



Dokumenttype:

[DokumentTypeVisning]

Revideres av:

Aas Per-Arne

Versjon:

[VersjonVisning]

Dokumentansvarlig:

Johansen Ketil

Godkjent dato:

19.09.2019

KRAVSPESIFIKASJON



Standarder for IKT

Fredrikstad kommune Virksomhet Digitalisering Revidert 06.09.2019

1 Innhold

1	Innhold	2
2	Innledning.....	4
2.1	Generelt	4
2.2	Anbud/Leveranse	4
2.3	Innføring av nye IKT-systemer	4
2.4	Organisering	4
2.5	Tiltakshaver	4
3	Systemtekniske krav.....	5
3.1	Generelle krav.....	5
3.1.1	Windows plattform.....	5
3.1.2	Databasestandarder.....	5
3.1.3	Kommunikasjonsprotokoller	5
3.1.4	Utskriftstjenester	5
3.1.5	Epost.....	5
3.1.6	Intranett/Internett.....	6
3.1.7	Distribusjon og Publisering av programvare.....	6
3.1.8	Sikkerhetsarkitektur	6
3.1.9	Nettverksprinsipper	8
3.2	Krav til lokalt installerte programmer/applikasjoner.....	9
3.2.1	Installasjon	9
3.2.2	Oppdateringer og nye versjoner	9
3.2.3	Programvarelås.....	10
3.3	Databaser	10
3.4	Krav til integrasjon med andre systemer	10
3.5	Forhold til eksisterende løsninger.....	10
3.6	Arkivering og deponering.....	11
3.7	Leverandørtilgang.....	11
3.8	Brukeradministrasjon.....	11
3.9	Segmentering av brukergrupper	11
3.10	Krav til brukergrensesnitt	11
4	Krav til skytjenester	12
5	Standard applikasjoner	13
6	Krav til opplæring	14
7	Krav til dokumentasjon	14
7.1	Systemdokumentasjon	14
7.2	Brukerdokumentasjon.....	14
8	Telefonsentraler.....	15
9	Kabling.....	15
9.1	Spesifikasjon for installasjon av strukturert kabling for IKT	15
9.2	Horisontal kabel.....	15
9.3	Fiberkabel	15
9.4	Merking	16
9.5	Testing og Dokumentasjon	17
9.6	Kabelføringsveier	18
9.7	Punktplassering.....	18
9.8	Utvendige framføringsveier.....	18
10	Datarom	18
10.1	Sentrale/større rom.....	18

10.2	Perifere/små rom	18
10.3	Dataskap/rack.....	19

2 Innledning

2.1 Generelt

Fagområdet informasjonsteknologi, kommunikasjon og telefoni forvaltes av virksomhet Digitalisering i Fredrikstad kommune.

Dette innebærer følgende:

Innføring av IKT-baserte systemer skal gjøres i samarbeid med virksomhet Digitalisering i Fredrikstad kommune.

Dette dokumentet er utarbeidet for IT anskaffelser:

- IKT-systemer
- Vesentlige endringer av eksisterende IKT-systemer
- Nybygg, bygningsmessige utvidelser eller større restaureringsarbeider som berører kommunikasjonsområder.

Det vil være slik at enkelte deler av dokumentet er irrelevant for enkelte leveranser (*eksempelvis vil databasestandarder være irrelevant hvis leveransen er fysiske kablingsarbeider*).

2.2 Anbud/Leveranse

Når en leverandør skal besvare et anbud etter en forespørsel fra Fredrikstad kommune er de nedenfor stående krav og spesifikasjoner gjeldende.

2.3 Innføring av nye IKT-systemer

Fredrikstad kommune har rutiner for innføring av nye IKT løsninger som må gjennomgås før installasjonen iverksettes. Herunder også bygningsprosjekter.

Dette er i hovedsak regulert i kommunens IKT-strategi. I hovedsak medfører dette at virksomhet Digitalisering må godkjenne løsningen før den anskaffes.

2.4 Organisering

Ved etablering av IKT-prosjekter skal leverandøren stille med de fagpersonene som skal gjennomføre prosjektet i oppstartfasen og i samarbeid med virksomhet Digitalisering.

2.5 Tiltakshaver

I de fleste IKT-prosjekt finnes en intern tiltakshaver i kommunen. Dette er den som er ansvarlig for den interne prosjektledelsen. Ved innføring/anskaffelse er dette normalt ikke virksomhet Digitalisering.

3 Systemtekniske krav

3.1 Generelle krav

Fredrikstad kommune har selveid infrastruktur med en Microsoft basert hyperkonvergent infrastruktur i eget datasenter og et godt utviklet driftsmiljø som ivaretar dette. Lokalt installerte løsninger i eget datasenter vil således bli foretrukket fremfor skybaserte tjenester såfremt vi ikke finner andre vektige argumenter for å velge en tjeneste i sky. I tilfeller der markedet ikke tilbyr lokal drift kan skytjeneste aksepteres under visse forutsetninger. Dette er beskrevet i kapittel 4. Leveranseform vil være et kvalitetskriterium og vektes i den enkelte konkurranse.

3.1.1 Windows plattform

Det stilles følgende systemtekniske krav og forutsetninger:

- Minimum 32 bits kode. Fortrinnsvis 64 bit for serverapplikasjoner.
- Programvare for sluttbrukere skal være kjørbare på Citrix XenApp 7.15 eller leveres som MSI for «unattended» installasjon fra MS SCCM.
- Servere har Microsoft OS og minimum Windows server 2016
- Tykke klienter er sentralt administrert fra MS SCCM og har som standard installert Windows 10 enterprise 64-bit.
- Programmer som tilbys kommunen skal kunne kjøres på virtuelle servermiljøer basert på Hyper-V.

3.1.2 Databasestandarder

- Oracle database, minimum versjon 12c
- MS-SQL minimum versjon 2016

3.1.3 Kommunikasjonsprotokoller

Det er kun TCP/IP som tillates i det ordinære data-nettverket. De fysiske standardene er beskrevet i kapittel 8.

3.1.4 Utskriftstjenester

Systemet skal benytte kommunens print-servere og nettverksskrivere for all utskrift. Lokalt tilknyttede skrivere tillates ikke til ordinære utskriftsformål. Eventuelle drivere skal leveres 64-bit Windows systemer.

Løsninger skal fungere i en «Follow-me» print / Pull print infrastruktur

Eventuelle avvik for spesielle formål må godkjennes i hvert enkelt tilfelle.

3.1.5 Epost

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

3.1.6 Intranett/Internett

Standard Web-server system:

System	Applikasjon
Operativsystem	Windows server 2016
WEB-server system	MS-IIS 10.0
Intranettplattform	Sharepoint 2016
Internettplattform	EPI-server 10

3.1.7 Distribusjon og Publisering av programvare

Windows basert programvare kan distribueres på to måter.

Fagapplikasjoner med sensitivt innhold skal publiseres fra Citrix XenApp applikasjonssiloer. Brukere med korrekt tilgang vil nå fagapplikasjonene direkte fra applikasjonssilo som en publisert applikasjon.

Andre fagapplikasjoner skal som hovedregel være pakket for utrulling til klient-PC med SCCM. Dette gjelder også påfølgende oppgraderinger/oppdateringer av programvaren.

Web-baserte løsninger skal som hovedregel kunne kjøre i Internet Explorer og skal aksesseres direkte fra tykke klienter. Chrome er tilgjengelig for brukerne som alternativ nettleser for spesielle behov.

3.1.8 Sikkerhetsarkitektur

Nasjonal Sikkerhetsmyndighets «Grunnprinsipper for IKT-sikkerhet» skal etterleves i tillegg til Datatilsynets krav og retningslinjer.

3.1.8.1 Nettverk

Fredrikstad kommunes sikkerhetsarkitektur er basert på følgende prinsipper

- Nettverket er inndelt i mange sikkerhetssoner (DMZ soner, Interne-soner og lukket-sone, brukere, teknisk, gjestenett, byod, med flere)
- Det er klart skille mellom tjenester og klienttyper inndelt i relevant sikkerhetspolicy
- Tilgang til tjenester reguleres gjennom bruk av sikkerhetsbarrierer (brannmur, 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 nødvendigvis tilgang til en sone med lavere sikkerhetsnivå.
- Hver sone inneholder ett eller flere nettverkssegmenter.

- Kommunikasjon med tjenester på internett skal som hovedregel alltid initieres fra interne nett.
- Tjenester på internett som krever aksess til interne tjenester skal termineres i en mellomtjener

Sikkerhetssoner

Sikker-sone, DMZ-1, og DMZ-2 er noen av sonene i vi benytter. Det er definert en rekke soner som skal benyttes avhengig av hvilken type tjeneste det gjelder.

DMZ (Demilitarisert sone)

Det er etablert to DMZ soner, DMZ-1 og DMZ-2:

DMZ-1:

Servere eksponert mot internett, ukjente adresser; men avgrenset på port og tjeneste. Trafikk fra DMZ-1 til internett skal gå mot spesifikke porter eller tjenester.

DMZ-2:

DMZ-2, er en sikrere og mer restriktiv sone, sonen inneholder servere som kun skal kommunisere med kjente adresser på internett. I DMZ-2 åpnes det kun for spesifiserte adresser/adresseområder og porter, eller enheter som har godkjent sertifikat og som kommuniserer på spesifiserte porter. Trafikk fra DMZ-2 til internett skal i utgangspunktet gå mot spesifikke porter, adresser, adresseområder eller tjenester.

Det finnes et eget dokument som beskriver DMZ-sonene i FK, «Brannmur DMZ soner i Fredrikstad Kommune».

FK har følgende tjenester organisert i DMZ:

DMZ-1

- 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
- Skype for business, federering mot eksterne
- Proxy-server

DMZ-2

- Velferdsteknologi
- Skype for Business
- Eksterne nettsider (med restriksjoner for DMZ-2)
- MDA

Sikker-sone

Alle tjenester og systemer som inneholder sensitive personopplysninger ref. personopplysningsloven § 2-8 og alle virksomhetskritiske systemer plasseres i sikker sone. Tilganger er regulert basert på tjeneste og brukerautorisasjon.

3.1.8.2 Nettverkstjenere (Servere)

- Alle servere skal sikkerhetsoppdateres fortløpende
- Virtuelt miljø kjøres på Windows Server 2016 Hyper-V. Løsningen kjører fordelt på to lokasjoner, Hanco (Virksomhet for Digitalisering) og Fredrikstad Rådhus.
- UAC skal være aktivert på server der andre enn administratorer skal kunne logge inn, henholdsvis alle Citrix XenApp servere.
- Lokal brannmur skal være aktivert og korrekt tilpasset aktuell tjeneste!
- Tjenester som ikke er nødvendig for driften eller tjenesten, skal stenges ned.
- Spesielle behov for backup skal dokumenteres. Vi benytter for tiden Veritas Netbackup.
- Skadevare: Windows Defender skal være aktivert på alle servere. Nødvendige unntak skal dokumenteres av leverandør.

3.1.8.3 Klientmaskiner

Operativsystem: siste versjon av MS Windows 10, maks 2 versjoner bakover (ny versjon fra MS ca. hver 6. mnd.) Fortløpende sikkerhetsoppdateringer.

Vi benytter Citrix XenApp for applikasjonslevering, og lokalt installert programvare installert via System Center Configuration Manager. Pakkeformatet MSI prefereres.

Standard nettleser er for tiden Internet Explorer. Chrome er tilgjengelig som alternativ nettleser.

Sikkerhetsmekanismer

- Windows Defender
- Lokal brannmur
- Bruker har ikke lokal administratortilgang
- Bruker kan få midlertidig administratortilgang ved forespørsel
- Standard AD Windows pålogging
- AD Group Policies for tilgangsstyring
- Oppdateringer av operativsystem styres av SCCM, 1 gang pr. mnd.

Standard programvare

- Office 2016
- Acrobat Reader
- Citrix Receiver
- Configuration Manager Agent
- AlwaysOn VPN klient på Mobilt kontor løsning

3.1.9 Nettverksprinsipper

Alle løsninger skal benytte FKs eksisterende nettverk. FK har egen fiberbasert infrastruktur som knytter sammen de fleste kommunale virksomheter. Hver lokasjon har eget lokalnett

med minimum CAT-5e standard spredenett. All aksess og tilknytning til lokalnettet avtales med virksomhet Digitalisering. Bærende protokoll for all kommunikasjon mellom klient/node til serverinstallasjoner skal være TCP/IP. Det skal ikke etableres nye lokale trådløse nettverk. FK's eksisterende løsning for trådløs aksess skal benyttes.

IoT-nettverk

FK har etablert egen infrastruktur for IoT sensorteknologi basert på LoRaWan. Nye IoT-løsninger og sensorteknologi skal fortrinnsvis benytte denne teknologien der radiooverføring av signaler er hensiktsmessig.

Gjeldende nettverksstandarder:

- Ethernet 100/1000BaseT
- Power over Ethernet (802.3af og 802.3at)
- WiFi 802.11 b/g/ac/n
- DHCP reservasjoner for alt permanent tilknyttet utstyr
- LoRaWan IoT nettverk

For all navngiving og adressering finnes det interne standarder som skal benyttes. Tilbyder skal avtale med virksomhet Digitalisering for tildeling av navn og IP adresser til løsningene ved implementering. Navngiving og adressering skal være enkelt å endre i løsningen.

3.2 Krav til lokalt installerte programmer/applikasjoner

3.2.1 Installasjon

Klientprogrammer skal kunne installeres/rulles ut ved hjelp av MS System Center Configuration Manager. De skal leveres på MSI-fil format og kunne settes opp til å installeres "unattended".

3.2.2 Oppdateringer og nye versjoner

Tilsvarende rutine og krav som under pkt. 3.2.1. Enhver ny versjon av et program skal leveres virksomhet Digitalisering for kvalitetssikring før den settes i produksjon. Alle oppgraderinger skal leveres som en komplett installasjon av programvaren.

Tjenester som krever domenerettigheter skal kjøre med en «servicebruker» med nødvendige rettigheter. Virksomhet Digitalisering oppretter disse på forespørsel.

Leverandøren kan få tilgang med egen leverandørkonto. Se eget avsnitt. 3.7

Adresseringer

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

- Filområder applikasjonen benytter skal kunne styres til eksterne lagringsenheter, normalt også andre servere. Det skal benyttes UNC-bane og det skal være støtte for DFS.
- Det skal ikke være krav om at data lagres sammen med den eksekverende delen av programmet.

3.2.3 Programvarelås

Det tillates ikke leveranser av programvare med noen form for fysisk programvarelås, dongler, USB brikker etc. Dersom det er behov for lisenskontroll skal dette være serverbasert.

3.3 Databaser

Det skal ikke være krav om dedikerte databaseservere. Eksisterende server-miljø for MS-SQL og Oracle skal benyttes. Det skal ikke installeres annen programvare på databaseplattformene. Dette skal om nødvendig inn på egne servere spesifikke for aktuell løsning.

Gjenbruk av data i eksisterende databaser skal som hovedregel baseres på integrasjoner mot eksisterende API'er. Duplisering av data skal i størst mulig grad unngås og må ev. begrunnes.

3.4 Krav til integrasjon med andre systemer

Utover de ovenstående reglene for databaserelasjoner gjelder også;

- Eventuelt eksisterende tjenestegrensesnitt skal benyttes ved integrasjoner
- Alle integrasjonslogikk skal ligge i det integrerende systemet.
- Utveksling av data mellom systemet og eksisterende løsninger skal gå automatisk der det er mulig.

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 tilbydereren 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.

3.5 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 systemets brukergrensesnitt.

Tilbyder er ansvarlig for integrering mot eksisterende systemer. Kommunen kan være behjelpelig med å etablere kontakt med aktuelle IT leverandører.

Følgende garantier må gis i tilbudet:

- Dersom løsningen det skal integreres mot tilbyr et ferdig integrasjonslag skal dette benyttes så langt det er mulig.
- 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 gjøre dette etter bestilling fra kommunen.

I motsatt fall, at en annen leverandør trenger opplysninger om det innkjøpte systemet forplikter leverandøren å tilrettelegge slik at en av FK's andre underleverandører for tilgang på nødvendig informasjon. Herunder eksempelvis tilgjengelige API'er databasestrukturer, kildekode etc. Likeledes forplikter FK's leverandører seg til å etablere et gjensidig samarbeid med FK's andre aktuelle leverandører. FK er behjelpelig med å etablere kontakt.

3.6 Arkivering og deponering

Fagsystemer som inneholder arkivverdig dokumentasjon eller materiale skal integreres med kundens eksisterende Noark arkivkjerne. Noark5 tjenestegrensesnitt er foretrukken metode. Det kan også baseres på Geointegrasjon eller Ephorte EIS interne integrasjonslag. Arkiveringen skal fortrinnsvis være løpende og automatisk.

Pasientjournalssystemer skal i påvente av nye forskrifter ikke avlevere data løpende men oppbevares sikkert i fagsystemet. Pasientjournalssystemet skal ha funksjoner for elektronisk deponering av pasientjournaler til et bevaringsverdig elektronisk format. Dette for å sikre bevaring av journaler som ikke lenger er aktive eller sikre bevaring der journalssystemet ikke lenger skal benyttes.

3.7 Leverandørtilgang

Leverandørtilgangen er regulert i kontrakts form, mellom FK og den enkelte leverandør. Leverandører kontakter Virksomhet Digitalisering for å få opprettet en slik samarbeidsform. Avtalen gir leverandør mulighet til fjernoppkobling mot servere relevant for leveransen.

Det er utarbeidet en egen rutine/instruks for denne ordningen som skal følges. Leverandøren vil bli opplyst om dette ved inngåelse av en slik kontrakt.

Systemansvarlige kan få tilgang til skjermdeling via Skype for business. Andre former fjernstyring er ikke tillatt.

3.8 Brukeradministrasjon

Det stilles krav til administrasjon av brukere. Systemet skal støtte SSO med Windows pålogging. Man skal kunne legge til tilgangsnivåer og styre rettighetene til de enkelte brukere internt i systemet.

3.9 Segmentering av brukergrupper

Systemet skal kunne benyttes av flere virksomheter/selskaper. Der det er behov må de kunne operere på forskjellig datagrunnlag. Brukere skal defineres og ha ulike tilgangsrettigheter. Kontroll av brukeridentitet må skje ved pålogging.

3.10 Krav til brukergrensesnitt

Systemet skal benytte grafisk brukergrensesnitt, og følge standard MS-Windows konvensjoner. Systemet skal ha en lettforståelig struktur av skjermbilder og menyer.

Web-baserte publikumstjenester skal følge krav om universal utforming og ha et responsivt design blant annet for å understøtte mobile plattformer.

Web-baserte interne systemer bør på generelt grunnlag også ha et responsivt design.

4 Krav til skytjenester

Fredrikstad kommune har selveid infrastruktur med en Microsoft basert hyperkonvergent infrastruktur i eget datasenter og et godt utviklet driftsmiljø som ivaretar dette. Vi har således ikke behov for eller ønske om infrastruktur eller plattformtjenester dersom ikke dette er konkret etterspurt i konkurransen.

Det er et strategisk viktig valg for Fredrikstad kommune å beholde eierskap til egne data. Våre data skal være fritt tilgjengelig for oss når vi selv ønsker det eller har behov for å integrere eller sammenstille data fra forskjellige fagsystemer. I tilfeller der leverandøren ikke kan garantere dette for sin skytjeneste så skal løsningen installeres i vår private sky og driftes av Fredrikstad kommune.

Programvare som tjeneste kan aksepteres både som allmenn, privat eller hybrid skytjeneste. Følgende er generelle krav gjeldende for alle leveranser. Hvis vi ser det som hensiktsmessig å fravike noen av disse kravene i en konkurranse vil det begrunnes og beskrives i konkurransegrunnlaget.

- Fredrikstad kommune beholder eierskap til våre forretningsdata. Leverandøren kan ikke utnytte disse i andre sammenhenger dersom det ikke er gjort spesiell avtale på dette.
- Utover brukergrensesnitt skal systemet tilby et godt beskrevet og dokumentert og åpent programmeringsgrensesnitt (API) som dekker alle vesentlige kjernefunksjoner. Det skal være basert på åpne standarder for datautveksling (eks. SOAP, REST og WS-*).
- Ved opphør av avtale skal data overføres til Fredrikstad kommune vederlagsfritt på et maskinlesbart format. Dette skal spesifiseres i avtalen.
- Dersom løsningen behandler personopplysninger skal det ved inngåelse av kontrakt også undertegnes en databehandleravtale. Den skal være i tråd med norsk lovverk og utformes i et samarbeid mellom leverandør og oppdragsgiver. Ved eventuell motstrid går databehandleravtalen foran de øvrige avtaledokumentene. Vi benytter for tiden følgende maler fra KINS: <https://kins.no/verktoykasse/maler-for-databehandleravtaler/>.
- Leverandørens vilkår og tjenestenivå vil være gjenstand for evaluering. Her vil fleksibilitet i forhold til kundens ønsker vektlegges. I tilfeller der det ikke behandles personopplysninger og leverandørens vilkår ikke alene er tilstrekkelige skal databehandleravtale allikevel inngås.
- Leverandør må garantere for at tjenesten vil bli holdt oppdatert i forhold til de endringer som skjer i relevant lovverk, ev. krav om rapportering til SSB, KOSTRA osv.
- All datakommunikasjon skal krypteres. Datakommunikasjon over forbindelser med lav tillit skal benytte sterk kryptering
- Sensitive data som mellomlagres på mobile enheter skal være kryptert
- Autentiseringsmekanismen skal være motstandsdyktig mot forsøk på uautorisert tilgang. Kommunens egne ansatte skal kunne benytte ADFS-integrert SingleSignOn. Allmenn skytjeneste skal kunne tilby to-faktor autentisering.
- Tilgang til data skal styres av Fredrikstad kommune og skal kunne gjøres på individ og gruppenivå.
- Dersom tjenesten erstatter en eksisterende løsning skal aktuelle forretningsdata fra dagens fagsystem kunne konverteres til nytt system.
- Tjenester som produserer arkivverdig materiale skal integreres med kommunens arkivkjerne for løpende arkivering.

- Arkivverdig materiale skal ikke lagres i datasenter utenfor Norges grenser
- Regnskapspliktig materiale skal ikke lagres i datasenter utenfor Skandinavia
- Personopplysninger skal ikke lagres på datasentre utenfor EU/EØS.

Eierskap og nærhet til egne data er et viktig prinsipp for Fredrikstad kommune. Tilgang til og muligheter for gjenbruk av egne data er et vesentlig moment. Det samme gjelder fleksibilitet med tanke på vilkår for bruk av tjenesten. Ved evaluering av leveransemodell for tjenesten vil vi derfor vurdere følgende forhold:

- Hybrid sky der data er lagret i vår lokale private sky vil bli vektet som den mest fordelaktige leveranseformen. Forsystemer og brukergrensesnitt kan således driftes i en leverandørstyrt privat eller allmenn sky avhengig av sikkerhetskrav.
- Leverandørkontrollert privat sky, der Fredrikstad kommune har all kontroll på tilgangen til data og tjenester gjennom våre sikkerhetsbarrierer mens leverandøren driver både databaser og tjenester, vil bli vurdert som mindre fordelaktig.
- Allmenn tilgjengelig skytjeneste vil bli vurdert som den minst fordelaktige leveranseformen.

Andre forhold som vil bli evaluert i en konkurranse er:

- Sikkerhetstiltak, sikkerhetsrevisjoner, risikohåndtering, avvik- og varslingshåndtering, personvernkonsekvenser og garantier
- Service nivå og kvalitet på tjenesten
- Rutiner og policy for sikkerhetskopiering av data
- Vedlikeholdsvinduer og varslingsrutiner

5 Standard applikasjoner

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

Type	Produkt
Kontorstøtte	MS-Office 2016 og MS Exchange
Internett Browser	MS-Internett Explorer 11 og Chrome
ERP	Visma Enterprise
Sak/arkiv-system	Evry Ephorte Elements
Dørlås og alarmsystem	Integra
CallCenter	Competella
Telefoni/samhandling	Skype for business

Skal tilbudt system integreres mot andre standardapplikasjoner må tilbyder ta kontakt med Fredrikstad kommune v/Virkksomhet Digitalisering for å få rede på hvilke øvrige applikasjoner som er standard. Tilsvarende gjelder også for spesielle applikasjoner/fagapplikasjoner, der det finnes en liste over godkjente programmer.

6 Krav til opplæring

Spesifiseres nærmere i den enkelte anskaffelse

Leverandøren må kunne gjennomføre opplæring av brukere og/eller av løsningsansvarlige for systemet, når dette kravstilles av kommunen. Endelig omfang av opplæringen avtales nærmere.

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 må kunne stille et forhåndsavtalt antall konsulenttimer til rådighet for kommunen til bruk i opplæringsøyemed.

Det må utarbeides komplett opplæringsmateriell som kommunen kan distribuere til sine brukere.

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

7 Krav til dokumentasjon

Brukerdokumentasjonen skal omfatte alle deler av systemet og skal være på norsk.

Dokumentasjonen skal sikre at systemet brukes på en forsvarlig og korrekt måte.

7.1 Systemdokumentasjon

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

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

Rutiner for avlevering av arkivverdig materiale skal dokumenteres.

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.

7.2 Brukerdokumentasjon

Det skal være system for oppdatering av brukerhåndbøkene. Oppdatering kan skje ved oppdaterte e-læringspakker eller ved overføring av filer m/dokumentasjon.

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

8 Telefonsentraler

Fredrikstad kommune har ip-basert telefoni og samhandlingsplattform. Denne er basert på Microsoft Skype for business og gjelder for alle kommunens virksomheter med unntak av legevakten.

For mer informasjon, kontakt Virksomhet Digitalisering.

9 Kabling

9.1 Spesifikasjon for installasjon av strukturert kabling for IKT

Den europeiske standarden for kabling av bygg EN 50173 og EN 50174 er i alt vesentlig lagt til grunn for spesifikasjonene og skal gjelde for det ferdige produktet.

9.2 Horisontal kabel

Det skal benyttes minimum 4-pars **CAT 6a/Klasse Ea/båndbredde 500 MHz/uskjernet**

Kablene skal være halogenfrie og av brannhemmende materiale.

Maksimal fysisk kabellengde for horisontal kabel skal ikke overstige 90m.

Spredenett skal termineres i RJ45-uttak med 568B-standard på pinne utlegget i kontaktene. Uttak skal være av typen dobbel RJ-45 og frontplate med ramme for innfelling i samme utførelse som for elkraftuttak. Det skal alltid leveres dobbelt uttak, med dobbelt uttak menes 2 nettverksuttak.

Terminering av horisontal kabel i dataskap/rack skal utføres på 19" RJ45-panel med 24 porter. Det skal monteres et horisontalt føringspanel for hvert termineringspanel.

Ved utvidelse av eksisterende anlegg skal det benyttes kabel og koblingsmateriell av samme fabrikat som er benyttet fra før. Systemet skal leveres med en systemgaranti (min. 15-20 års systemgaranti) for etterspurt transmisjonskvalitet og hastighet. Systemgaranti skal leveres Virksomhet Digitalisering før oppstart, og systemleverandør skal oppgis.

9.3 Fiberkabel

All bygnings-/områdestamkabel skal være av typen Singelmode (9/125 µm),

kategori OS2 (G.657), klasse OF-2000, samt konnektorer type SC/UPC. Det skal ikke benyttes mindre fiberkabler enn 24-fiber, med unntak av luftstrekke. Der kan det benyttes 12-fiber. Dette skal avklares med Virksomhet Digitalisering ved hvert enkelt tilfelle.

Fiberkabelen skal termineres i fiberskuffer/hyller i begge ender, inkl. nødvendige adaptere. Fiberkabler skal kveiles opp i fiberskuff før terminering for å sikre at fibreene kan re termineres.

Det skal benyttes kabel som har egenskaper tilpasset bruksområde, installasjonssted og miljø.

Utendørskabel skal generelt termineres mindre enn 2 m fra innføringsstedet der kabelen bryter brannsonen – gulv, tak, vegg. Alternativt kan kabelen bringes lenger inn i bygget forutsatt at den forlegges i brannsikker føringsvei – for eksempel i metallrør.

Single modus fiberkabel skal oppfylle alle krav angitt i NEK EN 50173 med hensyn til optiske, transmisjonsmessige og mekaniske egenskaper.

Fiber kabel og konnektorer må godkjennes av Virksomhet Digitalisering før den bestilles.

Alle fiberkabler skal testes iht. gjeldende standard og det skal leveres komplett dokumentasjon på at dette er utført, samt oppgi type instrument det er brukt,

Komplett levert, montert og testet inkl. fiberskuffer/hyller (dvs. en hylle pr. kabel) med adaptere.

Fiberkabler skal termineres med SC/UPC-konnektor i 19" fiberskuff. Det skal monteres et horisontalt føringspanel for hvert termineringspanel. Ved visse tilfeller kan vegboks benyttes. Dette skal avklares med Virksomhet Digitalisering ved hvert enkelt tilfelle.

9.4 Merking

Datarommene har lokaliseringskode og systemkode:

Eks.

+AH2210=520.002

+AH2258=520.001

Forklaring til merkingen:

+ står for lokalisering

A står for Bygg A

H2 står for Hovedetasje 2

210 og 258 er de ulike romnumrene.

= står for system

520.001 og 520.002 er de to forskjellige systemene/skapene som er plassert i disse rommene.

Komponentene som datauttak og kabler skal starte med 001, 002 osv. dvs. løpende nummerering, og samme løpenummer på uttak og kabel, men forskjellig komponentkode:

Kabel heter f.eks. –KX001 og tilhørende datauttak heter –UD001

Punkt:

IKT punktmerking skal følge samme løpenummer som kabel.

NB! Løpenummer er fortløpende dvs. 303, 304 osv., ikke 101/201, 101A/101B eller 101T/101D osv.



Gir entydig info om:

1. EF plassering (rom)
2. Funksjon / Kabeltype (UD= Uttak Data)
3. Hvilken port

Figur x-x - Eksempel på merking av datauttak

I lokasjoner der det er merket i henhold til Fredrikstad kommunes tidligere merkesystem skal det merkes etter eksisterende merking.

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 1A-1, 1A-2 osv. Eventuelt et neste skap i 1. etasje skal få navnet 1B, punktene 1B-1, 1B-2 osv. Samme måte om det er flere etasjer; F.eks. 2A tilsier at skapet er i 2. etasje, og punktene skal hete 2A-1, 2A-2 osv.

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

Døra til skapet skal ha en klar merking: F.eks. 1A, og om mulig skal også døren til patcherommet merkes.

9.5 Testing og Dokumentasjon

Det skal utarbeides en målerapport som verifiserer at installasjonen tilfredsstiller de krav stilt i funksjonsbeskrivelsen. Testen utføres etter NEK EN 50346:2002 Informasjonsteknologi - Kablingsinstallasjoner - Prøving av installert kabel. Siste versjon av ovennevnte normer, inkludert eventuelle tillegg (amendments), skal legges til grunn for prosjektering, installasjon og testing. Omfatter alle komponenter i kabelnettet. Det vil si kabel, terminering og koblingsmateriell i kommunikasjonsrom, Målerapporten skal i tillegg vise kabelens lengde, samt en verifikasjon på at alle pinner og ledere er riktig terminert. I tillegg skal det oppgis type testinstrumenter som er brukt samt serienummer. Testdokumentasjon skal leveres IT-avdelingen (Fredrikstad kommune) elektronisk på pdf-format

Installatør skal være autorisert som teleinstallatør av Post- og Teletilsynet

9.6 Kabelføringsveier

Virksomhet Digitaliserings kravspesifikasjon og Byggehåndboka skal følges. Ved fremføring over himlinger og lignende skal det 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.

I nybygg og ved rehabiliteringer skal føringsveier etableres med minimum 30 % reservekapasitet.

9.7 Punktplassering

Plassering av innvendige datapunkter skal gjøres i samråd med Virksomhet Digitalisering og aktuell virksomhetsleder for bygget. Tilsvarende gjelder også mengde.

9.8 Utvendige framføringsveier

Ved nybygg eller ved endringer av eksisterende framføringsveier av signalkabler skal Virksomhet Digitalisering kontaktes. Ved spørsmål eller avgjørelser vedrørende eksterne grensesnitt kan Virksomhet Digitalisering kontaktes i hvert enkelt tilfelle.

10 Datarom

Det defineres/finnes to type datarom:

- Sentrale/større rom
- Perifere/små rom

Hvordan hvert enkelt rom defineres avgjøres i samråd med Virksomhet Digitalisering.

10.1 Sentrale/større rom

Design og utførelse av datarom skal foretas i samarbeide med Virksomhet Digitalisering. Det skal legges datagulv med minimum 15 cm effektiv plass for signalkabling.

Videre skal alle sterkstrømskabler 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.

Rommet skal låses av med Fredrikstad kommunes låssystem Integra,

10.2 Perifere/små rom

Minimumskrav på 4 kvadratmeter forbeholdt IT-utstyr.

Grunnet viftestøy bør rommet etableres i god avstand fra faste arbeidsplasser.

Om nødvendig skal kjøling 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.

Rommet skal låses av med Fredrikstad kommunes låssystem Integra,

I noen tilfeller kan låsesylinder med OLH nøkkel benyttes. Dette skal avklares med Virksomhet Digitalisering

10.3 Dataskap/rack

Bredde 800 mm dybde 800 mm høyde 2000 mm 42 høydeenheter.

Rackene skal ha tilstrekkelig med føringsbøyler for både horisontal og vertikal føring

Det skal generelt avsettes reserveplass i rack for 30% utvidelsesmulighet.

Strøm distribueres i rack ved bruk av horisontalt/vertikalt monterte strømskinner.

Detaljplanlegging av samtlige IKT rom utføres i samarbeid med Fredrikstad kommune Virksomhet Digitalisering og forslag til møbleringsplan for utstyr i alle fordelingsrom