

Kravspesifikasjon IKT

Krav og standarder for Informasjon-, kommunikasjon- og telefonsystemer i Ringerike kommune.

Dato 6. februar 2018

**Utarbeidet av:
IT-enheten**

Innholdsfortegnelse

1.	Innledning.....	4
2.	Systemtekniske krav.....	5
2.1.	Generelle krav.....	5
2.1.1.	Windows plattform	5
2.1.2.	Databasestandarder	5
2.1.3.	Kommunikasjonsprotokoller	5
2.1.4.	Utskriftstjenester	5
2.1.5.	Elektronisk post.....	5
2.1.6.	Intranett/Internett	6
2.1.7.	Serverstruktur	6
2.1.8.	Publisering av applikasjoner.....	6
2.1.9.	Sikkerhetsarkitektur	6
2.1.10.	DMZ soner	7
2.1.11.	Intern sone.....	7
2.1.12.	Sikker sone.....	8
2.1.13.	Nettverksprinsipper	8
2.2.	Krav til programmer/applikasjoner	8
2.2.1.	Installasjon	8
2.2.2.	Oppdatering -" Nye versjoner"	8
2.2.3.	Adresseringer	8
2.2.4.	Programvarelås	9
2.2.5.	Fjerndrift/-leveranse	9
2.3.	Database regler.....	9
2.3.1.	Data skal kun finnes ett sted	10
2.3.2.	Opprettelse av "sysposter"	10
2.3.3.	Handlinger mot eksisterende systemer	10
2.3.4.	Oppgradering av databaseserver	10
2.4.	Krav til integrasjon med andre systemer	10
2.5.	Forhold til eksisterende løsninger	11
2.6.	Leverandørtilgang.....	11
2.7.	Brukeradministrasjon	11
2.8.	Krav til systemadministrasjon	12
2.9.	Krav til brukergrensesnitt	12
2.10.	Krav til oppgraderinger	12
2.11.	Virtuelle server-miljøer	12
3.	Standard applikasjoner	13
4.	Krav til opplæring	14
5.	Krav til dokumentasjon	15
5.1.	Systemdokumentasjon	15
5.2.	Brukerdokumentasjon	15
6.	Telefonsentraler	16
7.	Kabling.....	17
7.1.	Kabelføringsveier	17
7.2.	Punkt plassering	18
7.3.	Utvendige framføringsveier.....	18

7.4.	Datarom.....	18
7.5.	Sentrale/større rom.....	18
7.6.	Perifere/små rom	19
7.7.	Undervisningsrom	19
7.8.	Møterom.....	19
7.9.	Kommunikasjon	19
8.	Krav til innhold i bygg.....	20
8.1.	Prosess.....	20
8.2.	Hva skal gjøres av IT.....	20
8.3.	Hva gjøres ikke av IT	20
8.4.	Typer bygg	20
8.4.1.	Beboer (Leilighet/hus av privat karakter)	20
8.4.2.	Kontor/ansatte/brukere (Bygninger med arbeidsplasser, institusjonsplasser). 21	
8.4.3.	Velfersteknologi/SD-anlegg/Adgangskontroll.....	21

Dokumenthistorikk

Dato	Versjon	Laget av	Godkjent av	Beskrivelse av endring
01.10.14	0.5	TD		Dokument opprettet
07.01.15	1.0	TD		Gjennomgang i IT-enheten
22.01.15	1.1	TD		Oppdateringer ifht tilbakemeldinger fra IT-enheten og Rådmann.
17.04.15	1.2	TD		Oppdateringer ifht dokument for system
15.10.15	1.3	KES		Skilt ut krav til eksterne (leverandører)
13.03.15	1.4	HS		Lagt til Kravspesifikasjon innhold i bygg

1. Innledning

Fagområdet informasjonsteknologi, kommunikasjon og telefoni forvaltes av IT-enheten i Ringerike kommune.

Dette dokumentet er utarbeidet av IT-enheten for bruk ved:

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

Leverandører som skal innføre IKT-orienterte systemer skal ha godkjenning fra, og arbeide i samråd med IT-enheten.

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

Dokumentet holdes oppdatert av IT-enheten og er tilgjengelig på intranett under IT-enheten.

2. Systemtekniske krav

2.1. Generelle krav

2.1.1. Windows plattform

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 6.0 og nyere, Citrix ver. 4.5 (Windows 2003 R2 server) og Citrix versjon 6.5 (Windows 2008 R2 server).
- Horizon applikasjonsteknologi er Windows 7 64bit Enterprise med vdi persona management (roaming profiles).
- Servere kjører Windows 2012, 2012 R2, 2008, 2008R2 og Windows 2003R2 (Standard og Datacenter Edition) 64bit.
- Tykke klienter kjører Windows 7 Enterprise 64-bit eller nyere.
- Programmer som tilbys kommunen skal kunne kjøres i et virtuelt servermiljø. Kommunen benytter i dag VMware som plattform.
- Flerbrukersystem – i praksis ingen begrensning på antall samtidige brukere
- Det er fordel om systemet er web-basert (plattform spesifisert nedenfor).

2.1.2. Databasestandarder

- Oracle database, ver 11g
- MS-SQL 2008R2

MS-SQL prefereres.

2.1.3. Kommunikasjonsprotokoller

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

2.1.4. 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.

2.1.5. Elektronisk post

Standard system for elektronisk post er MS-Outlook 2010/2013 på klientsiden og MS-Exchange 2010 på serversiden. Utover Outlook tillates det kun SMTP og IMAP i kommunikasjon mot Exchange som må avtales spesielt i hvert enkelt tilfelle.

2.1.6. Intranett/Internett

Standard Web-server system:

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

*Et produkt levert av Sem & Stenersen og EPI Norge.

2.1.7. 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/>.

2.1.8. Publisering av applikasjoner

Applikasjoner distribueres og pakkes, til tykke klienter med SCCM 2012 og til tynnklienter via VMware Horizon og/eller Citrix. Alle nye applikasjoner må støtte alle disse måtene å distribueres på.

2.1.9. Sikkerhetsarkitektur

Sikkerhetsarkitektur er basert på følgende prinsipper

- Nettverket er delt i fire soner (DMZ, Intern, intern DMZ og sikker).
- 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

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:

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

2.1.10. 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 passerer. Ytterligere informasjon får man ved beskrivelse av hva som ønskes i en egen henvendelse til IT-enheten.

Følgende tjenester er organisert i DMZ:

- 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

2.1.11. 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.

2.1.12. Sikker sone

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

2.1.13. 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 spredt nett. All aksess og tilknytning til lokalnettet avtales med IT-enheten. Bærende protokoll for all kommunikasjon mellom klient/node til serverinstallasjoner skal være TCP/IP.

- Ethernet 10/100/1000BaseT
- Power over Ethernet (802.3af og 802.3at)
- WiFi 802.11 b/g/a/n 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.

2.2. Krav til programmer/applikasjoner

2.2.1. Installasjon

Alle programmer som skal installeres skal leveres på MSI-fil format. Alternativt kunne settes opp til å installeres "unattended". Når en ny applikasjon installeres skal denne først installeres på en testserver og testes under det rette miljøet simulert. 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).

2.2.2. Oppdatering -" Nye versjoner"

Tilsvarende rutine og krav som under pkt. 3.2.1. Enhver ny versjon av et program skal leveres IT-enheten og testes i det simulerte miljøet (testmiljø) før den settes i produksjon. Alle oppgraderinger skal leveres som en komplett installasjon av programvaren.

2.2.3. 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 disk, normalt også andre servere.
- At databaser legges på egne servere.

- 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.

2.2.4. 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.

2.2.5. Fjerndrift/-leveranse

Alle dataprogrammer som krever installasjon og kommunikasjon i kommunens nettverk skal som hovedregel kjøres på server lokalisert ved kommunens datasentral. Alle programmer, tjenester og annet som installeres i kommunens datasentral/nettverk skal avklares og avtales med IT-enheten. Datasentral er tilknyttet internett og fungerer som skyløsning (Private Cloud), så alle installerte systemer i kommunens datasentral kan tilgjengelig gjøres i skyen.

IT-enheten har til vanlig ikke kapasitet til å påta seg ansvaret for drift av IAAS løsninger som ligger hos andre leverandører, der dette kreves må det godkjennes spesielt og økonomiske konsekvenser for drift gjennomføres.

Der det er gunstig er det ønskelig med SAAS (Software As A Service), som driftes av leverandøren. Ved SAAS løsning er det leverandøren som har ansvar for drift og oppgraderinger, integrasjoner mm. av løsningen, ønskes det at IT-enheten skal ta deler av ansvaret må dette beskrives og avtales særskilt. Det skal gjøres rede for hvor løsningen driftes fra, hvordan sikkerheten for data blir ivarettatt og hvilke underleverandører tilbyr eventuelt støtter seg på for drifts- og lagringsformål.

Systemeier/bestiller har ansvar for avtaler og at det foretas en risiko- og sårbarhetsanalyse (GDPR). Løsninger som baserer seg på data som overføres/integreres med eksisterende datasett i kommunens datasentral, skal beskrives detaljert. Systemeier/bestiller har ansvar for å involvere eier av dataene som overføres/integreres i avgjørelsesprosessen.

Det kreves at data fra SAAS løsninger skal overleveres kommunen på forespørsel, ved kontrakts endring som krever dette eller fratredelse av avtale. Dataene som overleveres skal være komplett og med beskrivelse av tabellverk og relasjoner/sammenhenger.

I alle nevnte tilfeller skal tilbyder gjøre rede for hvilke plattform og servere løsningen kjører på.

2.3. 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, triggerer eller annen kontakt med eksisterende databaser gjelder alle hovedreglene herunder.

2.3.1. Data skal kun finnes ett sted

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 ekte View (ev. snapshot) mot de eksisterende tabellene. Det tillates ikke at tabeller kopieres over til systemet.

2.3.2. 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.

2.3.3. Handlinger mot eksisterende systemer

All programkode (Triggerer, 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.

2.3.4. 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. Leverandøren vil bli kontaktet i hvert enkelt tilfelle.

2.4. 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 tilbydereren beskrive hvorledes rutine 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.

2.5. 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. IKT er behjelpelig med å etablere kontakt.

2.6. 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.

2.7. Brukeradministrasjon

Det stilles krav til administrasjon av brukere. Systemet skal støtte SSO (Single Sign-On) mot AD. Man skal kunne legge til tilgangsnivåer og styre rettighetene til de enkelte brukere av systemet internt i systemet.

2.8. 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.

2.9. Krav til brukergrensesnitt

Systemet skal være brukervennlig og Windows-basert. Systemet skal benytte grafisk brukergrensesnitt, og følge standard MS-Windows konvensjoner. 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.

2.10. 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.

2.11. Virtuelle server-miljøer

IT-enheten benytter VMware for å kjøre virtuelle servermiljøer. Standarder i dag er VMware med Vcenter 5.5. På hostene er ESXi 5.5 installert. Dette kjøres over flere fysiske maskiner i HA-cluster.

3. Standard applikasjoner

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

Type	Produkt
Kontorstøtte	Microsoft Office 2013, 32bit
Internett «Browser»	Internett Explorer 11, 64 bit
Bildebehandling	MS-Paint og Paint.Net
Verktøy	Til enhver tid siste versjon av Java, Adobe produkter, Silverlight, Flash og .Net
Dørlåssystem/adgangskontroll	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.

4. Krav til opplæring

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

Opplæringen må tilpasses de enkelte brukeres behov, og derfor deles opp i minimum to grupper:

- 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 konsulents 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.

Krav om opplæring må tas med i kontrakt og utlysning.

5. 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.

5.1. Systemdokumentasjon

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

Systemdokumentasjon, oppsettparametere, -regler, maskinelle kontroller og tilgangsrettigheter 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.

5.2. 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.

6. Telefonsentraler

Ringerike kommune er i en overgangsprosess til IP-telefoni/Lync. Nye plattformer er basert på Microsoft Lync 2013. Nye virksomheter skal derfor ikke ha ordinær telefonsentral.

Alle tiltak, ønsker og tanker om telefoniløsninger og -sentraler skal IT-enheten involveres i før beslutninger tas.

7. Kabling

Denne instruksjonen gjelder for all kabling i Ringerike kommune.

IT-enheten leverer selv alt nettverksutstyr og overvåking av dette, skal leverandør levere dette må dette avtales med IT-enheten og leverandør står ansvarlig for daglig drift av utstyret.

Termineringspanel	Kabler	Kontakter
<p>Generelt I alle termineringspunkter skal det benyttes RJ45.</p> <p>Utstyret skal være tilpasset 19" profiler</p> <p>Alt utstyr skal være i Category 6 (Class E/Ea)</p>	<p>Kabler til arbeidsplass Det skal benyttes category 6 kabler hele veien også dersom man skal tilfredsstillte spesielle branntekniske krav.</p>	<p>Datanett og telefoni Alle kontakter skal være av type RJ45 med 568Bstandard på pinneutlegget i kontaktene.</p> <p>Alle par skal termineres selv om punktet er beregnet for telefoni.</p>
<p>Fiber 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.</p>	<p>Fiber Alle fiberkabler, både utvendig og innvendig skal være singelmodus.</p>	<p>Fiber Det skal leveres med patchekabel SC-SC i passende lengde for tilkobling av switch.</p>
<p>Merking All merking skal følge merkesystemet Strukturert kabling.</p>	<p>Merking All merking skal følge merkesystemet Strukturert kabling.</p>	<p>Merking All merking skal følge merkesystemet Strukturert kabling.</p>

Alle kablingsarbeider skal utføres av sertifiserte installatører.

- Hvis det finnes eksisterende Category 5e kabling, kan denne typen benyttes etter avtale med IT-enheten i Ringerike kommune. Dette gjelder også ved uforutsette problemer som plassmangel o.l.
- 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 kan denne lengden være 100 meter.
- Der det benyttes flere, dataskap skal det kables 2 stk. category 6 forbindelser mellom disse. Eventuelt 2 stk. singlemodus fiber.

7.1. Kabelføringsveier

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.

7.2. Punkt plassering

Plassering av innvendige datapunkter skal gjøres i samråd med IT-enheten og aktuell virksomhetsleder for bygget. Tilsvarende gjelder også mengde.

7.3. Utvendige framføringsveier

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

7.4. Datarom

Det defineres/finnes 2 typer datarom:

- Sentrale/større rom
- Perifere/små rom

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

7.5. 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. Rack (skap) skal være 19 tommer, med en minimums dybde på 55 cm fra monteringskinnene i forkant til monteringskinnene i bakkant av skapet.

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

Av sikkerhetsmessige årsaker er det slik at alle servere skal plasseres i kommunens Datacenter, ikke på datarom rundt i kommunen. Er det spørsmål eller usikkerhet rundt definisjon av dette, kontakt IT-enheten.

7.6. Perifere/små rom

Minimumskrav på 4 kvadratmeter forbeholdt IT-utstyr. Rack (skap) skal være 19 tommer, med en minimums dybde på 55 cm fra monteringskinnene i forkant til monteringskinnene 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.

Av sikkerhetsmessige årsaker er det slik at alle servere skal plasseres i kommunens Datacenter, ikke på datarom rund i kommunen. Er det spørsmål eller usikkerhet rundt definisjon av dette, kontakt IT-enheten.

7.7. 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.

7.8. 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.

7.9. Kommunikasjon

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

8. Krav til innhold i bygg

Kravspesifikasjon fra IT ifbm nybygg og rehabiliteringer i kommunal regi og regi av eiendomsservice.

8.1. Prosess

- Bestiller beskriver hvem som skal bruke bygget og hvordan.
- Bestiller avgjør hvilke type nettløsning som skal bestilles til bygget, se typer nedenfor.
- IT må involveres der ansatte skal ha faste arbeidsplasser (nivå 2 og 3) + Velfersteknologi/SD-anlegg/Adgangskontroll:
 - IT skal tidligst mulig gjøre en vurdering av kommunikasjonsmuligheter
 - IT skal involveres før prosjektet legges på anbud
 - IT skal involveres hvis telefoniløsninger utover mobiltelefoni vurderes
 - IT skal delta i første møte med elektriker for svakstrøm i byggeprosjekt/rehabiliteringsprosess
 - IT blir med å går ferdigbefaring og skal få overlevert kopi av all dokumentasjon for svakstrøm

8.2. Hva skal gjøres av IT

- Stille krav til kabling, alt fra kvalitet på kabel til hvor de termineres
- Bestille og montere nettverksutstyr, brannmur, switcher og trådløse sendere
- Sjekke at utførelse er jfr. bestilling i møte med elektriker
- Bestille inngående samband/kommunikasjon ved nivå 2 og 3 installasjoner
- Sette opp tilgang til Datacenter/serverrom der det er lagt til rette for standardløsninger innen SD-anlegg, adgangskontroll og velferdsteknologi

8.3. Hva gjøres ikke av IT

- Betaler fakturaer for prosjektet
- Testing av kabling/anlegg
- Brannsikkerhet
- Prosjektledelse
- Oppfølging av underleverandører

8.4. Typer bygg

8.4.1. Beboer (Leilighet/hus av privat karakter)

- Etablere et felles koblingsskap for svakstrøm der flere enheter er samlokalisert
- Etablere trekkerør fra koblingsskap til kum/gate diameter min. 50mm
- Dobbelpunkt til TV fra koblingsskap
- Dobbelpunkt til trådløst nettverk hver boenhet
- Alle kostnader for kabling, utstyr ol. dekkes av den enkelte enhet eventuelt byggeprosjektmidler
- Ansatte som trenger tilgang til kommunalt nettverk, kjører hjemmekontor via beboer sitt nettverk eller 3G/4G

- Kommunikasjon etableres til koblingsskap og kostnader belastes beboer eller den enkelte enhet
- Der det kreves flere trådløse rutere, kontakt bredbåndleverandør eller eventuelt gjør avtale med elektriker

8.4.2. Kontor/ansatte/brukere (Bygninger med arbeidsplasser, institusjonsplasser)

- 1 nivå: Midlertidige/leide/periodiske brukte lokaler. Ansatte får tilgang til Ringerike kommunes nettverk via ekstern nettverk eller 3G/4G.
- 2 nivå: Permanent arbeidsplasser. Ansatte får tilgang til Ringerike kommunes nettverk via Trådløs dekning, som driftes av IT-enheten.
- 3 nivå: Det etableres kablet og eventuelt trådløst nettverk for ansatte. Må etableres låsbare svakstrømrom som overholder sikkerhetskrav.

8.4.3. Velfersteknologi/SD-anlegg/Adgangskontroll

- Der det planlegges slik teknologi må det planlegges en prosess med IT-enheten