Kristiansund kommune
I medvind uansett vær

x

IKT Arkitektur og standarder

Kristiansund kommune

IKT enheten

V1.2 - Sist revidert 29.3.2019

Standarder for IKT, Kristiansund kommune

Innholdsfortegnelse:

1 Innledning

Fagområdene informasjonsteknologi og utstyr, kommunikasjon og samhandling samt applikasjon og brukergrensesnitt forvaltes av IKT-enheten i Kristiansund kommune.

Leverandører som skal innføre nye eller oppgradere systemer og løsninger som inngår i eller støttes av kommunens IKT-systemer skal samarbeide med Kristiansund kommunes IKT-enhet.

Dette dokumentet er utarbeidet for bruk ved

- Anskaffelser av nye IKT-systemer og løsninger
- Vesentlige endringer og oppgradering av eksisterende IKT-systemer og løsninger
- Nybygg, bygningsmessige utvidelser eller større restaureringsarbeider hvor IKT-systemer og IKT–infrastruktur berøres.

Enkelte deler av denne kravspesifikasjonen vil være irrelevant for noen leveranser.

1.1 Anbud og leveranse

For leverandører som besvarer anbud etter forespørsel fra Kristiansund kommune er kravene i dette dokumentet å regne som A-krav (Må-krav) med mindre annet er angitt.

1.2 Avtaletekst

Statens standardavtaler skal benyttes ved alle IT-leveranser til Kristiansund kommune. Ønsket avtaletekst oppgis i konkurransegrunnlag.

Mest brukt er:

- **Avtale om løpende tjenestekjøp (SSA-L)** ved kjøp av standardiserte skytjenester ("As-A-Service" leveranse)

  https://www.anskaffelser.no/verktoy/kontrakter-og-avtaler/avtale-om-lopende-tjenestekjop-ssa-l

- **Kjøpsavtalen (SSA-K)** ved kjøp av it-utstyr og/eller programvare

  https://www.anskaffelser.no/verktoy/kontrakter-og-avtaler/kjopsavtalen-ssa-k

- **Utviklings og tilpasningsavtalen (SSA-T)** Ved utvikling eller tilpasses kommunes behov.
  https://www.anskaffelser.no/verktoy/kontrakter-og-avtaler/utviklings-og-tilpasningsavtalen-ssa-t

1.3 Innføring av nye IKT-systemer

Kristiansund kommune har rutiner for innføring av nye IKT-løsninger, disse skal følges og gjennomgås før installasjonen iverksettes. Alle nye tjenester skal inn i kommunens IT tjenestekatalog, med systemeier og dokumentasjon.

Kommunesamarbeid

Kristiansund kommune er medlem i et kommunesamarbeid på Nordmøre, IKT Orkidé. Samarbeidet er organisert etter kommunelovens §27 og jobber for samordning, standardisering og IKT-støttet faglig utvikling for kommunenes tjenester.

Link: https://www.iktorkide.no/

2 Krav til leveranser av programvareløsninger

2.1 Generelle krav

2.1.1 Klientutstyr

Kristiansund kommunes klientmaskiner har frem til 2017 vært basert på Windows 7 med unntak av noen tynnklienter.

Fra 2017 er det vedtatt å tilby alle tjenester som en webtjeneste eller via Citrix med utstyr som velges av brukeren selv. Framtidige programmer må derfor kunne benyttes via Web eller installert i kommunens Citrix løsning. "Bring Your Own Device" (BYOD) tanken må derfor støttes. Kommunale PC'er vil derfor ikke være medlem i Active Directory.

Webtjenester hvor personopplysninger behandles skal beskyttes med multifaktor autentisering. Kristiansund kommune benytter fra før felleskomponenten «ID Porten» og Microsofts MFA-løsning. Dersom sensitive opplysninger behandles, skal sikkerhetsnivå 4 benyttes.

Høyeste sikkerhetsnivå (nivå 4)

BankID, BankID på mobil, Buypass og Commfides leverer elektronisk ID på høyeste sikkerhetsnivå. Dette er som MinID en to-faktorløsning, i tillegg blir e-ID-en utlevert ved personlig oppmøte og legitimering, for å unngå at kodegeneratoren til BankID, smartkortet til Buypass eller USB-pinnen til Commfides havner i feil hender.

2.1.2 Server

Når nye IT-tjenester opprettes skal eventuelle servere opprettes i kommunens valgte plattform, Microsoft Azure, sammen med nødvendige nettverks, lagrings og funksjonstjenester.

2.1.3 Database

Alle databaseløsninger skal støtte Microsoft Azure.

2.1.4 Utskriftstjenester

Kommunen benytter seg av en skyløsning for utskrift og systemer skal benytte dette for all utskrift.

2.1.5 E-Post

Standard kontorstøtteprogramvare er Microsoft Office 365.

2.1.6 Serverstruktur

Kristiansunds IKT-tjenester leveres via Microsoft Azure og kommunale fellesløsninger i fra servere hos IKT Orkidé.

2.1.7 Publisering av applikasjoner

Kristiansund kommune benytter Citrix som terminalserverplattform.

Applikasjoner som ikke er rene webgrensesnitt skal kjøres på terminalserver og være publisert som enkeltapplikasjon. Brukere har ikke tilgang til selve Windows-skrivebordet på terminalserveren og fagapplikasjon skal ikke installeres lokalt på pc.

2.2 Kildesystemer og integrasjoner

Våre IT-løsninger skal samhandle for å unngå unødvendig dobbeltføring av identitetsinformasjon og vedlikehold. Det er et krav for alle nye IT-systemer at det tilrettelegges for identitetshåndtering med kommunens IDM-løsning for oppretting av brukerkonto og tildeling av roller i systemet. Se 2.2.3.

Følgende viktige kildesystemer finnes

2.2.1 Personal og økonomistyring

Kommunen benytter et fagsystem for personal og økonomistyring. HRM-modulen i dette systemet er integrert med Active Directory gjennom IDM.

HRM (Human Resource Management)

Fagsystemer som krever personopplysninger om kommunens ansatte (Brukerinfo) skal hente informasjonen fra personalsystemet eller i fra Microsoft AzureAD.

Kommunen benytter for tiden Visma Enterprise for personal og økonomistyring.

2.2.2 Katalogtjeneste - Active Directory

Azure Active Directory i fra Microsoft Azure benyttes for autentisering. Tjenester som leveres fra kommunens Azure løsning eller som en levert tjeneste fra leverandør må støtte ADFS eller direkte mot Microsoft AzureAD på til enhver tid gjeldende protokoll. (For tiden oAuth2). Alle nye løsninger skal derfor autentisere med allerede eksisterende brukerkonto. Det skal ikke opprettes særskilte brukernavn og passord for ansatte og elever.

2.2.3 Identity management (IDM)

Kommunen benytter LifeCycle Services (LCS) levert som en tjeneste fra IKT Orkidé for automatisk forvaltning av identitetsinformasjon i forskjellige løsninger basert på kommunens personalsystem.

LCS håndterer oppretting, endring og sletting av brukerkontoer, rollestyring og tilgangskontroll i alle nye løsninger. Dette gjøres gjennom API-kall, script eller i unntakstilfeller med oversending av forespørsler i kommunens helpdesksystem.

2.2.4 Integrasjonsplattform

Kommunen benytter systemet Microsoft Azure Logic Apps som integrasjonsplattform for transaksjoner og oppslag mellom løsninger som ikke omhandler identitet.

2.3 eLæring

Ved anskaffelse av nye tjenester som benyttes av mer enn 15 personer skal tilbyder utarbeide eLæring for grunnleggende bruk av systemet, dette skal være myntet på førstegangsbrukere og holdes fortløpende oppgradert ved endringer.

Kommunen kan be om eLæring for flere grupper i konkurransegrunnlag ved en anskaffelse.

Kommunens plattform for eLæring er KS Læring.

2.4 Organisering

Ved etablering av et prosjekt skal prosjektets eier eller leder starte et samarbeid med IKT-enheten. Ved oppstartsmøte skal ansvarlig fra leverandøren stille med de fagpersonene som skal gjennomføre prosjektet.

Ved prosjektarbeid forventes det at prosjektmandatet inneholder informasjon om budsjett, ressursbehov, milepælplan og mål for prosjektet.

IKT-enheten stiller relevante ressurser på slike møter.

2.5 Personvern

Kristiansund kommunes krav til personvern skal ivaretas ved leveranse av nye IT-løsninger. Spesielt betyr dette:

- behandling av personopplysninger må være lovlig. Leverandør har godt grunnlag for å bistå Kristiansund kommune med å dokumentere rettslig grunnlag for behandling av personopplysninger.
- Dersom løsningen fungerer etter formålet uten identifiserbare opplysninger, skal det ikke innhentes identifiserende opplysninger.
- Programvaren skal sørge for å ivareta den registrertes rettigheter og friheter etter personvernregelverket.
- Behandlingen av personopplysninger skal være gjennomsiktig.
    - Tilbudt løsning skal ha funksjonalitet for å gi informasjon om hvilke opplysninger som behandles og hva de brukes til, samt mulighet for de registrerte til å gjøre seg kjent med sine rettigheter og hvordan de skal utøve disse.
- Personopplysninger skal kun lagres så lenge det er nødvendig. Tilbudt løsning skal inneholde funksjonalitet for automatisk sletting eller periodisk gjennomgang for å sikre at personopplysninger ikke oppbevares lengre enn nødvendig.
- Integritet og fortrolighet
    - Løsningen skal ha tiltak mot uautorisert utlevering og tilgang til personopplysninger.
    - Løsningen skal ha tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger.
    - Løsningen skal som standard sørge for at personopplysninger er tilgjengelige for autoriserte personer når det er nødvendig.
    - Løsningen skal som standard sikre at personopplysninger ikke gjøres tilgjengelig for et ubegrenset antall mennesker uten den berørte personens medvirkning.

    - Løsningen skal ha tiltak for å spore endringer som gjøres i systemet og for å kunne håndtere sikkerhetsbrudd
    - Løsningen skal ha tiltak for å sikre at systemene som behandler personopplysninger, er robuste mot for eksempel sårbarheter, angrep, og uhell.
- Når personopplysningene innhentes fra andre enn den registrerte skal det foreligge funksjonalitet som sørger for at den registrerte informeres om
    - hvilke kategorier av personopplysninger som behandles
    - fra hvilken kilde personopplysningene stammer fra

2.6 Standard formater og universell utforming

Brukergrensesnitt og rapporter fra systemer skal tilfredsstille krav til universell utforming. Alle nettløsninger skal derfor være universelt utformet etter standarden WCAG 2.0.

https://www.techweb.no/blogg/hva-er-universell-utforming

Rapporter skal kunne eksporteres i format som tilfredsstiller krav i "Forskrift om IT-standarder i offentlig sektor".

https://lovdata.no/dokument/LTI/forskrift/2013-03-15-285

Kommunen benytter Microsoft Office 365 og OOXML-formatterte dokumenter for redigering.

https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/referansekatalogen/publisering-av-tekstdokumenter

2.7 Åpne data

Kommunen praktiserer meroffentlighet og sikter mot å presentere alle åpent tilgjengelige nøkkeldata i standardisert form. Dette skal helst gå automatisert rett fra fagsystem.

Rapporter skal kunne tas ut formattert som datasett etter offentlig standard for datasett, DCAT-AP-NO-1.1

https://doc.difi.no/dcat-ap-no/

Kommunen forvalter rapportene og vil i utgangspunktet legge ut data som ikke er unntatt offentlighet. Det er Norsk Lisens for Offentlige Data (NLOD) som benyttes.

https://data.norge.no/nlod/no

3 Opplæring

KS Læring er en læringsplattform spesialtilpasset norske kommuner. Alle norske kommuner har tilgang og tilbys eget område på løsningen i tillegg til at en kan benytte felles kurs som andre har laget. Løsningen dekker både elæring og påmelding til

klasseromskurs. All kursfullføring logges slik at kommunenes ledere får full oversikt over egne medarbeidere.

KS Læring benytter eFaktors kompetansestyringsverktøy i en modifisert utgave som skal møte kommunenes behov for registrering av noe mer metadata enn standard. Likeså forventes det at det utvikles noen tilleggsrapporter.

Organisasjonsstrukturen er bygget opp med den enkelte kommune på topp og deretter sektorer, enheter, avdeling og arbeidstakere. En bruker kan registrere mer enn ett arbeidssted i egen profil og mer enn en jobbrolle. Dette fordi mange brukere har deltidsjobber på flere arbeidssteder. Likeså at de ofte kan ha mer enn en jobbrolle selv om de arbeider på kun ett arbeidssted.

Kommunen sine opplæringer for nye systemer skal skje i KS Læring. Kurs utarbeides av kommunens kursholdere, fagledere og av leverandører av løsninger til kommunen.

4 Nettverk og tekniskrom

4.1 Nettverk

4.1.1 Nettverksstruktur

Kommunale bygg disponerer eget nettverk med direkte tilgang til internett.

Alle bygg har egne IP-adresseområder for IPv4 og for IPv6.

4.1.2 IPv6

Kommunen jobber med overgang til IPv6. Det er i dag mulig å benytte både IPv4 og IPv6 på alle bygg.

4.1.3 Tilknytning til kommunalt nettverk

Kommunen benytter kun egne nett pr bygg med egen internett tilgang. All kommunal fellestrafikk mellom bygg skal kun gå til Microsoft Azure. Noen bygg er koblet sammen i klynger som deler én internettilkobling.hans arvid

4.1.4 Samband mellom kommunikasjonsrom internt i bygg

Ved behov for flere tekniskrom, skal ett rom etableres som hovedfordeling. Det er dette rommet som skal ha mediekonverteringsutstyr for utgang til internett. Etasjefordelere knyttes til hovedrommet med fiber i såkalt «stjernekonfigurasjon».

4.2 Horisontal kabling/spredenett

Kabling fra nettverksutstyr til fordeling i etasjen skal i hovedsak gjøres til aksesspunkter.

Det skal ikke kables til hver enkelt arbeidsplass, men det vil være aktuelt å etablere kablet nettverkspunkt for spesialutstyr som krever nettverk og strøm i samme kabel.

IKT-enheten skal involveres i planlegging av horisontal kabling og spredenett.

Norsk Elektroteknisk norm for elektriske lavspenningsinstallasjoner (NEK400) skal følges.

4.3 Trådløst nettverk

Kommunen har i dag en blanding av utstyr fra Cisco Enterprise og Unifi Ubiquiti sine trådløse produkter.

Et trådløst nett skal planlegges slik at dekning og kapasitet håndterer 3 trådløse enheter pr. person, samt at det er satt maks 15 personer pr. aksesspunkt.

Det trådløse nettet skal dekke hele byggets areal og uteareal.

I alle nye bygg skal Unifi Ubiquiti benyttes med unntak av knutepunkt hvor Cisco utstyr skal benyttes.

Det skal kables til alle aksesspunkt med minimum kat. 6A kabling.

4.4 Generelle krav til tekniskrom

Avhengig av byggets størrelse vil et bygg kunne inneholde ett eller flere tekniskrom. Et tekniskrom vil typisk kunne inneholde byggfordeler, etasjefordeler og nettelektronikk.

4.5 Bygningstekniske krav:

Tekniskrom skal gi nødvendig sikkerhet mot skade, datainnbrudd og tyveri av utstyr, samt forhindre uautoriserte personer tilgang. Avhengig av byggets størrelse og utforming skal det være underfordelinger andre steder i bygget.

Størrelse på tekniskrom bestemmes ut fra behov og eventuelt framtidig behov for utvidelse. Maksimal lengde for installert horisontalkabel som er gitt av NEK EN 50173 er i mange tilfeller den viktigste parameteren for plassering og antall tekniskrom.

Sikker plassering i bygning, dvs. ved plassering i kjeller/underetasje bør rommet etableres over grunnvannslinjen.

Vinduer frarådes grunnet mulighet for uønsket tilgang, og må eventuelt sikres mot innbrudd med gitter eller lignende.

Nærhet til byggets hovedføringsveier for kabel, dvs. kabelsjakter og bruer.

Unngå plassering som kan medføre tilleggsvarme i form av soloppvarming.

Gulv må tåle vekt på inntil 300 kg/m2 (må vurderes opp mot reell racklast og i et større datarom vil behovet kunne være 1500 kg/m2).

Grunnet viftestøy må rommet etableres i god avstand fra faste arbeidsplasser

Etableres i trygg avstand fra installasjoner som genererer elektriske felter (eks. trafoer, elektromotorer, kraftkabler, heis etc.), ref. segregasjonskrav i NEK EN 50174-2. Lavfrekvente magnetiske felter skal ikke overskride 1,25 µT (EN50024 / CISPER 24)

Vedrørende brannbestandighet skal alle bygningsdeler som avgrenser IKT-rommet tilfredsstille til enhver tid gjeldende regelverk (Plan og bygningsloven) og minimum tilfredsstille brannklasse EI60 (A60).

Ideell takhøyde bør være 2600 mm fra overkant ferdig gulv og til underkant, takmonterte installasjoner med unntak for bruer for tele-/datakabling. Ideell fri avstand over rack bør være 400 mm. Kravet kan avvikes, spesielt for små/mellomstore installasjoner, men da i forståelse med byggherre.

Alle flater, dvs. vegger, tak og eventuelt undergulv skal være behandlet med støvbindende materialer. Gulv skal ha ESD-gulvbelegg. Motstand fra ethvert punkt i gulvbelegget og til jord skal være 1MΩ<Rj<10 MΩ. Jfr. NEK EN 50174-1:2009.

Dersom datagulv etableres skal det ha samme høyde som gulv i tilstøtende rom/korridor.

For adkomst etableres dører 900x2100 mm (BxH) Dør skal være utrustet med lås og elektronisk adgangskontroll.

Branndeteksjon/brannslukking: Rommene skal minimum være utrustet med punktdetektor for branndeteksjon tilkoblet automatisk brannalarmsentral. Viktige rom skal være utrustet med aspirasjonsdetektor. Alle rom skal være utrustet med CO2 brannslukkingsapparat (min 6 kg). I kritiske rom bør invert luft vurderes. Vannsprinkling bør unngås. Rommet skal tilfredsstille offentlig regelverk med hensyn til deteksjon og slukking.

4.5.1 Kjøling/vann/ventilasjon

Rommet skal utrustes med kjøling og kjølebehovet må beregnes ut fra tilført effekt fra utstyr og rom.

Normalt anses takmonterte kjølere å være tilfredsstillende, men ved større kjølebehov må gulvplasserte dataromskjølere benyttes.

Alle typer fremmedvann skal unngås, dvs. det er ikke tillatt med gjennomgående vann-/avløpsrør i rommet. Sluk i gulv kan etableres, men vil også kunne medføre tilbakeslag og vanninntrenging.

Rør og andre installasjoner i overliggende etasjer, som ved lekkasjer kan ha konsekvens for tekniskrom skal unngås.

Vannrør til kjølere skal være isolert for å unngå kondens.

Anbefalt romtemperatur: 20 – 25 °C. Terskelverdi for alarm 25 °C med maksimal tillatt temperatursvingning er 5 °C pr. time.

Luftfuktighet: 40 – 55 % RF (relativ fuktighet). Avhengig av type utstyr kan befuktning utgå, men må avklares med byggherre.

Inngående luft skal være renset for støv, røyk, smuss etc. Lufttrykk inne i rommet bør være høyere enn omliggende rom. Dette for å hindre inntrengning av urenheter.

Benyttes SD-anlegg skal dette overvåke lufttemperatur og fuktighet, samt styre kjøleenheter hvor dette er mulig. Avhengig av beliggenhet og innredning kan det være aktuelt å tilkoble fuktfølere til SD-anlegg. Det skal være mulig å hente ut statistikk for temperatur og luftfuktighet fra SD-anlegget.

4.5.2 Strømforsyning/Belysning/Føringsveier

Behovet for normalkraft, reservekraft og avbruddsfri kraft (UPS) må avklares med byggherre. Alt teknisk utstyr skal være tilkoblet UPS levert av entrepenøren. Kapasitet på UPS skal beregnes så alt tilkoblet utstyr kan kjøre uavbrutt i 60 minutter. Det er derfor viktig at behovet for reservekraft og kapasitet på UPS gjennomgås.

Systemer som har dobbel strømforsyning skal forsynes med normal-/reservekraft og UPS. For systemer som ikke støtter dobbel strømforsyning skal strøm gå via UPS kurs.

UPS bør plasseres i tilstøtende rom i forhold til tekniskrom, for mindre installasjoner kan rackmonterte UPS'er benyttes inne i tekniskrom. UPS skal overvåkes via IP.

Det etableres 2 stk. 16A 230 V kurser normal-/reservekraft og 2 stk. 16A 230 V UPS kurser pr rack. Hver kurs skal ha dobbel stikkontakt installert på bru over rack. I større installasjoner kan det være aktuelt å benytte 400V/16A eller 400V/32A for både svitsjer og servere. Dette må ses i sammenheng ved bruk av PDU-er (Power Distributed Unit) for intern distribusjon i rack.

Overordnet krav til jording er nedfelt i NEK EN 50310. Se avsnitt "512 Jording".

Rombelysning: Horisontalplan 500-800 lux og vertikalplan 200 lux.

Det skal etableres separate føringsveier for elkraft og tele-/datakabler. I rom med flere enn ett rack skal det etableres trådbru for patchekabler. Trådbru skal installeres over og i framkant av rack. Separasjonskrav i NEK EN 50174 legges til grunn for utførelse.

4.5.3 Dataskap

Før beslutning om valg av type skap/rack foretas skal dybde på utstyr som skal installeres kontrolleres.

Standard rackstørrelse er: 800 x 800 x 2200 mm (BxDxH). Rack for servere vil kunne ha større dybde. Fri plass foran rack: 1200 med mer, på sidene til rack samt fri plass bak rack: 1000 mm (Ved mindre installasjon kan dette fravikes)

Normalt benyttes kun åpne skap, dvs. uten dører, sidevegger, topp og bunn i tekniskrom. Ved spesielt krav når kjøling av utstyr gjøres ved bruk av styrte luftstrømmer må det benyttes skap med sidevegger, dører, topp og bunn.

Datanett vil kunne inneholde gradert informasjon og i tilfeller der flere institusjoner og/eller bedrifter deler tekniskrom skal de kommunale skapene utrustes med låsbare dører, sidevegger og topp. Det må også velges løsninger som muliggjør god luftventilering og føring av kabel ut av skap og intern kabling

I mindre anlegg med lite utstyr skal en vurdere vegghengte skap.

4.5.4 Diverse

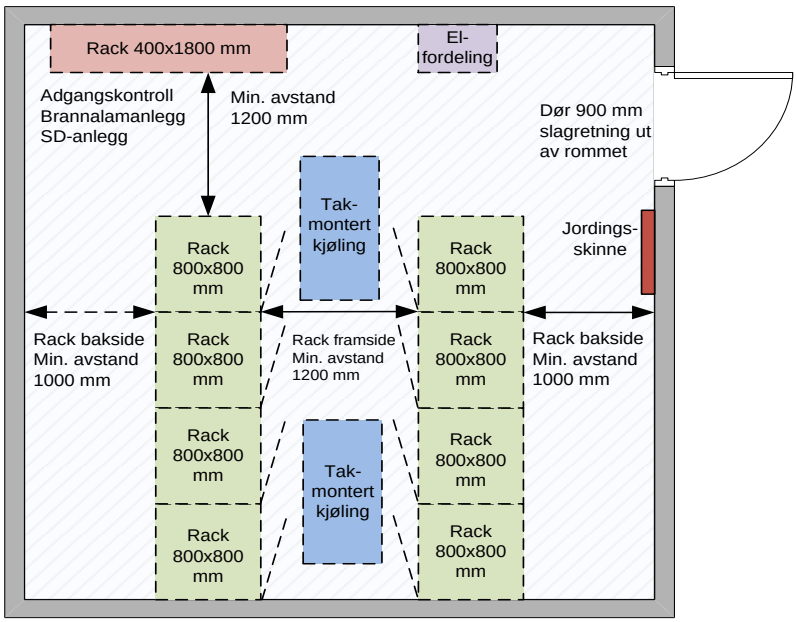
Det er ikke tillatt å benytte tekniskrom som lager.

Adgang til rommene skal være begrenset til byggherre og kommunens IT-personell

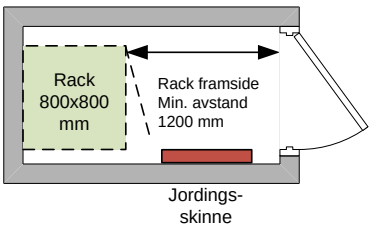
Service og driftspersonell skal ha tilgang til rommene, men i henhold til sikkerhetsinstruks.

Tekniskrom skal ved overlevering være rengjort. Det er viktig at byggstøv fjernes fra alle bygningsmessige elementer som kabelbruer, skap, armaturer etc. Videre skal rommet inngå i byggets generelle rengjøringsrutiner og minimum rengjøres 1 gang pr måned. Egen rutine for rengjøring må lages.

Etterfølgende figurer viser typisk innredning av et større tekniskrom og en nisje. Samme prinsipper skal legges til grunn, uavhengig av størrelse.



Eksempel på innredning av tekniskrom.



Eksempel på innredning av mindre tekniskrom/nisje hvor kravet til fri plass bak skap avvikes.