellesskapet.

Referansekatalogens krav er knyttet opp til anvendelsesområder, da bruk av en standard kan variere avhengig av bruksområdet.

**EHF (elektronisk handelsformat – faktura)**
https://www.difi.no/artikkel/2015/10/elektronisk-handel-e-handel

Leverandører må kunne levere elektronisk faktura til Ringerike kommune sitt fakturamottak på Elektronisk Handelsformat (EHF), fastsatt av Fornyings-, administrasjons- og kirkedepartementet. Leveranse av elektroniske fakturaer skal skje via såkalte aksesspunkt gjennom det offentlige PEPPOL-nettverket. Leverandøren må selv bære de eventuelle kostnader leveranse av elektronisk faktura måtte medføre for denne. Kommunen gjør oppmerksom på at det finnes nettbaserte fakturasystem hvor elektroniske fakturaer kan sendes med stykkpris som et alternativ til egen oppkobling mot PEPPOL-nettverket.

**Meldingsutveksling i helse- og omsorgssektoren**
Ringerike kommune benytter helsenett for meldingsutveksling i helse- og omsorgssektoren. Se https://www.difi.no/artikkel/2015/11/helse-referansekatalogen-e-helse for beskrivelse av standarder

**Hva er et API?**
API er en forkortelse for «application programming interface» eller programmeringsgrensesnitt på norsk og er et grensesnitt i en programvare som gjør at spesifikke deler av denne kan aktiveres («kjøres») fra en annen programvare.
Det betyr at svært man kan gjøre endringer, kjøre prosesser eller på annen måte behandle data i en større kontekst. Slike samarbeidende programvaredeler betegnes gjerne som komponenter.

API-et beskriver de metoder som en gitt programvare eller et bibliotek kan kommunisere med.

For eksempel kan en utvikler bruke et API til å spørre om de ti neste avgangene fra et spesifikt busstopp.

Eksempel på et åpent API: https://www.last.fm/api

For mer utfyllende informasjon se Wikipedia:
https://no.wikipedia.org/wiki/Programmeringsgrensesnitt

**Hva menes med åpne API'er**
Med «åpne API'er» mener vi et API som er allment tilgjengelig grensesnitt for bruk utenfor det systemet som eier API'et. På engelsk skiller man på «public» og «private» som kanskje beskriver det litt bedre. Åpne API'er utveksler data over kjente protokoller (f.eks. SOAP, REST, HTTP) og med kjente formater (f.eks. XML, JSON).

Et lukket eller privat API er gjerne brukt internt i et lukket system og utveksler ofte data på et proprietært format.

Selv om et API er åpent vil det ofte trenges autentisering for å få tilgang til metodene som API'et eksponerer. Dette er fornuftig da det gir eier av API'et mulighet til å beskytte systemet bak ved å differensiere tilgangen til både tjenester og data. En slik autentisering foregår ofte i et eget lag som også håndterer antall spørring per minutt (throttling) og skalerbarhet. Dette laget er bedre kjent som «API Management» eller «API Gateway».
Et eksempel på et åpent API er DNB-Vipps sitt API for både kommersielle og offentlige virksomheter kan ta betalt for tjenester mot privatpersoner.

For mer utfyllende informasjon se Wikipedia: https://en.wikipedia.org/wiki/Open_API (engelsk)

**Hva er åpne data?**
Åpne data er informasjon som er fritt tilgjengelig for bruk og viderebruk av alle, både mennesker og maskiner.
Se https://data.norge.no for en oversikt over åpne datasett i Norge.

**Hva menes med Webhooks?**
Webhooks er bruker-definerte HTTP Callback url'er. Spesielt ved hendelser kan kjerneløsningen gjøre en HTTP forespørsel til den URL som er definert for en webhook, og gjennom denne si ifra om en hendelse. I moderne systemer er dette mye brukt ved overvåkning av løsninger gjennom 3je parts systemer.

For mer utfyllende informasjon se Wikipedia: https://en.wikipedia.org/wiki/Webhook

# 17. Oppsummering av krav/ønsker/behov

Under følger en sammenfattet oversikt over de krav som dette dokumentet beskriver. Spesifikke krav til den enkelte anskaffelse finnes i de enkelte kravspesifikasjoner.

## 17.1. *Krav – Arkitektur*

Se kap. For Arkitekturprinsipper for utdypende forklaring av arkitekturprinsippene.

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | **Helhetlig tilnærming:** Oppdragsgiver ønsker at behov og endringer i systemet må sees i lys av en helhetlig og tverrfaglig utvikling. Beskriv tilbyders strategi rundt utvikling av systemets tjenester sett i ett helhetlig virksomhetsperspektiv. | Bør | | |
| 2 | **Helhetlig tilnærming:** Beskriv tilbyders strategi for å følge nasjonale føringer. | Bør | | |
| 3 | **Prosessorientering:** Oppdragsgiver ønsker at det tas utgangspunkt i fagprosesser ved utforming av IKT-løsninger. Beskriv hvordan tilbyder har designet systemet for å være prosess-støttende. | Bør | | |
| 4 | **Tjenesteorientering:** Oppdragsgiver ønsker at systemet er bygget opp som en samling avgrensede delsystemer som legger til rette for mest mulig gjenbruk. Beskriv hvordan dette løses av tilbyder, og legg ved en skisse som viser systemets oppbygging. | Bør | | |
| 5 | **Tjenesteorientering:** Oppdragsgiver ønsker minst mulig bindinger i systemet. Det optimale er at komponenter/tjenester kan byttes ut, uten at dette går ut over eksisterende | Bør | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | integrasjoner. Beskriv tilbyders strategi rundt dette og hvordan dette eventuelt gjenspeiles i systemet som tilbys. | | | |
| 6 | **Tjenesteorientering:** Oppdragsgiver har ingen bestemt plattform som mellomvare lokalt. Beskriv tilbyders forhold til mellomvare generelt og bruk av mellomvare i tilbudt løsning. | Bør | | |
| 7 | **Interoperabilitet:** Oppdragsgiver ønsker at systemet skal være i stand til å utveksle og dele data og informasjon med andre systemer gjennom standardiserte grensesnitt. Beskriv hvordan tilbyder vil løse dette og hvordan tilbyder vil tilpasse seg eventuelle fremtidige nasjonale standarder. | Bør | | |
| 8 | **Interoperabilitet:** Beskriv tilbyders foretrukne integrasjonsarkitektur. Beskriv hvilke krav og ønsker tilbyder har til andre systemer det skal integreres mot. Beskriv hvordan tilbyder ønsker å motta og levere data. | Bør | | |
| 9 | **Interoperabilitet:** Beskriv hvilken ansvarsfordeling tilbyder har til andre leverandører i forbindelse med integrasjoner. Hvor begynner tilbyders ansvar og hvor slutter det? | Bør | | |
| 10 | **Interoperabilitet:** Beskriv tidligere arbeid med integrasjoner mot andre systemer. Legg ved referanser. | Bør | | |
| 11 | **Interoperabilitet:** Oppgi eventuelle | Bør | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | standardiseringsprosjekter som tilbyder har vært bidragsyter til. | | | |
| 12 | **Tilgjengelighet:**<br>Ved utforming av arbeidsflater ønsker oppdragsgiver at brukergrensesnittet tilfredsstiller gjeldende nasjonale krav til universell utforming.<br>Beskriv hvordan tilbyder innfrir dette. | Bør | | |
| 13 | **Informasjonssikkerhet:**<br>Beskriv hvordan systemet ivaretar krav til konfidensialitet, integritet og tilgjengelighet. | Bør | | |
| 14 | **Brukskvalitet:**<br>Høy brukskvalitet i en IKT-løsning kjennetegnes ved at den er intuitiv, effektiv, har få feil, er feiltolerant, stabil og brukermotiverende.<br>Beskriv hvordan dette er ivaretatt av tilbyder. | Bør | | |
| 15 | **Endringsevne/Fleksibilitet:**<br>Oppdragsgiver ønsker systemer utviklet og lisensiert på en slik måte at det er forberedt på endringer i bruk, innhold, organisering, eierskap og infrastruktur.<br>Beskriv hvordan dette løses av tilbyder. | Bør | | |
| 16 | **Åpenhet:**<br>Oppdragsgiver foretrekker systemer som er basert på åpne eller godkjente standarder.<br>Beskriv hvilke standarder tilbyders system er basert på og eventuelle krav til teknologi hos brukerne. | Bør | | |
| 17 | **Skalerbarhet:**<br>Oppdragsgiver ønsker systemer som er forberedt på endringer i antall brukere, datamengde og livslengden til tjenesten. | Bør | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | Beskriv systemets evne og mulighet for skalering (datamengder, volum, moduler, antall brukere, etc.). Forklar detaljert hvordan en økning/reduksjon blir håndtert. Forklar evt. begrensninger med hensyn til skalering. | | | |

## 17.2. ***Krav - Digitalt økosystem***

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | Oppdragsgiver ønsker løsninger som tilbyr åpne API'er. Beskriv hvordan systemet innfrir dette. | Bør | | |
| 2 | Hvis ja over, beskriv hva tilbyder legger i begrepet et åpent API. | Bør | | |
| 3 | Hvis ja over, beskriv hvordan API'ene er sikret slik at informasjonsflyt kan sikres basert på autentisering og autorisasjon? | Bør | | |
| 4 | Oppdragsgiver ønsker at innhold utveksles på standardiserte formater som XML eller JSON. Beskriv hvilket innholdsformat som brukes ved utveksling av data. | Bør | | |
| 5 | Oppdragsgiver ønsker at løsningen eksponerer hendelsesbasert informasjon slik at andre systemer kan få beskjed om hendelser og gjøre seg nytte av dette i andre digitale prosesser? Det er ønskelig at dette kan gjøres ved å registrere WebHooks i løsningen. (Publish/Subscibe) Beskriv om løsninger har funksjonalitet for dette. | Bør | | |
| 6 | Oppdragsgiver ønsker å kunne utveksle data mellom ulike | Bør | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | løsninger på en sikker måte som f.eks. HTTPS eller SFTP. Beskriv hvordan utveksling av data fra løsningen kan skje kryptert. | | | |

## 17.3. *Krav – Identitets- og tilgangsstyring*

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | Oppdragsgiver ønsker løsninger som lar seg integrere med oppdragsgivers eksisterende løsninger for identitetshåndtering (IDM) for tilordning av tilganger med brukere og roller. Beskriv hvordan løsninger lar seg integrere med en IDM-plattform. | Bør | | |
| 2 | Oppdragsgiver ønsker seg muligheten for import av brukere og brukergrupper via LCS (LifeCycleServer) med for eksempel webservice, DB, XML, API eller lignende. Beskriv hvordan løsningen kan gjøre dette. | Bør | | |
| 3 | Oppdragsgiver ønsker seg løsninger som støtter Single Sign On (SSO) med Active Directory og/eller ADFS som katalogtjenester. For skole- og utdanning kan dette støtte FEIDE eller Google G-suite. Beskriv hvordan systemet støtter SSO. | Bør | | |

## 17.4. *Krav – Infrastruktur*

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | Oppdragsgiver ønsker seg løsninger som kan overvåkes og varsle som kritiske feil i PRTG fra Paessler. | Bør | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | Beskriv om tilbyder kan levere dette. | | | |
| 2 | Dersom over ikke kan leveres, beskriv tilbyders muligheter for å tilby overvåkning av løsningen. | Bør | | |
| 3 | Utskriftsløsninger må ha støtte for Uniflow universelle printerdrivere og følg meg utskrift. | Bør | | |
| 4 | Trådløse løsninger som skal benytte trådløs infrastruktur må støtte 802.11n/ac på 5Ghz og 802.1x autentisering. | Bør | | |
| 5 | Løsningen skal gi tilfredsstillende ytelse og responstid. Beskriv krav til tekniske løsning, som f.eks. krav til kapasitet/båndbredde i LAN/WAN, minne og CPU i servere. | Bør | | |
| 6 | Løsninger installert på oppdragsgiver sine servere, må kunne settes opp med lastbalansering, eventuelt annen form for skalering. Beskriv hvordan dette kan løses. | Bør | | |
| 7 | Løsninger installert på oppdragsgiver sine servere bør støtte Windows 2016 server. | Bør | | |
| 8 | Løsninger installert på oppdragsgiver sine servere bør benytte MS SQL som databaseplattform og støtte MS SQL 2016/MS SQL 2017. Beskriv krav til databaseplattformen. | Bør | | |
| 9 | Beskriv løsningen sine krav til eventuelle sertifikater, sikre kommunikasjonsprotokoller og åpninger i brannmur. | Bør | | |
| 10 | Løsningen bør kunne kjøres på alle klient-typer som PC, VDI, nettbrett og mobiltelefon. | Bør | | |
| 11 | Løsninger installert på oppdragsgiver sine servere, må kunne installeres på virtualiseringsteknologi på serverplattformen. Teknologiene | Bør | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | som skal benyttes er VMware og Horizon VDI. | | | |
| 12 | Der det er behov må løsningen samhandle med Microsoft Office 2016 og/eller G-suite hvis løsningen er for lærere og elever. | Bør | | |

## 17.5. *Krav – Integrasjon med Noark 5 Sak- og arkivsystem eller frittstående Noark 5 kjerne.*

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | Oppdragsgiver krever at tilbydere som integrerer seg mot en Noark 5 kjerne eller ett komplett Noark 5 sak-arkivsystem, primært skal benytte Noark 5 tjenestegrensesnitt for integrasjon. Alternativt og sekundært kan GI standarden for Arkiv benyttes.<br>Beskriv hvordan løsningen integrerer seg mot en Noark5 kjerne og/eller Noark5 sak-arkivsystem. | Må | | |
| 2 | Oppdragsgiver stiller krav om en detaljert oversikt over leverandørens metode og plan for integrasjon mot sak-arkivsystem. Beskriv hvordan dette gjøres. | Må | | |
| 3 | Oppdragsgiver ønsker sammen med tilbyder å lage en oversikt over hvilke data som er relevante og skal overføres mellom fagsystemer og en arkivkjerne, eller en komplett sak- arkivløsning. Beskriv hvordan en slik prosess kan settes opp. | Må | | |

## 17.6. *Krav – Skytjenester (SaaS)*

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | Beskriv hvilke metoder for autentisering og føderering som løsningen støtter. | Bør | | |
| 2 | Oppdragsgiver ønsker at løsningen kan integreres med AD eller ADFS for Single SignOn. For lærere og elever kan Feide og/eller G-suite benyttes for SSO. Beskriv løsningens muligheter for integrering med SSO. | Bør | | |
| 3 | Beskriv hvordan kommunikasjon mellom sky og «on-prem» ivaretas, herunder dataoverføringer og integrasjoner. Legg ved skisse som beskriver kommunikasjon fra kunde til tjenesten. | Må | | |
| 4 | Oppdragsgiver krever at løsninger som leveres som skytjenester, lagrer data innenfor EU/EØS.<br>Beskriv tilbyders strategi for lagring av data hvis løsningen er skybasert. | Må | | |
| 5 | Tilbyder skal som besvarelse av dette punkt kort gjøre rede for hvilke plattform og servere løsningen kjører på, hvor den driftes fra (eventuelle underleverandører som tilbyr hosting (eventuelt housing hvis tilbyder bruker eget hardware, men leier fysisk lokasjon) , hvordan sikkerheten for data blir ivaretatt og hvilke underleverandører tilbyder eventuelt støtter seg på for drifts- og lagrings formål. | | | |
| 6 | Beskriv sikkerheten knyttet til pålogging fra eksterne nettverk, herunder mulighet for 2-faktor autentisering. | Må | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 7 | Løsningen skal gi tilfredsstillende ytelse og responstid. Beskriv krav til tekniske løsning, som f.eks. krav til kapasitet/båndbredde i LAN/WAN, minne og CPU i servere. | Må | | |
| 8 | Tilbyder skal levere alle data fra SAAS løsningen til kommunen når avtalen går ut. Dataene som overleveres skal være komplett og med beskrivelse av tabellverk og relasjoner/sammenhenger. | Må | | |
| 9 | Der kommunen har behov for bruk av dataene i SaaS løsningen til andre formål, f.eks. (BI oppslag, BigData, Backup, konvertering, gjennbruk av data ol. skal det være mulig. Beskriv hvordan dette overholdes. | Må | | |

## 17.7. *Krav – IKT Service og vedlikehold*

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | **Støtte for IT-teknisk personell:** I noen tilfeller er det ikke tilbyder som produserer/utvikler systemene. I de tilfeller hvor tilbyder ikke har egen IT-teknisk kompetanse, ønsker oppdragsgiver at tilbyder gir en beskrivelse av hvordan IT-teknisk støtte skal foregå og hvilke bakenforliggende avtaler som gjelder. Beskriv tilbyders forhold til slik dokumentasjon. | Bør | | |
| 2 | **"På stedet" støtte:** Oppdragsgiver ønsker at tilbyder lager en beskrivelse av betingelsene for "på | Bør | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | stedet" støtte hvor responstid, tidsrom for støtte og kostnader for tjenesten kommer frem.<br>Beskriv tilbyders rutiner for dette. | | | |
| 3 | **Fjernstøtte:**<br>Oppdragsgiver ønsker at tilbyder lager en beskrivelse av betingelsene for fjernstøtte hvor responstid, tidsrom for støtte og kostnader for tjenesten kommer frem.<br>Beskriv tilbyders rutiner for dette. | Bør | | |
| 4 | **Telefonstøtte:** Oppdragsgiver ønsker at tilbyder lager en beskrivelse av betingelsene for telefonstøtte hvor responstid, tidsrom for støtte og kostnader for tjenesten kommer frem.<br>Beskriv tilbyders rutiner for dette. | Bør | | |
| 5 | **Systemoppdatering:**<br>Oppdragsgiver krever at tilbyder har rutiner for å informere om både oppdateringer som retter feil og om ny eller endret funksjonalitet.<br>Beskriv tilbyders rutiner for dette. | Må | | |
| 6 | **Generell IT-støtte fra leverandør:**<br>Oppdragsgiver krever at de personer hos tilbyder som skal drive fjernstøtte eller annen IT-teknisk støtte på kommunens IT-systemer, må skrive under kommunens taushetserklæring.<br>Beskriv tilbyders forhold til dette. | Må | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 7 | **Generell IT-støtte fra leverandør:** Oppdragsgiver krever at alle endringer på systemene skal loggføres. I de tilfeller der tilbyders IT-personell gjør endringer på systemet, skal tilbyders IT-personell også loggføre endringene. Beskriv tilbyders rutiner for dette. | Må | | |

## 17.8. *Krav – Brukskvalitet web og portalløsninger*

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | Oppdragsgiver krever at løsningen oppfyller kravene som er nedsatt i norsk lov for universell utforming av IKT (WCAG 2.0 AA). Beskriv tilbyders strategi for å oppfylle dette kravet. | Må | | |
| 2 | Oppdragsgiver ønsker at løsningen skal oppfylle flest mulig krav i henhold til WCAG 2.0 AAA-standarden. Beskriv hvordan løsningen forholder seg til dette. | Bør | | |
| 3 | Oppdragsgiver krever at i de tilfeller der et grensesnitt skal tilbys kommunens innbyggere som sluttbrukere, skal det være mulig å tilpasse grensesnittet gjennom CSS. Beskriv hvordan løsningen lar seg tilpasse gjennom CSS. | Må | | |
| 4 | Oppdragsgiver krever at i de tilfeller der et grensesnitt skal tilbys kommunens innbyggere som sluttbrukere, skal det være mulig å tilpasse grensesnittet gjennom HTML og JavaScript. Beskriv hvordan løsningen lar seg | Bør | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | tilpasse gjennom HTML og JavaScript. | | | |
| 5 | Oppdragsgiver krever at løsningen skal være testet med sluttbrukere, det være seg om løsningen retter seg mot innbyggere, ansatte, næringsliv eller andre målgrupper. Beskriv tilbyders rutiner for slik testing. | Må | | |

## 17.9. *Krav – Norm for informasjonssikkerhet*

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | Oppdragsgiver krever at løsninger for helse og omsorgstjenesten følger kravene i norm for informasjonssikkerhet (Normen). Se Faktaark 38 - Sikkerhetskrav for systemer fra Direktoratet for e-helse på ehelse.no, leggs ved tilbud ferdig utfylt. | Må | | |

## 17.10. *Krav – Personvern og GDPR*

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| 1 | Oppdragsgiver krever at løsningen følger føringene i den nye personvernforordningen GDPR. Beskriv tilbyders forhold til den nye personvernforordningen og hvordan dens regelverk er implementert i løsningen. | Må | | |
| 2 | Oppdragsgiver krever at håndtering av personopplysninger, både bruken av og lagring, skal være godt dokumentert. Beskriv hvordan løsningens håndtering | Må | | |

| Nr | Krav | Krav type Må/Bør | Oppfylles – Ja/Nei/Delvis | Hvordan |
|---|---|---|---|---|
| | av personvernopplysninger er dokumentert. | | | |
| 3 | Oppdragsgiver ønsker at tilbyder allerede under utvikling av nye løsninger og tjenester tar personvern på høyeste alvor. Beskriv hvilket forhold tilbyder har til «Privacy by Design». | Bør | | |
| 4 | Oppdragsgiver krever at det skrives en databehandleravtale mellom tilbyder og kommunen for å ivareta den nye forordningens ansvarsfordeling mellom databehandler og behandlingsansvarlig. | Må | | |

## 17.11. *Krav – Informasjonssikkerhet og Databehandleravtale*

| Nr | Krav | Oppfylles – Ja/Nei/Ikke relevant | Databehandlers beskrivelse<br>Hvis det refereres til andre dokumenter må referansen være nøyaktig mht dokument, sidenr, avsnitt, URL, etc. |
|---|---|---|---|
| 1 | Har databehandler fordelt ansvar og oppgaver for informasjonssikkerhet dokumentert i et organisasjonskart e.l.? | | |
| 2 | Er sikkerhetsmål for virksomheten fastsatt? | | |
| 3 | Er sikkerhetsstrategi for å nå sikkerhetsmålene utarbeidet? | | |
| 4 | Er ansvarsforhold og sikkerhetsmål gjort kjent for alle i organisasjonen? | | |
| 5 | Er alle medarbeidere informert om sin taushetsplikt og klar over dens innhold og omfang? | | |
| 6 | Er konsekvenser ved brudd på taushetsplikten beskrevet? | | |

| Nr | Krav | Oppfylles – Ja/Nei/Ikke relevant | Databehandlers beskrivelse<br>Hvis det refereres til andre dokumenter må referansen være nøyaktig mht dokument, sidenr, avsnitt, URL, etc. |
|---|---|---|---|
| 7 | Har databehandler et levende styringssystem (ISMS) for informasjons-sikkerhet, basert på god praksis som f.eks. angitt i ISO27001/2? | | |
| 8 | Er det utarbeidet rutiner for gjennomføring av risikovurderinger, inkludert oppfølging av tiltak? | | |
| 9 | Er alle sikkerhetstiltak dokumentert (organisatoriske, fysiske og tekniske)? | | |
| 10 | Gjennomføres det sikkerhetsrevisjon jevnlig og minimum årlig? | | |
| 11 | Hvilke punkter/hva dekker sikkerhetsrevisjonen? | | |
| 12 | Er det etablert prosedyre for oppfølging av resultatet (avvik) av sikkerhetsrevisjoner? | | |
| 13 | Er alle medarbeidere klar over ansvaret de har for å melde avvik? | | |
| 14 | Er det etablert prosedyre som sikrer at Databehandlingsansvarlig varsles umiddelbart ved uautorisert utlevering eller endring av personopplysninger, eller andre sikkerhetsbrudd? | | |
| 15 | Gjennomføres og dokumenteres ledelsens gjennomgang av sikkerheten minimum årlig? | | |
| 16 | Er det iverksatt tiltak for å hindre at teknisk | | |

| Nr | Krav | Oppfylles – Ja/Nei/Ikke relevant | Databehandlers beskrivelse<br>Hvis det refereres til andre dokumenter må referansen være nøyaktig mht dokument, sidenr, avsnitt, URL, etc. |
|---|---|---|---|
| | personell misbruker sin autorisasjon? | | |
| 17 | Er det etablert prosedyrer for fysisk adgang der data behandles/oppbevares? (administrasjon av nøkler/adgangskort i adgangskontrollsystemet) | | |
| 18 | Er det iverksatt tekniske og organisatoriske tiltak for sikker tilgang fra ikke-sikrede lokaler (som f.eks. hjemmekontor, og via mobilt utstyr)? | | |
| 19 | Er det etablert sikkerhetstiltak slik at kun autorisert personell får adgang til driftsutstyr (servere, nettverksutstyr, SAN, backupmedia med mer)? | | |
| 20 | Er det utarbeidet konfigurasjonskart over informasjonssystemene? | | |
| 21 | Er det utarbeidet teknisk beskrivelse av konfigurasjonen? | | |
| 22 | Er kommunens data separert fra andre kunders data? | | |
| 23 | Har løsningen tilstrekkelig kapasitet, uavhengig av den totale lasten leverandør har fra andre kunder | | |
| 24 | Har leverandøren beredskapsplaner for bortfall av løsning? | | |
| 25 | Har databehandler forsvarlige backup- og restore-rutiner som testes regelmessig? | | |

| Nr | Krav | Oppfylles – Ja/Nei/Ikke relevant | Databehandlers beskrivelse<br>Hvis det refereres til andre dokumenter må referansen være nøyaktig mht dokument, sidenr, avsnitt, URL, etc. |
|---|---|---|---|
| 26 | Har leverandøren gjennomført tekniske eller organisatoriske tiltak mot hacking? | | |
| 27 | Gjøres det regelmessig penetrasjonstester for å avdekke svakheter? | | |
| 28 | Har databehandler forsvarlige rutiner for autorisering og autentisering av brukere? | | |
| 29 | Har databehandler tekniske tiltak mot tjenestenektangrep? | | |
| 30 | Har databehandler gode løsninger for logging og sporbarhet? | | |
| 31 | Benytter databehandler egne «dummy» testdata? | | |
| 32 | Krypteres data ved lagring? | | |
| 33 | Krypteres data i transit (kommunikasjon)? | | |
| 34 | Har løsningen mulighet for å gi kommunen tilgang til live overvåkning til kommunens overvåkningsløsning? | | |
| 35 | Har løsningen mulighet for å gi kommunen tilgang til logger, samt fortløpende eksportere loggdata til kommunens SIEM løsning? | | |
| 36 | Ved bruk av IoT devices, har leverandøren et godt regime for bruk av sterke passord, og regelmessig endring av disse? | | |