Kravsspecifikation
for
ADK-systemer

Dato	Sagsbehandler	Firma	Version	Handling
06-2018	AZ33430	Aarhus Kommune	1.0	Oprettet
24-05-2019	AZ33430	Aarhus Kommune	2.0	Godkendt af BKG og obligatorisk at følge
13-10-2020	AZTBC86 / AZ49419	Aarhus Kommune	2.1	Godkendt af BKG og obligatorisk at følge
23-05-2021	AZTBC86 / AZ49419	Aarhus Kommune	2.2	Godkendt af BKG og obligatorisk at følge

TEKNIK OG MILJØ
Fællesadministrationen MTM
Aarhus Kommune

Bygninger
Karen Blixens Boulevard 7
8220 Brabrand

Kontakt:
Ejendomssystemer

Version 2.2

Resumé

Dette dokument omhandler obligatoriske generelle krav til elektroniske adgangskontrol og elektroniske låsesystemer i Aarhus Kommune – forkortet ADK.

ADK er en sikringsinstallation, hvis formål er automatisk eller semiautomatisk at sikre adgangsforhold.

Behovet for generelle krav til sikringsydelser er opstået på baggrund af et ønske i Aarhus Kommune om standardisering af tekniske krav.

Der opleves en tilvækst og variation i bygningstekniske installationer, og derfor bliver indkøb, kontrahering, systemejerskab, applikationer, sikkerhedshåndtering mv. samlet set mere kompleks.
Formålet med standardiseringen er, at de rette krav stilles, og at driftshåndteringen bliver mere sikker og effektiv.

MTM har fungeret som projektleder på projektet og nærværende kravsspecifikation er blevet til i samarbejde med øvrige magistratsafdelinger.

Med vedtagelse af denne kravsspecifikation er det obligatorisk, at magistratsafdelinger, som ændrer, køber eller installerer sikringsydelser eller tilhørende leverancer, følger nærværende krav til systemer/platforme samt stiller tilhørende design- og produkt/leverandørkrav mv.

Kravsspecifikationer kan generelt lokaliseres på Aarhus Kommunes intranet og på kommunens hjemmeside.

Indhold

1. Indledning

Aarhus Kommune fastlægger igennem dette dokument en obligatorisk kravsspecifikation for ADK.
Succeskriteriet for denne kravsspecifikation er, at der i Aarhus Kommune fremadrettet vælges og indbygges tekniske løsninger, som opfylder Aarhus Kommunes krav på området, så risikoen for tyveri, hærværk og anden form for kriminalitet minimeres i de perioder, hvor der er hel eller delvis adgang til kommunens lokaliteter.

ADK, der er projekteret og installeret i henhold til denne kravsspecifikation, har det formål, at de kontrollerer og evt. registrerer adgang til et fysisk afgrænset område. Ved anvendelse af ADK-systemer kan adgangsrettigheder defineres på områder, dage og tidspunkter på medarbejdergrupper, samarbejdspartnere eller enkeltpersoner.

ADK-systemer må ikke forveksles med Automatiske Indbrudsalarmeringsanlæg (AIA), som har til formål automatisk at alarmere om indbrud eller forsøg herpå.

ADK er mest relevant i større offentlige institutioner med mange ansatte og særlige aflåsningsbehov for at beskytte særlige værdier og/eller følsomme informationer.

ADK-systemer implementeres og anvendes som et supplement til traditionelle mekaniske låse og låsesystemer af bl.a. følgende årsager:

- Mekaniske låse kræver fysiske nøgler, der kan tabes eller kopieres og dermed udgøre en risiko for misbrug og/eller en økonomisk byrde ved omlægning af låsene og anskaffelse af nye nøgler samt distribution af disse. I et ADK-system kan ID-nøgler hurtigt slettes, hvis en ID-nøgle tabes, stjæles eller misbruges på anden vis, uden det påvirker de øvrige brugere

- Adgangsdøre i et ADK-system kan opbygges og programmeres efter behov, og adgangsrettigheder kan defineres på de enkelte døre eller områder. Hovedindgange, der anvendes af borgere, kan f.eks. programmeres til at være åbne/oplåst i den normale åbningstid, og personaleindgange vil typisk kræve anvendelse af adgangskort. På samme måde kan ADK anvendes til enkelte rum eller områder, så kun personer med legalt ærinde opnår adgang.

- I visse perioder kan nøglebrikker og adgangskort kombineres med anvendelse af personlig PIN-kode, så risikoen for misbrug af tabte eller stjålne adgangskort minimeres. Endeligt kan der være

bygninger, områder eller rum med særligt kostbart udstyr eller følsomt materiale f.eks. rum med servere og krydsfelter, hvortil der kræves brug af PIN-kode på alle dage og tider.

- ADK kan desuden benyttes som supplerende informationskilde til et tv-overvågningssystem, så logninger fra ADK-anlægget f.eks. kan anvendes til søgninger i tv-overvågningssystemet efter uregelmæssigheder eller kriminelle.

- Hvor der er installeret et ABA-anlæg, kan brandalarmsignal fra ABA-anlægget gives til ADK-anlægget, så ADK-døre oplåser i flugtvejsretningen ved brandsignal. Denne løsning skal godkendes af den lokale brandmyndighed.

I valget af ADK-system må den offentlige institution gøre sig overvejelser om, hvad systemet skal kunne, set i forhold til institutionens størrelse, sikringskrav, risikoprofil og funktionsønsker.
Et ADK-system kan bidrage til håndtering af en række risici, f.eks. indbrud, hærværk, trusler, terror og brand.

2. Begreber

2.1. Aarhus Kommunes Organisation

2.1.1. Magistratsafdeling

Aarhus Kommune er opdelt i 6 Magistratsafdelinger:

- BA - Borgmesterens afdeling, bl.a. IT og Digitalisering
- MTM - Teknik og Miljø
- MSB - Sociale forhold og beskæftigelse
- MSO - Sundhed og Omsorg
- MKB - Kultur og Borgerservice
- MBU - Børn og Unge

Hver Magistratsafdeling ledes af en direktør og en af byrådet udpeget Rådmand. Rådmænd og direktører mødes ugentligt i ”magistraten”, der fungerer som et beslutningsdygtigt forretningsudvalg for Byrådet.

2.1.2. Forvaltning

Hver magistratsafdeling er opdelt i et antal forvaltninger, der varetager en eller flere af Kommunens kerneopgaver med reference til Magistratsafdelingens direktør og Rådmand. På flere områder er der etableret fællesfunktioner, herunder ejendomsområdet.

2.1.3. Institution

En forvaltning kan drive en eller flere Institutioner, der yder en specifik kommunal serviceydelse til borgerne.

2.2. Aarhus Kommunes bygninger og lokationer

Ejerforhold, opgaver og ansvar:
Ejendomsområdet er karakteriseret ved en hhv. central og decentral struktur, hvor ejerskab til bygninger er placeret i hver magistratsafdeling, mens andre områder forvaltes mere centralt.
Afdelingen Ejendomme i Teknik og Miljø udgør Kommunens fællesfunktion på ejendomsområdet og rådgiver om - og varetager - vedligehold og genopretning af klimaskærm, tekniske anlæg og udenomsarealer for hovedparten af de kommunale bygninger. Derudover håndteres og rådgives om byggetekniske- og planmæssige forhold samt service og drift.
Tværgående funktioner som Ejendomssystemer (ADK, AIA, TVO ol.), energiledelse, håndtering af og rådgivning om problematiske stoffer, bæredygtighed, bygningsteknisk netværk, metode og systemsupport til FM-system og afrapportering på tværs af bygningsområdet ledes af Ejendomme og sker koordineret og i samarbejde med øvrige magistratsafdelinger.

Hver magistratsafdeling administrerer og håndterer en række bygninger, og håndterer ejer/lejer-, drifts-, vedligeholds- og serviceansvar for disse bygninger samt om-, til- og nybyggeri.

Ansvarsfordeling kan overordnet illustreres med nedenstående diagram[1]:

<table>
<tr><th colspan="8">Roller, opgaver og ansvar</th></tr>
<tr><th>Mag. afd.</th><th>Ansvar i alle mag. afd.</th><th colspan="6">Fællesfunktionen i Ejendomme, MTM</th></tr>
<tr><td>MBU</td><td>Ejerskab til bygninger
Planlægning</td><td rowspan="5">Vedligehold/genopretning
Klimaskærm, tekniske installationer</td><td rowspan="5">Rådgivning vedr. Byggefaglige forhold, service mv.
Tværgående koordinering</td><td rowspan="5">Ejendomssystemer, metode og FM–system</td><td rowspan="5">Aa+ program</td><td rowspan="5">Energiledelse</td></tr>
<tr><td>MKB</td><td>Strategi, behov/organisering
Modernisering/forbedringer</td></tr>
<tr><td>MSB</td><td>Indvendigt vedligehold
Visse installationer</td></tr>
<tr><td>MSO</td><td>Fleste sikringsydelser
Forbrug – el, vand, varme</td></tr>
<tr><td>MTM</td><td>Rengøring, service</td></tr>
<tr><td>MBA</td><td colspan="6">Krav vedr. teknisk netværk/opkoblede installationer. Personfølsomme oplysninger</td></tr>
</table>

[1] Der henvises til mere detaljeret snitfladebeskrivelse, som fastlægges i samarbejdsaftalerne mellem MTM og øvrige magistratsafdelinger

3. Definitioner

Aarhus Kommune anvender definitioner for ADK-systemer, som er lig Forsikring & Pensions nyeste standarder og begreber på området. Disse er indeholdt i det såkaldte Suppleringskatalog. Når Aarhus kommune henviser til teknologiske standarder og teknologisk funktionalitet vil det i videst muligt omfang være med reference til Sikkerhedsbranchens nyeste Suppleringskatalog[2]. Emner som f.eks. ”Adgangskontrolenhed”, ”ID-nøgle”, ”Sikringsniveau” og ”Skalovervågning” (listen over emner er ikke udtømmende) skal dermed hentes fra www.forsikringogpension.dk:

- Suppleringskatalog Kapitel 2 - ADK - september 2017[3] - version GES-2012-00141 Dok ID 343459 eller nyere
- Suppleringskatalog Kapitel 2, Appendiks A Teknisk Specifikation Elektronisk adgangskontrol[4] - GES-2012-00141 Dok ID 344396 eller nyere
- Suppleringskatalog Kapitel 2, Appendiks B Behovsvurdering Elektronisk adgangskontrol[5] - GES-2012-00141 Dok ID 344387.

I forbindelse med udbud af en ydelse vil det være de standarder på www.forsikringogpension.dk, som var gældende ved udbuddets offentliggørelse som er gældende.

4. Roller

4.1. Driftsoperatør, systemejer, systemleverandør

Driftsoperatøren er i Aarhus Kommune ”Fælles service, Infrastruktur” i Borgmesterens afdeling, eller et firma, der har en driftsaftale med Fælles Service. Driftsoperatøren/”Fælles Service, Infrastruktur” leverer drift af LAN og WAN, servere, print og arbejdspladser.

Driftsydelsen aftages af **Systemejere.** Systemejerens primære funktion er ansvar og økonomisk beslutningskompetence, og som tegner systemet overfor såvel interne som eksterne interessenter. Systemejeren har bl.a. det overordnede ansvar for systemets anskaffelse og finansiering, for dets drift

[2] http://info.forsikringogpension.dk/virksomheder/fpsikring/tyveri/kataloger_og_vejledninger/Sider/Suppleringskatalog.aspx

[3] http://info.forsikringogpension.dk/virksomheder/fpsikring/tyveri/Documents/Suppleringskatalog%20Kapitel%202%20-%20ADK%20-%20september%202017.pdf

[4] http://info.forsikringogpension.dk/virksomheder/fpsikring/tyveri/Documents/ADK%20-%20Appendiks%20A%20-%20september%202017.pdf

[5] http://info.forsikringogpension.dk/virksomheder/fpsikring/tyveri/Documents/ADK%20-%20Appendiks%20B%20-%20september%202017.pdf

og support, for rettighedsstyringen, for overholdelsen af interne retningslinjer og lovkrav, for dialogen med alle interessenter for dokumentation og for systemets rettidige udfasning. Systemejeren fastlægger ADK-systemets tilgængelighed og funktionalitet, og er ansvarlig for databehandleraftaler til driftsoperatør og vagtoperatør.

En **systemleverandør**, er en leverandør af den systemtekniske installation eller ydelse, og vil typisk have den tekniske dialog omkring tilgængelighed og performance direkte med driftsoperatøren, tvister og beslutninger med funktionel eller økonomisk konsekvens eskaleres til Systemejeren.

Driftsoperatøren har som udgangspunkt ikke behov for at kunne tilgå streamede og lagrede data fra et ADK-anlæg, men vil af systemtekniske og driftsmæssige årsager ofte have adgang til dem alligevel. Driftsoperatørens tilgang til data skal derfor reguleres af en databehandleraftale.

4.2. Vagtoperatør

"Østjyllands Brandvæsen" er af Aarhus Kommunes Byråd udpeget til at være Vagtcentral (alarmmodtager) for Aarhus Kommunes bygninger og dermed fungere som vagtoperatør. Vagtcentralen har bemyndigelse til at iværksætte reaktion på alarmer ud fra en nærmere defineret forholdsordre, og Vagtcentralen er derfor en væsentlig interessent for Systemejeren.

4.3. IT-Sikkerheds områdeansvarlig

Aarhus Kommune håndterer de forhold, der vedrører Persondatalovgivningen i en særskilt IT-Sikkerhedsorganisation. F.eks. sager vedrørende aktindsigt og Borgerens rettigheder til egne data og udlevering af logdata, herunder ADK-data, til Politiet i forbindelse med efterforskning.

Den IT-Sikkerhedsområdeansvarlige[6] for en organisatorisk enhed, hvor der anvendes ADK-anlæg, er derfor en væsentlig interessent for Systemejeren, idet den IT-Sikkerhedsområdeansvarlige - bl.a. ud fra adgang til ADK-data, skal kunne vurdere, om der i en given sag er juridisk grundlag for at foretage en politianmeldelse, og/eller om der er sket brud på interne retningslinjer.

Den IT-Sikkerhedsområdeansvarlige har behov for i konkrete situationer at kunne tilgå specifikke lagrede data fra ADK-anlægget direkte i systemet eller gennem krypterede udtræk. Den IT-Sikkerhedsområdeansvarliges adgang til data kan tildeles fra sag til sag af den for magistratsafdelingens og systemets respektive systemejer.

[6] Udpeges af forvaltningen og godkendes jfr. Aarhus Kommunes IT-sikkerhedspolitik af IT-sikkerhedschefen. Ønskes den it-sikkerheds områdeansvarlige kontaktet, benyttes: itsikkerhed@aarhus.dk

4.4. Administrative institutionsleder

Et ADK-anlæg kontrollerer og styrer typisk én, flere eller alle adgangene i bygningerne i en institution, og den administrative institutionsleder er derfor en vigtig interessent for Systemejeren, da den administrative institutionsleder er den primære aftager af det konkrete ADK-anlægs sikringsleverance, og også den primære betaler for det konkrete ADK-anlægs omkostninger.

Den administrative institutionsleder er også en vigtig interessent for den IT-sikkerhedsområdeansvarlige, idet dialog om en eventuel politianmeldelse på basis af ADK-data initieres af den administrative institutionsleder.

Den administrative institutionsleder har, i kraft af sit bygningsadministrative ansvar, behov for løbende at kunne tilgå data i ADK-anlægget for bl.a. at oprette og slette brugere eller som kontrol, hvis denne opgave foretages af en anden medarbejder.

4.5. Teknisk Servicemedarbejder

Det tekniske servicepersonale på en institution har behov for at kunne tilgå almindelige administrative data fra et ADK-anlæg, men har ikke nødvendigvis behov for at kunne tilgå lagrede personlige data. Begrænsninger reguleres af bygningsejeren.

5. Ikke funktionelle krav, afklares inden udbud

5.1. Persondataforordningen (GDPR)

GDPR foreskriver, at der ved relevant forespørgsel er udleveringspligt ift. data for Aarhus Kommune. For nuværende vurderer Aarhus Kommune, at ADK ikke falder ind under GDPR lovgivningen, da der ikke opbevares personhenførbare data. Der er desuden ikke pligt til at anmelde ADK-systemer på kommunens anmeldelsesportal.
En databehandling kan efter databeskyttelsesforordningen omfatte enhver håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse. Finder blot en af de nævnte former for håndtering af personoplysninger sted, vil der være tale om en behandling, som er omfattet af databeskyttelsesreglerne og dermed er der krav om oprettelse af en databehandleraftale.

5.2. Beskrivelse af ADK-behov

Ved etablering af ADK skal det som bruger nøje overvejes, hvad man reelt skal bruge den pågældende ADK til. Årsagen er, at mulighederne for funktionalitet og rolleinddeling i et ADK-system er under hastig udvikling, så en beskrivelse af brugerkrav er helt essentielt for en løsning, som tilgodeser både den teknologiske formåen, økonomi, databehandling, lagring og de reelle problemstillinger man må ønske ADK skal hjælpe med at løse.

Det primære formål med et adgangskontrolsystem er at sikre, at kun ønskede personer kan få adgang til et kontrolleret område. Adgangskontrolanlægget kan derfor beskytte personer, genstande, faciliteter m.m. mod uønskede personer, der vil kunne kompromittere sikkerheden, pålideligheden og fortroligheden.

Ved en behovsvurdering skal der først og fremmest tages stilling til den overordnede risikoprofil for institutionen, som afhænger af:

- Institutionstype
- Sikringsniveau
- Institutionens samlede værdier og generelle risikoprofil
- Forventning til uønskede personers midler og motivation for at omgå adgangskontrolsystemet.

Behovsvurderingen skal også på et overordnet niveau beskrive systemets rolle i institutionens samlede sikringsløsning, eller hvordan systemet indgår i institutionens samlede sikringsløsning.

Der henvises her til en dybere behovsvurdering baseret på Forsikring & Pensions Appendiks B[7] omhandlende behovsvurdering.

Aktiviteter og anvendelse af institutionen, af fx borgere uden for den normale arbejdstid, kan have stor indflydelse på behov, omfang og projektering af ADK-anlæg. Der vil typisk opnås en større smidighed, både for administrativt personale og brugere, når automatisk op/aflåsning af døre kan foretages via ADK-anlægget.

[7] http://info.forsikringogpension.dk/virksomheder/fpsikring/tyveri/Documents/ADK%20-%20Appendiks%20B%20-%20september%202017.pdf

5.3. Integration med andre systemer

ADK-integration i andre systemer (AIA, ABA, TVO og lignende) er en god mulighed f.eks. mht. tidligt varsel eller sammenkobling af kontrol. Det kan ofte øge værdien og funktionaliteten af ADK-systemet, hvis der sker dataudveksling mellem ADK og andre tekniske anlæg. Det skal i den sammenhæng vurderes, om der evt. tilsluttes nyt udstyr til eksisterende udstyr. Herunder om der skal foretages en lovliggørelse af eksisterende netværk, komponenter, udstyr eller anlæg.

Hvis ADK-anlægget indgår som en del af f.eks. et eksisterende AIA-anlæg, og/eller virker som en del der verificerer alarmer, skal ADK-anlæg inden for sikringsniveauerne være installeret af en certificeret installatør i henhold til den gældende kravsspecifikation for området.

Ved valg af endelig løsning skal valgte løsning som minimum afklares og beskrives ift. forhold, som kan have indflydelse på ADK herunder:

- AIA-integration: ADK-anlægget udveksler data med AIA-anlægget f.eks. med det formål at forhindre adgang til et kontrolleret område, hvor der er aktiv AIA-alarmovervågning eller med det formål at til/frakoble AIA overvåget område fra ADK-anlæggets kortlæsere eller andet genkendelsesudstyr. Integrationen skal endvidere tilsikre, at der udløses en AIA-alarm, såfremt ADK-døre opbrydes eller er åbentstående længere tid end tilladt.

- ABA-integration: Automatisk Brandalarm Anlæg udveksler data med ADK-anlægget f.eks. med det formål at frigive alle døre ved detekteret brand.

- TVO-integration: Adgangskontrolanlægget udveksler data med et TV-overvågningsanlæg f.eks. med det formål at kunne verificere personer, der ønsker adgang, eller med det formål at starte optagelser ved alarm fra adgangskontrolanlægget.

- Anden integration: Adgangskontrolanlægget kan udveksle data med andre typer tekniske anlæg med det formål at opnå en forbedret funktion af et eller begge af de anlæg, der integreres. GDPR-krav skal overholdes, når der udveksles data imellem ADK og andre systemer.

Integration/dataudveksling kan foregå på flere niveauer: Mellem klienter, mellem fordelerbokse eller på komponentniveau.

5.4. Forholdsordre

Forholdsordre er en skriftlig instruktion, som beskriver den ønskede reaktion i tilfælde af alarm fra et AIA-anlæg. Herunder også fra andre systemer og anlæg der er integreret med AIA-anlægget f.eks. ADK-anlægget.

Såfremt ADK-anlæg udveksler data med andre sikringsinstallationer, skal dette fremgå af forholdsordren, så alarmhåndtering og reaktion på alarmer sker målrettet og effektivt.

5.5. Beskrivelse af ydelsesgrænser

Det anbefales generelt, at ydelsesgrænser imellem bruger- og sikringsbehov, teknologiske ønsker, bygherre, rådgiver, service-provider og entreprenør nøje beskrives inden igangsætning af et projekt.
Det kan f.eks. forekomme, at el-låse, karmoverføringer og åbningskontakter m.v. leveres under anden entreprise, så de monteres fra fabrikken.

Specielt anbefales det at kontakte bygningsafdelingerne, Ejendomssystemer og Fælles Service via ServiceNow allerede i designfasen, da kyndig vejledning fra Kommunens specialister kan eliminere senere og fordyrende misforståelser.

Der henvises til bilag 2 som *kan* benyttes til en systematisk afdækning af ydelsesgrænserne.

Udgifter til nødvendige switche, som vurderes nødvendige for tilslutning til Aarhus kommunes kontrol-/vagtcentral(er), skal afholdes af ADK-projektet og medtages i tilbuddet.

Aarhus kommune forbeholder sig retten til at projektere og etablere nødvendigt IP-netværk fra ADK-systemets switch til netdistributørens kantrouter for transmission af evt. videosignal til Aarhus kommunes kontrol-/vagtcentral(er).

6. Krav til leverancen

Ved indkøb af ADK-anlæg skal følgende krav stilles til leverancen:

6.1. Datasikkerhed og standarder

Alle installerede ADK-systemer skal være åbne anlæg, hvilket som minimum medfører at:

- Alle service-, master- og administrationskoder/passwords skal vederlagsfrit udleveres til systemejeren
- ADK-systemer skal uden begrænsninger kunne serviceres af anden ISO9001 ADK certificeret installatør i henhold Forsikring & Pensions[8] retningslinjer
- Installerede anlægsdele, komponenter mv. skal være standardvarer, som skal kunne anskaffes uafhængigt af ADK-entreprenøren
- ADK-entreprenøren ved valg af komponenter skal sikre sig, og dokumentere ved grossist/leverandør, at disse som minimum er lagervare og kan supporteres i mindst 2 år, fra installationen er idriftsat og godkendt og Kommunen har modtaget en tilhørende "Installationserklæring"[9]
- ADK-leverandør/installatør skal være ISO9001 godkendt.

Anvender ADK-entreprenøren underleverandører, skal dette meddeles projektlederen/bygherren skriftligt i passende tid inden dennes arbejde påbegyndes. Disse underleverandører skal være ISO9001 certificerede. Kopi af certifikat udleveres inden kontraktindgåelse.
ADK-entrepriser skal udføres af certificerede, og dermed af faglært personale med relevante kompetencer.

6.2. Ejendomsret

Alle installerede ADK-anlæg og systemer skal være ejede, dvs. Aarhus Kommunes ejendom efter installation. Der må således ikke installeres abonnementsanlæg eller leaset udstyr.
I bygninger der ikke ejes af Aarhus Kommune, skal Kommunen have fuld brugsret og være systemejer og bestyrer af ADK-anlægget, som hvis der var tale om ejerskab.
Koder til anlægget er Aarhus Kommunes ejendom.
Er disse, af eller anden årsag, ikke registreret eller er det ikke de rette koder der er noteret, skal installatør til enhver tid udlevere dem uden beregning.
Dette glæder alle koder der giver adgang til anlægget, masterkode, servicekode, login til pc/server, login til software etc.

8 https://www.forsikringogpension.dk/

9 Se Bilag 1

6.3. Lovgrundlag og gældende forskrifter

ADK-entreprisen skal udføres i henhold til:

- Dansk Ingeniørforenings normer for bygningsinstallationer
- Danske Standarder
- De efter dansk lovgivnings ministerielle og kommunale bekendtgørelser
- De til enhver tid gældende bestemmelser og forskrifter, herunder specielt:
  - Sikkerhedsbranchens etiske retningslinjer
  - De gældende Almindelige Betingelser (AB/ABT/ABR)
  - EN 60839-11-1 og EN 60839-11-2, eller nyere, i sin helhed
- Persondataforordningen
- Anlægget skal opfylde bygherrens og Aarhus Kommunes øvrige politikker samt Forsikring og Pensions' forskrifter for ADK

I tilfælde af uoverensstemmelser mellem Forsikring og Pensions' forskrifter og Aarhus Kommunes krav fastsat i udbuddet, er Aarhus Kommunes krav i udbuddet gældende.

Herudover er følgende standarder gældende i nyeste version:

- AIA-kataloget 2008, Forsikring & Pension
- Sikringskataloget 2014, Forsikring & Pension
- Teknisk Specifikation for Adgangskontrolanlæg 2017, Sikkerhedsranchen
- DS/EN 60239 Stærkstrømsbekendtgørelse
- Fællesregulativet for elinstallationer
- Gældende bygningsreglement
- Arbejdstilsynets gældende forskrifter og meddelelser m.v.
- It-infrastrukturs forskrifter "Kundens IT-miljø", "Netværk i Aarhus kommune" og "Fire netværksopkoblinger til Bygningsteknisk net"
- ADK-kabling skal følge Aarhus kommunes "Kravspecifikation for IT-kabling" og tilhørende dokumenter.

7. Funktionelle krav til ADK-systemer

Aarhus kommune har en fælles administrativ platform for opkobling af ADK-systemer. Hvis det i et konkret udbud vurderes nødvendigt at etablere opkobling på denne Fælles platform til ADK, skal systemejeren for det pågældende bygningstekniske netværk inddrages i de designmæssige krav.

ADK-systemer skal, som udgangspunkt af bygningsejeren/bygherre, registreres i Aarhus kommunes FM system. De oplysninger, der skal registreres, er alle data, som er nævnt i Installationserklæringen[10], bruger, installationstidspunkt, installationstype, antal enheder, tegninger med placeringer.

7.1. Tekniske specifikationer

I forbindelse med leverandørens afdækning og udarbejdelse af kundens behov skal der udarbejdes en beskrivelse af de tekniske specifikationer, som tilbydes igennem leverancen. Aarhus Kommune tager udgangspunkt i den standardiserede og anerkendte systematiske tekniske beskrivelse som tilbydes af Forsikring og Pension:

- Suppleringskatalog Kapitel 2, Appendiks A Teknisk Specifikation Elektronisk adgangskontrol[11] - GES-2012-00141 Dok ID 344396 eller nyere.

Den tekniske specifikation har til formål at danne grundlag for en standardiseret beskrivelse og dokumentation for ADK-anlæggets funktioner og kapacitet.

Teknisk er der mange forhold, der skal overvejes, og parametre som skal bestemmes. Det er derfor vigtigt, at formålet med adgangskontrollen sammenholdt med de fysiske rammer på sikringsstedet danner baggrund for korrekt valg af funktioner, adgangstype og teknologi. Placering af f.eks. låse er desuden yderst vigtigt for, at en hændelse kan dokumenteres i den ønskede detaljeringsgrad. Funktionalitet i forbindelse med roller skal vurderes grundigt, og ønskes der integration i andre systemer skal det fastlægges allerede i designfasen.

De enkelte ADK-systemer projekteres teknisk af rådgiver eller den bydende virksomhed samt eventuelt i samarbejde med Ejendomssystemer, så ADK-fabrikantens forskrifter er opfyldt sammen med de opgavespecifikke og aktuelle krav til de sikringskategorier, som ønskes. Ved integration i andre

[10] Se Bilag 1

[11] http://info.forsikringogpension.dk/virksomheder/fpsikring/tyveri/Documents/ADK%20-%20Appendiks%20A%20-%20september%202017.pdf

sikringssystemer skal der projekteres ud fra Forsikring & Pensions Suppleringskataloger[12] for området.

Ved afgivelse af tilbud skal der sammen med de tekniske specifikationer afleveres bygningstegninger eller skitser, der illustrerer det tilbudte sikringsomfang og komponenters placering.

8. ADK-udstyr i Aarhus Kommunes IT-driftsmiljø

8.1. Netværk og tjenester på netværk

ADK-anlæggets central- og transmissionsudstyr skal placeres på Aarhus Kommunes bygningstekniske netværk, der er en særskilt VRF i Aarhus Kommunes IT-infrastruktur, hvorfra der kun er adgang til andre netværk, herunder leverandørens private netværk og andre netværk i Aarhus Kommunes infrastruktur, gennem firewallregler og/eller VPN.

Leverandøren kan få adgang til udstyret på Bygningsteknisk netværk med forskellige teknologier:

- Personlig VPN-opkobling for leverandørens medarbejdere med Cisco AnyConnect fra Internetsiden. Der anvendes digital medarbejdersignatur kombineret med et AD-login fra Aarhus Kommune og to faktor autentifikation med ”SoloId”.

- Site-2-Site VPN opkobling imellem leverandørens netværk og Aarhus Kommunes bygningstekniske netværk. Aarhus Kommune forbeholder sig ret til at kræve NAT’ning af leverandørens IP-adresser ved sammenfald med IP-adresser i Aarhus Kommunes netværk.

På Bygningsteknisk netværk anvendes statiske IP-adresser, som tildeles med DHCP.

DNS leveres af Aarhus Kommunes fælles DNS-tjeneste, der forwarder til Google DNS 8.8.4.4.

NTP leveres af Aarhus Kommunes interne NTP-tjeneste, og der er ikke adgang til eksterne NTP-tjenester.

Der er adgang til en SMTP-gateway for formidling af udgående e-mail.

[12] http://info.forsikringogpension.dk/virksomheder/fpsikring/tyveri/kataloger_og_vejledninger/Sider/Suppleringskatalog.aspx#

Der er udgående adgang til Internet på port TCP/80 http og TCP/443 https. Udgående adgang på andre porte tildeles kun på basis af ”change request” og kun til specifikke eksterne IP-adresser.

Indgående adgang fra Internettet til enheder på teknisk netværk tillades ikke.

På LAN vil der være adgang til 100 Mbit/s trådet netværk.

Hastigheden igennem Aarhus Kommunes Core netværk til ressourcer på Internettet eller i andre net i Aarhus Kommune afhænger af det lokale udstyrs funktionalitet og tidspunktet på dagen, men vil som udgangspunkt være >10 Mbit/s og < 100 Mbit/s.

8.2. Servere og Workstations i Aarhus Kommunes drifts-miljø

8.2.1. Servere

Skal en ADK-Server driftes i Aarhus Kommunes netværk, placeres den, afhængig af hvilke data der håndteres og lagres på den, i bygningsteknisk netværk eller i administrativt netværk.

Servere er virtuelle og driftsafvikles på Aarhus Kommunes VM-ware platform. Aarhus Kommune understøtter Windows Server 2012 og 2016 samt RedHat Linux.

Servere oprettes med A-record for deres FQDN i Aarhus Kommunes fælles DNS-tjeneste, og eventuelle webapplikationer på serveren oprettes med C-name-Alias, der peger på serverens FQDN.

Windows servere er domainjoined til Aarhus Kommunes AD domæner for hhv. administrativt og bygningsteknisk netværk, og vil være underlagt gruppepolitikker og rettighedsstyring fra Aarhus Kommune. Leverandøren kan have lokaladministratorrettigheder på serveren.

8.2.2 Workstations

Der kan ikke permanent tilsluttes workstations til bygningsteknisk netværk.

Medarbejdere i Aarhus kommune, der med klientprogrammel til Workstations skal tilgå servere eller enheder i bygningstekniske netværk, gør det fra deres administrative Windows10 pc tilsluttet administrativt netværk.

Installation af klientprogrammellet skal ske med Aarhus Kommunes SCCM softwaredistributionssystem, og klientprogrammel skal derfor leveres som MSI filer der kan eksekveres med unattended og silent mode. Aarhus Kommune varetager selv ompakningen til SCCM.

Leverandøren kan tilgå servere og enheder på bygningsteknisk netværk via egen workstation opkoblet med VPN.

8.3. Lagring af data

8.3.1 I ADK-enheden

Lagres data i selve ADK-enheden f.eks. i selve låsen hhv. nøglen, skal data - både når de beror i ADK-enheden og når de flyttes ud herfra - være krypteret med en anerkendt krypteringsalgoritme, og den private nøgle til dekrypteringen skal alene tilhøre Aarhus Kommune, og de samarbejdspartnere Aarhus Kommune ønsker at dele den med.

8.3.2 På Server/Filsystem eller NAS i Aarhus Kommunes driftsmiljø

Lagres data på medier, der driftsafvikles i Aarhus kommunes netværk, skal data være krypteret med en privat nøgle, der alene tilhører Aarhus Kommune fra kamera til lagringsmediet. Den fysiske placering af lagringsmediet, og rettighedsstyringen for adgang til lagringsmediet, anvises af Fælles Service, Aarhus Kommune. Aarhus Kommune kan kræve, at data forbliver krypteret på lagringsmediet.

8.3.3 Hos leverandøren

Lagres data hos leverandøren, skal data være krypteret med minimum SHA256 SSL-kryptering, hvis transporten foregår over Internettet, og SSL-certifikatet skal enten være udstedt af leverandøren selv, eller være min. OV og udstedt til leverandøren. Lagrede data er Aarhus Kommunes ejendom og skal desuden overholde de af Rigspolitiets opstillede krav til opbevaring af kundens informationer og data

9. Leverance og montering

ADK-anlæg skal projekteres i henhold til Forsikring & Pensions ADK-Katalog, og installeres af en Forsikring & Pension registreret og certificeret installatør.

9.1. Ny installation (arbejdets omfang)

Adgangskontrolanlæg, der er projekteret og installeret i henhold til Suppleringskatalog, Kapitel 2 "Adgangskontrol" fra Forsikring & Pension, har det formål, at de automatisk eller semiautomatisk skal sikre mod uønsket indtrængen, indbrud eller forsøg på indbrud. Adgangskontrolanlægget kan ved kompromittering afsende alarm til et automatisk indbrudsalarmanlæg og videre til en kontrol-/ vagtcentral, så en reaktion kan iværksættes og eventuelle følgeskader begrænses.

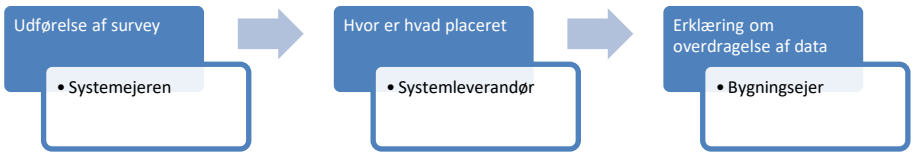
Under ADK-systemerne hører alle installations- og montagearbejder samt alle leverancer og ydelser, der er nødvendige for den fulde konditionsmæssige udførelse af alt arbejde i forbindelse med det foreskrevne ADK-system.

Adgang til lokationer aftales med projektlederen for projektet og brugeren af bygningen/bygningsejeren. Alle forhold omkring leveringstid og dokumentation aftales med bygningsejerens projektleder.

Det er entydigt installatøren, der er ansvarlig for og forestår alle installations- og montagearbejder på det lokalt tilbudte ADK-anlæg. Herunder forestår alle ydelser, der er nødvendige for den fulde konditionsmæssige udførelse og implementering samt test af det tilbudte ADK-system.

9.1.1. Survey og planlægning – Kortlægning inden udbud/intern info

For en given lokation skal der efter aftale med *systemejeren* og inden leverance og montering af adgangskontrolsystem udføres et survey, hvor låsenes placering er dokumenteret, og leverandøren skal skriftligt påtage sig ansvaret for lovligheden af den pågældende montering. Desuden skal bygningsejeren udfylde en erklæring (Databehandleraftale) om overdragelse af data til systemejeren.



Figur 1: Procesillustration

10. Service og Vedligeholdelse

ADK-entreprenøren er forpligtet at tilbyde at indgå en serviceaftale, som indeholder:

I perioden fra idriftsætning til garantiperiodens udløb:

- Et årligt tilsyn med tilhørende rapport
- Mulighed for differentieret afregning ved tilkald samt for rådighed (responstid)
- Fastprisaftale for teknikerbesøg samt for komponentudskiftning.
- Hvor dele af ADK-overvågningsanlægget virker som AIA-alarmverifikation, skal eftersyn af disse udføres årligt, efter samme retningslinjer som gældende for AIA-anlægget. Se specifikt Forsikring og Pensions AIA-katalog, fane 90[13].

Efter garantiperiodens udløb - hensigtserklæring:

- Servicekontrakt med samme dækning som i garantiperioden, indeholdende samme ydelser.

Serviceaftale skal være baseret på Aarhus kommunes paradigme "serviceaftale for ADK-anlæg". Adgangsforhold – ledsaget adgang skal fremgå af servicekontrakten. Service skal kunne fravælges efter garantiperiodens udløb.

11. Garanti og kvalitet

Der skal som minimum gives en toårig totalgaranti på alt udstyr, programmel, komponenter og installationsarbejde gældende fra aflevering.

Aflevering accepteres først, når der også foreligger fuld dokumentation samt en installationserklæring og udfyldt serviceaftale (alle bilag skal udfyldes).

Der skal i forbindelse med afleveringsforretningen overdrages følgende dokumentation på dansk til bygherre/bygningsejeren og til brugeren:

- Betjeningsvejledning, som muliggør betjening med et minimum af betjeningsfejl. Betjeningsvejledningerne skal udformes under hensyntagen til brugernes adgangsrettigheder, idet der henvises til Forsikring & Pensions retningslinjer

[13] http://info.forsikringogpension.dk/virksomheder/fpsikring/tyveri/kataloger_og_vejledninger/Documents/Fane%2090%20-%20AIA%20kataloget,%20september%202016.pdf

- Beskrivelse af de hensyn brugeren skal tage til f.eks. låse med henblik på at minimere antallet af fejlalarmer
- Anlægsdokumentationen skal udleveres til bygherre/bygningsejer.

Anlæggene skal være af en sådan kvalitet og robusthed, at uhensigtsmæssige nedbrud som manglende ADK-signal/visning, som skyldes systemtekniske forhold, maksimalt må udgøre 0,005% af samtlige driftstimer. ADK-systemets oppetid skal fremgå af en log / hhv. API overvåges med SNMP (Simple network messaging protocol). Dette opgøres af driftsejeren ved gennemgang af årlige rapporter, leveret af installatøren over serviceaftalerne.

Dokumentation skal afleveres i henhold til Aarhus Kommunes IKT-paradigme[14].

Dokumentationen skal være på dansk, undtaget dog datablade og eventuelle brochurer.

[14] Informations- og kommunikationsteknologi..Link: https://www.aarhus.dk/virksomhed/leverandoer-til-os/krav-til-leverandoerer-af-bygge-og-anlaegsprojekter/ikt-bim-cad-og-dokumentation/

12. Bilag 1 – ADK Installationserklæring

Erklæringen kan rekvireres som Word dokument på Ejendommes intranet-portal under Ejendomssystemer.

ANLÆGSEJER/-BRUGER

Navn	
Adresse	
Postnummer	By
Driftsansvarlig	Telefon

ISO 9001-CERTIFICERET VIRKSOMHED

Firmastempel
Installationsansvarlig
F&P-registreringsnr.

STAMOPLYSNINGER

Installationsadresse	Adresse, postnummer og by
Installationsnummer	
Ejerforhold - Er anlægget:	☐ Ejet ☐ Lejet/leaset eller lignende
Installationsstatus	☐ Nyinstallation ☐ Udvidelse ☐ Ændring/Dokumentation

ADGANGSPUNKTER (DØRE)
Adgangsspecifikationer jvf. gældende ADK Teknisk Specifikation.

ID	Navn	Indvendig (udgang)	Udvendig (Indgang)	Dør, overvågning	Tamper, overvågning	Funk-tionalitet	Grade	Ekstra funktion
1								
2								
3								
4								
5								
6								
7								
8								
	Se bilag for flere adgange.							

SYSTEMOPLYSNINGER

Adgangskontrol-software	Software-version:
Database-placering	☐ Lokal ☐ Central ☐ Cloud/hosted
Administration af ADK-anlægget	☐ Enkeltbruger ☐ Flerbruger (client/server) ☐ Import/export til HR ☐ Bruger selvbetjening
Transmission af alarmer	☐ Intern transmission ☐ Ekstern transmission ☐ AIA-transmission Kontrolcentral/ Driftcenter:
Integration med andre anlæg	☐ AIA ☐ ABA ☐ TVO Andet:
Kortproduktion	☐ Kortprinter ☐ Kamera ☐ Kortkoder Andet:
Specialfunktioner	☐ Betaling med kort ☐ Gæsteregistrering ☐ Evakuering Andet:
Backup af database	☐ Nej ☐ Ja ☐ Manuel ☐ Automatisk Medie:

AFLEVERING AF ANLÆG (låse og dørautomatik er ikke omfattet af denne installationserklæring)

Anlægget er solgt og installeret således at det overholder	☐ ADK-kravspecifikation
Bruger er informeret om	☐ Persondataforordningens bestemmelser
Dokumentation afleveret til kunde	☐ Brugermanual ☐ Placeringstegn. ☐ Systemdiagram ☐ Systemdele ☐ Drifts- og vedligeholdelsesvejledning
Træning og undervisning	☐ Bruger ☐ Superbruger
Afprøvning	☐ Afprøvning i.f.m. idriftssættelse
Mangelliste	☐ Nej Ellers dateret:

DRIFT

Vedligeholdelseskontrakt	☐ Ingen ☐ Helårligt ☐ Interval ☐ Fuld service og vedligeholdelse

Hermed bekræftes rigtigheden af ovenstående oplysninger.		**Hermed bekræftes, at aflevering er godkendt, og at der er rådgivet om ovenstående.**	
Dato	**Certificeret ADK-installatør**	**Dato**	**Anlægsejer/-lejer**

13. Bilag 2 – Ydelsesgrænser

IT-indholdet i sikringsinstallationer øges markant, og sammenholdt med at markedet for ADK vækster med over 8% om året, vil udviklingen fortsætte hurtigere og hurtigere i de kommende år. Det stiller en række krav til alle parter i et projekt om at afklare grænsefladerne mellem de forskellige ydelser, inden projektet iværksættes.

Til inspiration og hjælp til denne opgave er der udarbejdet et hjælpeskema, som kan benyttes som ”Ydelsesplan” i et Kommunalt projekt.

Skemaet er opbygget i 5 faser[15] svarende til et normalt entrepriseforløb:

Fase 1: Projektering

Fase 2: Projektopstart

Fase 3: Udførelse

Fase 4: Aflevering og drift

Fase 5: 1 & 5-års gennemgang

Farvebetydning: Lysegrå er ”Generelle ydelser” hvid er ”Ydelser med IT-indhold”.

Skemaet kan rekvireres som Excel ark på Ejendommes intranetportal under Ejendomssystemer.

”Bilag 2 – Ydelsesgrænser” tilsidesætter ikke AB18 som har en opdeling på:

- Ide oplæg / programfase
- Projektering
- Udbud
- Udførsel
- Aflevering
- Drift

Således skal afleveringsforretning følge AB18

[15] Hjælpeskemaet kan ikke benyttes som hovedfaser ifm. rådgivning jfr. ABR §11

nr.	Ydelse	Bygherre				Entreprenører				Service - providere		Rådgiver		
		Projektansvarlig	Sikringsansvarlig	IT-ansvarlig	Andet	Managementsystem	Sikringsanlæg	IT kabling	IT udstyr	Telefon	Internet	Projektleder	Projektmedarbejder	Byggepladsleder
	Fase 1 - Projektering													
1	Rekvirer eksisterende tegninger	U	D	D								I	U	
2	Besigtigelse i lokationer	D				(D)	(D)	(D)	(D)			I	U	
3	Sikringsanlægsprojektering	G	D	D								I	U	
4	IT-projektering	G	D	D								I	U	
	NETVÆRK (LAN/WAN)													
	Krav til netværksstruktur	G	D	D								I	U	U
	Krav til dedikeret netværk/fysisk netværk/ledere	G	D	D								I	U	U
	Monitorering/management på LAN	G	D	D								I	U	U
	Valg af domain	G	D	D								I	U	U
	Valg af WLAN metode/princip	G	D	D								I	U	U
	Beslutning om internetadgang	G	D	D								I	U	U
	Vurdering/krav til båndbredde	G	D	D								I	U	U
	HW													
	Krav til Levering af hardware og servere og switche	G	D	D								I	U	U
	Krav til levering fra ISP/WAN	G	D	D								I	U	U
	Krav til Levering af PoE-switche	G	D	D								I	U	U
	Krav til køling	G	D	D								I	U	U
	Krav til UPS/ nødstrømsforsyning	G	D	D								I	U	U
	Krav til spec. konnektorer, kabler (farver)	G	D	D								I	U	U
	Krav til transientbeskyttelse	G	D	D								I	U	U
	Krav til racks	G	D	D								I	U	U
	Krav til vertikalkabling	G	D	D								I	U	U
	Krav til horisontalkabling	G	D	D								I	U	U
	Krav til netværkselektronik	G	D	D								I	U	U
	Krav til storagekapacitet	G	D	D								I	U	U
	SW													
	Krav til operativsystem	G	D	D								I	U	U
	Krav til databasevalg	G	D	D								I	U	U
	Afklaring af softwaremiljø (virtualisering)	G	D	D								I	U	U
	Krav til levering af software	G	D	D								I	U	U
	Valg af antal licenser/klienter	G	D	D								I	U	U
	Backup	G	D	D								I	U	U
	Krav til integration med øvrige systemer	G	D	D								I	U	U
	DATASIKKERHED													
	Krav integration med øvrige systemer	G	D	D								I	U	U
	Krav til firewall	G	D	D								I	U	U
	Viruskanner	G	D	D								I	U	U
	Udrulning af patchesopdateringer	G	D	D								I	U	U
	Sikkerhedspolicies	G	D	D								I	U	U
	Krav hvis der er "remote services"	G	D	D								I	U	U
	Krav til fysisk sikkerhed	G	D	D								I	U	U
	Krav til redundans	G	D	D								I	U	U
	Krav til TIER-niveau	G	D	D								I	U	U
	Krav til arkivering	G	D	D								I	U	U
5	Projektgranskning	U	U	U								I	U	
6	Fremdriftsrapporter	O										U		
7	Projektafklaringer/ændringer	I/G	D	D								I/G	U	
8	Myndighedsbehandling	O										I	U	
9	Tilbudsindhentning+licitation	G	O	O		U	U	U	U			I	U	
10	Forhandling	G				D	D	D	D			I/U		
11	Endelig projektøkonomi	G	O	O								I/U		
12	Hovedtidsplan	G	O	O								I/U		
		D - Deltager			G - Godkender			I - Initierer		O - Orienteres			U - Udfører	

nr.	Ydelse	Bygherre				Entreprenører				Service - providere		Rådgiver		
		Projektansvarlig	Sikringsansvarlig	IT-ansvarlig	Andet	Managementsystem	Sikringsanlæg	IT kabling	IT udstyr	Telefon	Internet	Projekleder	Projektmedarbejder	Byggepladsleder
	Fase 2 - Projektopstart													
13	Endelig kontrakt med entreprenører	G				G	G	G	G			I/U		
14	Opstartsmøde	D	D	D								I	U	U
15	Projektgennemgangsmøde					D	D	D	D			I	U	U
16	KS-plan					U	U	U	U			I/G		
17	Detailtidsplan / koordinering					O	O	O	O			I/G		U
18	Prøveopsætning	G				U	U	U	U					I
19	IT	G	D	D		U	U	U	U			I		
	NETVÆRK (LAN/WAN)	G	D	D		U	U	U	U			I		
	Netværksstruktur og design freeze	G	D	D		U	U	U	U			I		
	IP-adresse plan	G	D	D		U	U	U	U			I		
	Valg af domainnavn	G	D	D		U	U	U	U			I		
	Fastsættelse af VLAN	G	D	D		U	U	U	U			I		
	Setup af internetadgang WAN	G	D	D		U	U	U	U			I		
	Båndbredde og storagekalkulationer	G	D	D		U	U	U	U			I		
	HW	G	D	D		U	U	U	U			I		
	Afklaring af levering af hardware og servere	G	D	D		U	U	U	U			I		
	Afklaring af levering af PoE-switche	G	D	D		U	U	U	U			I		
	Afklaring af kølebehov	G	D	D		U	U	U	U			I		
	Afklaring af UPS/nødstrømsforsyningsbehov	G	D	D		U	U	U	U			I		
	Placering af klienter og servere	G	D	D		U	U	U	U			I		
	Placering af udstyr, racks og føringsveje	G	D	D		U	U	U	U			I		
	Placering af ISP udstyr	G	D	D		U	U	U	U			I		
	Afklaring af strømforsyning, effekt, forsikringer mv.	G	D	D		U	U	U	U			I		
	Afklaring af storageplacering	G	D	D		U	U	U	U			I		
	SW	G	D	D		U	U	U	U			I		
	Afklaring af levering operativsystem	G	D	D		U	U	U	U			I		
	Databasevalg med integration	G	D	D		U	U	U	U			I		
	Endelig afklaring af softwaremiljø	G	D	D		U	U	U	U			I		
	Afklaring og levering af software	G	D	D		U	U	U	U			I		
	Fastlåsning af antal licenser/klienter	G	D	D		U	U	U	U			I		
	Afklaring af servicekontrakt	G	D	D								(D)	(D)	
	DATASIKKERHED	G	D	D		U	U	U	U			I		
	Integration til øvrige systemer	G	D	D		U	U	U	U			I		
	Opsætning af viruskanner	G	D	D		U	U	U	U			I		
	Endelig beslutning af metode til udrulning af patches	G	D	D		U	U	U	U			I		
	Implementering af sikkerhedspolicies	G	D	D		U	U	U	U			I		
	Opsætning af firewallregler	G	D	D		U	U	U	U			I		
	Opsætning af backup	G	D	D		U	U	U	U			I		
	Opsætning af remoteservice	G	D	D		U	U	U	U			I		
	Opsætning af arkiveringsrutiner	G	D	D		U	U	U	U			I		
		D - Deltager			G - Godkender			I - Initierer		O - Orienteres			U - Udfører	

nr.	Ydelse	Bygherre				Entreprenører				Service - providere		Rådgiver		
		Projektansvarlig	Sikringsansvarlig	IT-ansvarlig	Andet	Managementsystem	Sikringsanlæg	IT kabling	IT udstyr	Telefon	Internet	Projektleder	Projektmedarbejder	Byggepladsleder
	Fase 3 - Udførelse													
20	Indgåelse af aftale med ISP	G	O	I/U			U		U	D	D		U	
21	Byggemøder/tilsyn					D	D	D	D					I
22	Tidsplanopfølgning	O				D	D	D	D					I/U
23	Økonomistyring	G										I/U	D	D
24	IT (installation & test)	D	D	D		U	U	U	U			I / G		
	NETVÆRK (LAN/WAN)													
	Opsætning (programmering og test) af LAN og/eller VLAN	D	D	D		U	U	U	U			I/G		
	Opsætning af domain	D	D	D		U	U	U	U			I/G		
	Opsætning (programmering og test) af internetadgang	D	D	D		U	U	U	U			I/G		
	Måling af båndbredde	D	D	D		U	U	U	U			I/G		
	HW	D	D	D		U	U	U	U			I/G		
	Installering og opsætning af vertikalkabling	D	D	D		U	U	U	U			I/G		
	Installering og opsætning af horisontalkabling	D	D	D		U	U	U	U			I/G		
	Installering og opsætning af rack	D	D	D		U	U	U	U			I/G		
	Installering og opsætning af servere	D	D	D		U	U	U	U			I/G		
	Installering og opsætning af PoE-switche	D	D	D		U	U	U	U			I/G		
	Test af køling	D	D	D		U	U	U	U			I/G		
	Installering ,opsætning og test af nødstrømsforsyning, UPS og batterikapacitet	D	D	D		U	U	U	U			I/G		
	Installering, opsætning og test af selvstændig storage	D	D	D		U	U	U	U			I/G		
	SW	D	D	D		U	U	U	U			I/G		
	Installation af operativsystem	D	D	D		U	U	U	U			I/G		
	Test af firewall	D	D	D		U	U	U	U			I/G		
	Opsætning og test af database/databaser	D	D	D		U	U	U	U			I/G		
	Installering og test af software (på servere og klienter)	D	D	D		U	U	U	U			I/G		
	Installation og test af licenser (på servere og klienter)	D	D	D		U	U	U	U			I/G		
	DATASIKKERHED	D	D	D		U	U	U	U			I/G		
	Integration til øvrige systemer	D	D	D		U	U	U	U			I/G		
	Test af viruskanner	D	D	D		U	U	U	U			I/G		
	Opsætning af udrulning af patch	D	D	D		U	U	U	U			I/G		
	Test af sikkerhedspolicies	D	D	D		U	U	U	U			I/G		
	Test af backup	D	D	D		U	U	U	U			I/G		
	Test af remoteservice	D	D	D		U	U	U	U			I/G		
	Test af arkivering	D	D	D		U	U	U	U			I/G		
	Test af Datasikkerhed	D	D	D		U	U	U	U			I/G		
25	Udbedring af akutte fejl		O	O		U	U	U	U					I/G
		D - Deltager			G - Godkender			I - Initierer		O - Orienteres		U - Udfører		

nr.	Ydelse	Bygherre				Entreprenører				Service - providere		Rådgiver		
		Projektansvarlig	Sikringsansvarlig	IT-ansvarlig	Andet	Managementsystem	Sikringsanlæg	IT kabling	IT udstyr	Telefon	Internet	Projekteder	Projektmedarbejder	Byggepladsleder
	Fase 4 - Aflevering og drift													
26	IT (dokumentation)	**D**	**D**	**D**		**U**	**U**	**U**	**U**			**I / G**		
	NETVÆRK (LAN/WAN)													
	Dokumentation for installation, test og opsætning i fase 3	**D**	**D**	**D**		**U**	**U**	**U**	**U**			**I/G**		
	HW													
	Dokumentation for installation, test og opsætning i fase 3	**D**	**D**	**D**		**U**	**U**	**U**	**U**			**I/G**		
	SW													
	Dokumentation for installation, test og opsætning i fase 3	**D**	**D**	**D**		**U**	**U**	**U**	**U**			**I/G**		
	DATASIKKERHED													
	Dokumnentation for installation, test og opsætning i fase 3	**D**	**D**	**D**		**U**	**U**	**U**	**U**			**I/G**		
27	Færdigmelding (AB92)					I/U	I/U	I/U	I/U			O		O
28	Mangelgennemgang		D	D		D	D	D	D				U	I
29	Start af testperiode/driftafprøvningsperiode	U	U	U								I		
30	Afhjælpning af fejl og mangler					U	U	U	U			I		G
31	IT (fejlretning)					**U**	**U**	**U**	**U**			**I / G**		
	NETVÆRK (LAN/WAN)													
	Fejlretning af installation og opsætning fra fase 3					**U**	**U**	**U**	**U**			**I/G**		
	HW													
	Fejlretning af installation og opsætning fra fase 3					**U**	**U**	**U**	**U**			**I/G**		
	SW													
	Fejlretning af installation og opsætning fra fase 3					**U**	**U**	**U**	**U**			**I/G**		
	DATASIKKERHED													
	Fejlretning af installation og opsætning fra fase 3					**U**	**U**	**U**	**U**			**I/G**		
32	Afslutning af testperiode/endelig idriftsættelse (fejlrettet anlæg)	O	O	O		U	U	U	U			I		
33	Installationserklæring for sikringsanlæg					(U)	U	(U)	(U)			G	I	
34	Rettelse af As-built, dokumentation					U	U	U	U			I/G	D	
35	Afleveringsforretning (AB92)	O	O	O		D	D	D	D			I/G		
36	Byggeregnskab	G										I		U
37	Nedskrivning af sikkerhedsstillelse	O				I/U	I/U	I/U	I/U			G		
38	Evaluering	D	D	D			(D)		(D)			I	D	
39	Slurapportering	M	M	M								U		
40	Indgåelse af servicekontrakt	G	D	D			U		U			(D)	(D)	
		D - Deltager			G - Godkender			I - Initierer		O - Orienteres			U - Udfører	

nr.	Ydelse	Bygherre				Entreprenører				Service - providere		Rådgiver		
		Projektansvarlig	Sikringsansvarlig	IT-ansvarlig	Andet	Managementsystem	Sikringsanlæg	IT kabling	IT udstyr	Telefon	Internet	Projektleder	Projektmedarbejder	Byggepladsleder
41	**Fase 5 - 1 & 5 årsgennemgang**													
42	Indkaldelse til gennemgang	O				O	O	O	O			I		
43	Mangelgennemgang	O	D	D		D	D	D	D			I	U	
44	IT	D	D	D		D	D	D	D			I / G	U	
	NETVÆRK (LAN/WAN)													
	Test af båndbredde	D	D	D		D	D	D	D			I/G	U	
	HW													
	Test nødstrømsforsyning, UPS og batterikapacitet	D	D	D		D	D	D	D			I/G	U	
	Vurdering af storagemængde	D	D	D		D	D	D	D			I/G	U	
	SW													
	Vurdering af antal licenser/klienter	D	D	D		D	D	D	D			I/G	U	
	DATASIKKERHED													
	Integration til øvrige systemer	D	D	D		D	D	D	D			I/G	U	
	Virusskanner: Kontrol af drift og evt. gennemgang af fundne vira	D	D	D		D	D	D	D			I/G	U	
	Udrulning af patch	D	D	D		D	D	D	D			I/G	U	
	Sikkerhedspolicies	D	D	D		D	D	D	D			I/G	U	
	Kontrol af at backup er etableret og fungerer	D	D	D		D	D	D	D			I/G	U	
	Remoteservice	D	D	D		D	D	D	D			I/G	U	
	Arkivering	D	D	D		D	D	D	D			I/G	U	
	Kontrol af logninger og historik	D	D	D		D	D	D	D			I/G	U	
	Kontrol af servicerapporter	D	D	D		D	D	D	D			I/G	U	
45	Mangelafhjælpning		D	D		U	U	U	U			I/G		
46	Fremdriftsrapporter	O										U		
47	Frigivelse af sikkerhedsstillelse	G				I	I	I	I			U		
48	5 års gennemgang	O				D	D	D	D			I/U		
		D - Deltager			G - Godkender			I - Initierer		O - Orienteres			U - Udfører	