



Dokumenttype:
Informasjon

Revideres av:
Aas Per-Arne

Versjon:
3.0

Dokumentansvarlig:
Johansen Ketil

Godkjent dato:
09.01.2020

KRAVSPESIFIKASJON



Standarder for IKT

Fredrikstad kommune Virksomhet Digitalisering

1 Innhold

| | | |
|-------|---|----|
| 1 | Innhold | 2 |
| | Bilag | 3 |
| 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 | Tekniske forutsetninger | 5 |
| 3.1.1 | Windows plattform..... | 5 |
| 3.1.2 | Databasestandarder..... | 5 |
| 3.1.3 | Utskriftstjenester | 5 |
| 3.1.4 | Epost..... | 5 |
| 3.1.5 | Intranett/Internett..... | 6 |
| 3.1.6 | Sikkerhetsarkitektur | 6 |
| 3.1.7 | Nettverksprinsipper | 9 |
| 3.1.8 | IoT-nettverk..... | 9 |
| 3.2 | Krav til lokalt installerte programmer/applikasjoner..... | 9 |
| 3.2.1 | Oppdateringer og nye versjoner | 9 |
| 3.2.2 | Distribusjon og Publisering av programvare..... | 10 |
| 3.2.3 | Konfigurasjon..... | 10 |
| 3.2.4 | Programvarelås..... | 10 |
| 3.2.5 | Brukerautentisering | 10 |
| 3.3 | Databaser | 10 |
| 3.4 | Integrasjoner | 10 |
| 3.5 | Arkivering og deponering..... | 10 |
| 3.6 | Leverandørtilgang..... | 11 |
| 3.7 | Brukeradministrasjon..... | 11 |
| 3.8 | Segmentering av brukergrupper | 11 |
| 3.9 | Krav til brukergrensesnitt | 11 |
| 4 | Krav til skytjenester | 11 |
| 5 | Informasjonssikkerhet og personvern | 12 |
| 5.1 | GDPR..... | 12 |
| 5.2 | Sporbarhet og integritet | 12 |
| 5.3 | Databehandleravtaler for skytjenester | 12 |
| 6 | Standard applikasjoner | 13 |
| 7 | Krav til opplæring | 13 |
| 8 | Krav til dokumentasjon | 13 |
| 8.1 | Systemdokumentasjon | 14 |
| 8.2 | Brukerdokumentasjon..... | 14 |
| 9 | Telefoni | 14 |
| 10 | Kabling..... | 14 |
| 10.1 | Spesifikasjon for installasjon av strukturert kabling for IKT | 14 |
| 10.2 | Horisontal kabel | 14 |
| 10.3 | Fiberkabel | 15 |
| 10.4 | Merking..... | 15 |
| 10.5 | Testing og Dokumentasjon | 16 |

| | | |
|------|----------------------------------|----|
| 10.6 | Kabelføringsveier..... | 17 |
| 10.7 | Punktplassering | 17 |
| 10.8 | Utvendige framføringsveier | 17 |
| 11 | Datarom..... | 17 |
| 11.1 | Sentrale/større rom..... | 17 |
| 11.2 | Perifere/små rom..... | 18 |
| 11.3 | Dataskap/rack..... | 18 |

Bilag

| Bilagsnummer | Navn |
|--------------|---|
| Bilag 1 | Vedlegg til IKT kravspesifikasjon: Minimumskrav med redegjørelse og evalueringskrav |

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 regulert i kommunens Digitaliseringsstrategi. Dette medfører at kommunens digitaliseringsstyre må godkjenne løsningen før den anskaffes.

Det forutsettes at dersom tjenesten erstatter en eksisterende løsning skal aktuelle forretningsdata fra dagens fagsystem konverteres til nytt system hvis virksomheten finner det hensiktsmessig. Dersom aktuelt vil dette bli spesifisert i funksjonell kravspesifikasjon.

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 Tekniske forutsetninger

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 vektet i den enkelte konkurranse. Alle leveranser skal være kompatible med de tekniske forutsetningene i dette kapittel.

3.1.1 Windows plattform

- Minimum 32 bits kode. Fortrinnsvis 64 bit for serverapplikasjoner.
- Servere har Microsoft OS og minimum Windows server 2016
- Programvare skal kunne kjøres på Windows 10 enterprise 64-bit med Office 2016 32-bit.
- Server-programvare 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 Utskriftstjenester

Nettverksbasert utskrift benytter Windows 64-bit print-servere. Drivere skal leveres til 64-bit Windows systemer, og være kompatibel med «Follow-me» print / Pull print infrastruktur

3.1.4 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.

3.1.5 Intranett/Internett

Standard Web-server system:

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

3.1.6 Sikkerhetsarkitektur

Nasjonal Sikkerhetsmyndighets «Grunnprinsipper for IKT-sikkerhet» i tillegg til Datatilsynets krav og retningslinjer ligger til grunn for kommunens IKT-sikkerhetsarbeid.

3.1.6.1 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.
- Hver sone inneholder ett eller flere nettverkssegmenter.
- 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.

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

Fredrikstad kommune 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.

3.1.6.2 *Nettverkstjenere (Servere)*

- Alle servere 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 er aktivert på server der andre enn administratorer skal kunne logge inn, henholdsvis alle Citrix XenApp servere.
- Lokal brannmur er aktivert og korrekt tilpasset aktuell tjeneste.
- Tjenester som ikke er nødvendig for driften eller tjenesten, stenges ned.
- Vi benytter Veritas Netbackup.
- Skadevare: Windows Defender er aktivert på alle servere.

3.1.6.3 *Klientmaskiner administrativt*

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

Sikkerhetsmekanismer

- Windows Defender
- Lokal brannmur
- Bruker har ikke lokal administratortilgang
- Bruker kan få midlertidig administratortilgang ved forespørsel
- Standard AD Windows pålogging
- AD sikkerhetsgrupper 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
- Internet Explorer og Chrome

3.1.6.4 *Klientmaskiner Skole*

Operativsystemer

- MS Windows 10, maks 2 versjoner bakover. Fortløpende sikkerhetsoppdateringer.
- ChromeOS. Fortløpende sikkerhetsoppdateringer.

Sikkerhetsmekanismer Windows

- Windows Defender
- Lokal brannmur
- Bruker har ikke lokal administratortilgang
- Standard AD Windows pålogging

- AD sikkerhetsgrupper for tilgangsstyring

Standard programvare Windows

- Office 2016
- Acrobat Reader
- Configuration Manager Agent
- Internet Explorer og Chrome

Sikkerhetsmekanismer ChromeOS

- Innebygd i operativsystemet

Standard programvare ChromeOS

- Benytter Google Enterprise for Education for distribusjon og tilpasninger.

3.1.7 Nettverksprinsipper

Alle løsninger benytter Fredrikstad kommunes eksisterende nettverk. Fredrikstad kommune har egen fiberbasert infrastruktur som knytter sammen de fleste kommunale virksomheter. Hver lokasjon har eget lokalnett med minimum CAT-5e standard sprednett. 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. Fredrikstad kommunes eksisterende løsning for trådløs aksess skal benyttes.

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 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.

3.1.8 IoT-nettverk

Fredrikstad kommune har etablert egen infrastruktur for IoT sensorteknologi basert på LoRaWan. Som nettverksserver benyttes Lorient. Nettverket dekker store deler av Fredrikstad og Hvaler kommune.

3.2 Krav til lokalt installerte programmer/applikasjoner

3.2.1 Oppdateringer og nye versjoner

Enhver ny versjon av et program skal være tilgjengelig for virksomhet Digitalisering for kvalitetssikring før den settes i produksjon.

3.2.2 Distribusjon og Publisering av programvare

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

3.2.3 Konfigurasjon

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

Filområder applikasjonen benytter skal kunne styres til eksterne lagringsenheter, normalt også andre servere. Det skal benyttes UNC-bane og støtte DFS.

Data skal ikke lagres sammen med den eksekverende delen av programmet.

3.2.4 Programvarelås

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

3.2.5 Brukerautentisering

Programvaren skal støtte SSO mot Active Directory

3.3 Databaser

Eksisterende server-miljø for MS-SQL og Oracle skal benyttes. Det skal ikke installeres annen programvare på databaseplattformene. Annen programvare skal inn på egne servere spesifikke for aktuell løsning.

3.4 Integrasjoner

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

Dersom løsningen det skal integreres mot tilbyr et ferdig integrasjonslag skal dette benyttes.

Leverandøren forplikter seg til å tilrettelegge slik at andre underleverandører får tilgang på nødvendig dokumentasjon på tilgjengelige API'er. Likeledes forplikter leverandøren seg til å samarbeide med andre leverandører i forbindelse med integrasjoner. Fredrikstad kommune er behjelpelig med å etablere kontakt.

3.5 Arkivering og deponering

Fagsystemer som inneholder arkivverdig dokumentasjon eller materiale skal integreres med kundens eksisterende Noark arkivkjerne. Arkiveringen skal 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.

3.6 Leverandørtilgang

Leverandørtilgangen er regulert i kontrakts form, mellom Fredrikstad kommune 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.

3.7 Brukeradministrasjon

Brukere skal kunne ha ulike tilgangsrettigheter, og dette skal defineres internt i systemet.

3.8 Segmentering av brukergupper

Systemet skal teknisk sett kunne benyttes av flere virksomheter/selskaper. Der det er behov må de kunne operere på forskjellig datagrunnlag.

3.9 Krav til brukergrensesnitt

Systemet skal benytte grafisk brukergrensesnitt.

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.

- Fredrikstad kommune beholder eierskap til våre forretningsdata. Leverandøren kan ikke utnytte disse i andre sammenhenger dersom det ikke er gjort spesiell avtale på dette.
- Tilgjengeligheten på egne data gjennom programgrensesnitt er et kvalitetskriterium som blir evaluert.
- Ved opphør av avtale skal data overføres til Fredrikstad kommune vederlagsfritt på et maskinlesbart format. Dette skal spesifiseres av leverandøren i avtalen.

- Dersom skytjenesten behandler personopplysninger skal det før inngåelse av kontrakt undertegnes en databehandleravtale.
- 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 ev. lagres på mobile enheter skal være kryptert.
- Brukertilgang og autorisasjon til systemet skal styres av Fredrikstad kommune og skal kunne gjøres på individ og gruppenivå.
- Tjenester som produserer arkivverdig materiale skal integreres med kommunens arkivkjerne for løpende arkivering.
- Arkivverdig materiale skal ikke lagres i datasenter utenfor Norges grenser, jfr. Arkivloven.
- Regnskapspliktig materiale skal ikke lagres i datasenter utenfor Skandinavia, jfr. Regnskapsloven.
- Personopplysninger skal ikke lagres på datasentre utenfor EU/EØS, jfr. Personopplysningsloven.

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 vårt datasenter 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 eksempelvis med IP-VPN, der Fredrikstad kommune har all kontroll på tilgangen til data og tjenester gjennom våre sikkerhetsbarrierer. Leverandøren vil stå for drift av både databaser og tjenester. Alternativet vil bli vurdert som mindre fordelaktig.
- Allmenn tilgjengelig skytjeneste der leverandør forestår all sikkerhet vil bli vurdert som den minst fordelaktige leveranseformen.

5 Informasjonssikkerhet og personvern

5.1 GDPR

Tilbudt løsning skal etterleve personvernforordningen (GDPR).

5.2 Sporbarhet og integritet

Applikasjoner for arkivverdig dokumentasjon eller personopplysninger 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.

5.3 Databehandleravtaler for skytjenester

Databehandleravtalen 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 Difi:

<https://www.anskaffelser.no/verktoy/kontrakter-og-avtaler/databehandleravtale-utkast>

6 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 |
| Nettleser | MS-Internett Explorer 11 og Chrome |
| ERP | Visma Enterprise |
| Sak/arkiv-system | Evry 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/Virksomhet 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.

7 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. Omfang av opplæringen kravstilles i den enkelte konkurranse.

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.

8 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.

8.1 Systemdokumentasjon

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

Rutiner for avlevering av arkivverdig materiale skal dokumenteres.

8.2 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.

9 Telefoni

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.

Vi har p.t. ingen MDM løsning for mobile plattformer.

Telefonitjenester er på rammeavtale. Leveranser som innbefatter bruk av teletjenester må forholde seg til den enhver tid gjeldende rammeavtalen.

10 Kabling

10.1 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.

10.2 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.

10.3 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 luftstrek. 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.

10.4 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.

10.5 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

koblingsmaterieell 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

10.6 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.

10.7 Punkt plassering

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

10.8 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.

11 Datarom

Det defineres/finnes to type datarom:

- Sentrale/større rom
- Perifere/små rom

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

11.1 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,

11.2 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

11.3 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

Bilag 1: Vedlegg til IKT kravspesifikasjon: Minimumskrav med redegjørelse og evalueringskrav

Informasjon om kravspesifikasjon

Leverandøren skal besvare krav og tildelingskriterier slik hensikten er gitt i konkurransegrunnlaget. Dette betyr at alle krav skal besvares.

Det må klart fremkomme hvor nærmere informasjon i tilknytning til kravet finnes. En generell henvisning til vedlegg godtas ikke. Det skal da være tydelig henvisning til kravnummer.

Kolonnene "Beskrivelse av krav" og "Kravkategori" er utfylt av oppdragsgiver.

Tabellverk med minimumskrav og evalueringskrav er veiledende. Det vil si at krav som ikke er relevant for konkurransen blir fjernet og nye krav kan bli lagt til.

Beskrivelse av kolonnen «E og M/R»:

M = Minimumskrav (obligatorisk krav).

Minimumskrav (obligatorisk krav). Dersom krav med denne klassifiseringen i sin helhet ikke er innfridd i leverandørens svar, kan tilbudet avvises. Kravet vil ikke bli evaluert blant tildelingskriteriene

M/R= Minimumskrav (obligatorisk krav) med krav til redegjørelse. Leverandør skal gi en grundig beskrivelse/redegjørelse for kravet. Leverandør som ikke redegjør for minimumskrav kan avvises. Kravet vil ikke bli evaluert blant tildelingskriteriene.

E = Beskrivelse Bør-krav (evalueringskrav). Krav som det skriftlig skal redegjøres nærmere for, eventuelt med skisser/tegninger eller lignende. Svarene fra leverandør vil bli evaluert under tildelingskriteriene, jf. Konkurransegrunnlaget punkt 5, tildelingskriterier.

Kravene i tabellen nedenfor er basert på de krav som fremkommer i kravspesifikasjon – standarder for IKT.

Generelle minimumskrav med krav til redegjørelse:

| Krav nr. | Beskrivelse av krav | M/R/E | Leverandørs svar |
|----------|--|-------|------------------|
| 1. | Generelt Generelle krav i standard kravspesifikasjon skal være oppfylt. | M | |
| 2. | Løsningsarkitektur Beskriv oppbygning av løsningen. | M/R | |
| 3. | E-post Beskriv løsning for epost integrasjon. | M/R | |
| 4. | Backup/restore Hvordan og hva som må sikkerhetskopieres skal beskrives. | M/R | |
| 5. | Virus/malwareskanning Nødvendige unntak for optimal funksjonalitet skal dokumenteres av leverandør. | M/R | |
| 6. | Systemavhengigheter Beskriv all programvare som systemet er avhengig av for optimal funksjon, inkl. krav til versjoner både på server og klient (f.eks. Java, nettleser, tekstbehandler o.l.), samt eventuelle integrasjoner mot eksterne aktører. | M/R | |
| 7. | Sikkerhet Beskriv hvordan sikkerhet ivaretas ved dataoverføringer og integrasjoner, herunder bruk av f.eks. VPN, kryptering, sertifikater etc. | M/R | |

Tildelingskriterier i form av evalueringskrav:

Systemtekniske evalueringskrav

| Krav nr. | Beskrivelse av krav | M/E/R | Leverandørs svar |
|----------|--|-------|------------------|
| 8. | Utskriftstjenester Lokalt tilknyttede skrivere kan tillates til spesielle utskriftsformål. Avvik for spesielle formål skal beskrives | E | |
| 9. | Programvaredistribusjon Programvare for utrulling bør benytte SCCM for «unattended» installasjon. Dette gjelder også påfølgende oppgraderinger/oppdateringer av programvaren. | E | |
| 10. | Nettleser Web-baserte løsninger bør fungere i Internet Explorer og skal aksesseres direkte fra tykke klienter. Chrome er tilgjengelig for brukerne som alternativ nettleser. Krav til og kompatibilitet med nettlelere skal beskrives. | E | |
| 11. | Nettverkssikkerhet Kommunikasjon mellom tjenester på internett og intranett bør initieres fra interne nett. Beskriv tilbudt løsning. | E | |
| 12. | IoT-løsninger IoT-løsninger og sensorteknologi bør benytte LoRaWAN teknologien der radiooverføring av signaler er hensiktsmessig. | E | |
| 13. | Databaser - Gjenbruk av data Gjenbruk av data i eksisterende databaser bør baseres på integrasjoner mot eksisterende API'er der det er tilgjengelig. Duplisering av data bør unngås og må ev. begrunnes. Beskriv løsning. | E | |

| Krav nr. | Beskrivelse av krav | M/E/R | Leverandørs svar |
|----------|--|-------|------------------|
| 14. | Integrasjoner Utveksling av data mellom systemet og eksisterende løsninger bør baseres på integrasjoner mot eksisterende API'er. | E | |
| 15. | Arkivering og deponering Ved integrasjon for arkivering er Noark5 tjenestegrensesnitt foretrukken metode. Det kan også baseres på Geointegrasjon eller Elements EIS interne integrasjonslag. | E | |
| 16. | Brukeradministrasjon Muligheter for automatisert brukeradministrasjon og tilgangsstyring ved hjelp av AD og/eller et API vil være fordelaktig. | E | |

Krav til programvare eller programvaretjenester

| Krav nr. | Beskrivelse av krav | M/E/R | Leverandørs svar |
|----------|---|-------|------------------|
| 17. | Leveranseform Beskriv tilbudt leveranseform. Henviser til 3.2, ev. 4.0 i IKT Kravspesifikasjon. | E | |
| 18. | Tilgjengelighet på egne data I tilfeller der data bare er lagret i skytjenesten bør 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-*). | E | |

| Krav nr. | Beskrivelse av krav | M/E/R | Leverandørs svar |
|----------|---|-------|------------------|
| 19. | Distribusjonsmetode Beskriv tilbudt løsning. Minst mulig endringer i standard klientkonfigurasjon og brukermiljø vil vektas positivt. Henviser til 3.2 i IKT kravspesifikasjon. | E | |
| 20. | Brukerautentisering Beskriv tilbudt metode. Henviser til 3.2.5 og ev. 4 i IKT kravspesifikasjon. | E | |
| 21. | Krav til brukergrensesnitt Beskriv tilbudt løsning. Henviser til 3.9 i IKT kravspesifikasjon. | E | |

Krav til skytjenester

| Krav nr. | Beskrivelse av krav | M/E/R | Leverandørs svar |
|----------|--|-------|------------------|
| 22. | Leveranseform Beskriv alternative leveranseformer. On-premises, type skytjeneste eller lignende. Redegjør for ev. alternative leveranseformer. | E | |
| 23. | Leverandørens vilkår og tjenestenivå Beskriv vilkår og tjenestenivå. | E | |
| 24. | Sikkerhet og autentisering ved skytjeneste Autentiseringsmekanismen skal være motstandsdyktig mot forsøk på uautorisert tilgang. Kommunens egne ansatte bør benytte Azure AD-integrert SingleSignOn. Beskriv løsningen. | E | |