



Kravsifikation for AIA-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
14-10-2020	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
26-01-2022	AZTBC86 / AZ49419	Aarhus Kommune	2.3	Godkendt af BKG og obligatorisk at følge





Resumé

Dette dokument omhandler obligatoriske generelle krav til automatiske indbrudsalarmeringssystemer i Aarhus Kommune – forkortet AIA.

AIA er en sikringsinstallation, hvis formål er automatisk at alarmere om indbrud eller forsøg herpå.

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 under "Ejendomssystemer" og på kommunens hjemmeside.

26. januar 2022

Side 1 af 28

TEKNIK OG MILJØ

Fællesadministrationen MTM
Aarhus Kommune

Bygninger

Karen Blixens Boulevard 7
8220 Brabrand

Kontakt:
Ejendomssystemer

Version 2.3



26. januar 2022
Side 2 af 28

Indhold

Resumé	1
1. Indledning	4
2. Begreber	5
2.1. Aarhus Kommunes organisation.....	5
2.1.1. Magistratsafdeling	5
2.1.2. Forvaltning.....	5
2.1.3. Institution	5
2.2. Aarhus Kommunes bygninger og lokationer.....	6
3. Definitioner	7
4. Roller	7
4.1. Driftsoperatør, systemejer, systemleverandør.....	7
4.2. Vagtoperatør	8
4.3. IT-Sikkerhedsområdeansvarlig	8
4.4. Administrative institutionsleder	9
4.5. Teknisk Servicemedarbejder	9
5. Ikke funktionelle krav, afklares inden udbud	9
5.1. Persondataforordningen (GDPR)	9
5.2. Beskrivelse af AIA-behov.....	10
5.3. Forholdsordre.....	10
5.4. Find dit sikringsniveau	11
5.5. Beskrivelse af ydelsesgrænser	12
6. Krav til leverancen	12
6.1. Datasikkerhed og standarder.....	12
6.2. Ejendomsret.....	13
6.3. Lovgrundlag og gældende forskrifter	13
7. Funktionelle krav til AIA-systemer	14
7.1. Tekniske specifikationer.....	15
8. AIA-udstyr i Aarhus Kommunes IT-driftsmiljø	16
8.1. Netværk og tjenester på netværk	16
8.2. Servere og Workstations i Aarhus Kommunes driftsmiljø	17
8.2.1. Servere.....	17
8.2.2 Workstations.....	17



8.3. Lagring af data	18	26. januar 2022
8.3.1 I AIA-enheden	18	Side 3 af 28
8.3.2 På Server/Filsystem eller NAS i Aarhus Kommunes driftsmiljø	18	
8.3.3 Hos leverandøren	18	
9. Leverance og montering	19	
9.1. Ny installation (arbejdets omfang)	19	
9.1.1. Survey og planlægning – Kortlægning inden udbud/intern info	19	
9.2. Udvidelse af anlæg	20	
10. Service og Vedligeholdelse	20	
11. Garanti og kvalitet	20	
12. Bilag 1 – AIA Installationserklæring	22	
13. Bilag 2 – Ydelsesgrænser	23	



1. Indledning

26. januar 2022
Side 4 af 28

Aarhus Kommune fastlægger igennem dette dokument en obligatorisk kravspecifikation for AIA.

Succeskriteriet for denne kravspecifikation er, at der i Aarhus Kommune fremadrettet vælges og indbygges tekniske løsninger, som opfylder Aarhus Kommunes krav på området, så antallet af skader begrænses og skader nedbringes.

AIA, der er projekteret og installeret i henhold til denne kravspecifikation, skal tilsikre, at sikringsomfang og installationsprincipper modsvarer de stillede krav. AIA-systemer kan have samme eller forskellige niveauer i og uden for arbejdstiden. Tilsvarende kan niveauet af kontrol variere fra område til område i den kommunale ejendom eller offentlig institution.

Det er oftest større offentlige institutioner, som har komplicerede alarmeringsbehov, særlige værdier og/eller følsomme informationer, der benytter elektronisk alarmering.

AIA-systemer implementeres og anvendes blandt andet i forbindelse med supplement til, eller i stedet for, tv-overvågning og mekanisk aflåsning med traditionelle nøgler, f.eks.:

- I et AIA-system kan ID-nøgler/brugerkoder hurtigt udskiftes, også uden forstyrrelse af øvrige brugere
- Adgangsrettigheder i et AIA-system kan opbygges og programmeres på et væld af forskellige måder: Fra fuldautomatisk åbning og lukning af lokaliteter efter læsning af berøringsfri ID-nøgle til ekstra-højt sikkerhedsniveau med flere koder og ID-nøgler for alarmering eller åbning af lokaliteten
- AIA kan desuden suppleres af et TV-overvågningssystem, så hændelser kan verificeres og dokumenteres.

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

Det skal dog bemærkes, at røgdetektorer der evt. tilsluttes til et AIA-anlæg ikke kan sidestilles med ABA, da alarmeringen ikke automatisk medfører udrykning.



2. Begreber

26. januar 2022
Side 5 af 28

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 service/kerneydelse til borgerne.



2.2. Aarhus Kommunes bygninger og lokationer

26. januar 2022
Side 6 af 28

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 af fællesfunktionen på ejendomsområdet.

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 (AIA, TVO, ADK 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 diagram¹:

Roller, opgaver og ansvar						
Mag. afd.	Ansvar i alle mag. afd.	Fællesfunktionen i Ejendomme, MTM				
MBU	Ejerskab til bygninger	Vedligehold/genopretning Klimaskærm, tekniske installationer	Rådgivning vedr. byggefaglige forhold, service mv. Tværgående koordinering	Ejendomssystemer, metoder og FM-system	Aa+ program	Energiledelse
	Planlægning					
MKB	Strategi, behov/organisering					
	Modernisering/forbedringer					
MSB	Indvendigt vedligehold					
	Visse installationer					
MSO	Fleste sikringsydelse					
	Forbrug – el, vand, varme					
MTM	Rengøring, service					
MBA	Krav vedr. teknisk netværk/opkoblede installationer. Personfølsomme oplysninger					

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



26. januar 2022
Side 7 af 28

3. Definitioner

Aarhus Kommune anvender definitioner for AIA-systemer for indbrudsalarmer, 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. Emner som f.eks. "Adgangsrettigheder", "Alarmnettet", "Centraludstyr" og "Skalovervågning" (listen over emner er ikke udtømmende) skal dermed hentes fra www.forsikringogpension.dk:

- Forsikring og Pensions "AIA-katalog"² med alle faneblade

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**. Systemejeren primære funktion er ansvar og økonomisk beslutningskompetence, og den som tegner systemet overfor såvel interne som eksterne interessenter. Systemejeren har bl.a. det overordnede ansvar for systemets anskaffelse og finansiering, for dets drift 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 AIA-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.

² <http://www.forsikringogpension.dk>



26. januar 2022
Side 8 af 28

Driftsoperatøren har som udgangspunkt ikke behov for at kunne tilgå streamede og lagrede data fra et AIA-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 interesse for Systemejeren.

Vagtcentralens ydelser er derfor afhængig af AIA-systemets tilgængelighed og funktionalitet.

Vagtcentralen kan efter behov tilgå lagrede data i alle AIA-anlæg, og operatørens adgang hertil skal reguleres af en databehandleraftale.

Eftersom Østjyllands Brandvæsens vagtcentral ikke er en rigspoliti godkendt kontrolcentral, vil der være enkelte anlæg som de ikke må modtage alarmer fra, som følge af krav herom.

Som udgangspunkt skal alle AIA-anlæg sende til Østjyllands Brandvæsen, hvis der skal afviges fra dette, kan det ikke ske uden forudgående dialog med MTM-Ejendomssystemer.

4.3. IT-Sikkerhedsområdeansvarlig

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 AIA-data, til Politiet i forbindelse med efterforskning.

Den IT-Sikkerhedsområdeansvarlige³ for en organisatorisk enhed, hvor der anvendes AIA-anlæg, er derfor en væsentlig interesse for Systemejeren, idet den IT-Sikkerhedsområdeansvarlige - bl.a. ud fra adgang til AIA-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 AIA-anlægget direkte i systemet eller gennem krypterede udtræk. Den IT-Sikkerhedsområdeansvarliges adgang til

³ Ønskes den it-sikkerheds områdeansvarlige kontaktet, benyttes: itsikkerhed@aarhus.dk



data kan tildeles fra sag til sag af den for magistratsafdelingens og systemets respektive systemejer.

26. januar 2022
Side 9 af 28

4.4. Administrative institutionsleder

Et AIA-anlæg sikrer typisk adgang til områderne på en adresse, og den administrative leder er derfor en vigtig interessent for Systemejeren, da den administrative leder definerer AIA-anlægs sikringsleverance, og er dermed også den primære betaler for det konkrete AIA-anlægs omkostninger.

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

Den administrative leder har behov for løbende at kunne tilgå og administrere data i AIA-anlægget.

4.5. Teknisk Servicemedarbejder

Det tekniske servicepersonale har behov for at kunne tilgå almindelige administrative data fra et AIA-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 AIA ikke falder ind under GDPR lovgivningen, da der ikke opbevares personhenførbare data. Der er desuden ikke pligt til at anmelde AIA-systemer på kommunens anmeldelsesportal.

En databehandling kan efter databeskyttelsesforordningen omfatte enhver håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfindning, 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 AIA-behov

26. januar 2022
Side 10 af 28

Ved etablering af AIA-anlæg skal bruger nøje overveje, det konkrete sikringsbehov samt de adfærdsmæssige begrænsninger, der ofte følger med, når der installeres et AIA-anlæg. Årsagen er, at mulighederne for funktionalitet og rolleinddeling i et AIA-system er under hastig udvikling, så en beskrivelse af brugerkrav og -adfærd er helt essentiel for en løsning, som tilgodeser både den teknologiske formåen, økonomi, databehandling, lagring og de reelle problemstillinger, man må ønske AIA skal hjælpe med at løse.

Det primære formål med et automatisk indbrudsalarmeringsystem er at sikre, at kun ønskede personer kan få adgang til et kontrolleret område. AIA-anlægget skal derfor alarmere kontrol-/vagtcentralen, hvis genstande, faciliteter m.m. kompromitteres af uønskede personer – eller hændelser, 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:

- Institutionstypen
- Sikringsniveauet
- Institutionens samlede værdier og generelle risikoprofil
- Forventning til uønskede personers midler og motivation for at omgå indbrudsalarmeringssystemet.

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 Sikringsniveauer og varegrupper⁴.

5.3. Forholdsordre

Forholdsordren 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.

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

⁴ <http://www.forsikringogpension.dk>



foretages en lovliggørelse af eksisterende netværk, komponenter, udstyr eller anlæg.

26. januar 2022
Side 11 af 28

AIA-anlæg og komponenter fra andre anlæg til at detektere og/eller verificerer alarmer, skal være installeret af en certificeret installatør i henhold til den gældende kravspecifikation for området.

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

- ADK-integration: Adgangskontrolanlægget udveksler data med et AIA-anlæg, 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 adgangskontrolanlæggets kort-læsere eller andet genkendelsesudstyr.
- TVO-integration: TV-overvågningsanlæg udveksler data med AIA-anlægget, f.eks. med det formål at kunne verificere personer, der ønsker adgang, eller med det formål at starte optagelser ved alarm fra AIA-anlægget.
- Anden integration: AIA-anlægget 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 AIA og andre systemer.
- Se specifikt Forsikring og Pension AIA-katalog fane 110⁵.

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

5.4. Find dit sikringsniveau

I forbindelse med afdækning og beskrivelse af brugerbehovet for AIA, bør det overvejes, hvilket sikringsniveau man ønsker at opnå. Der kan, af et forsikrings-selskab, af bygningschefen, igennem risikostyringsprogrammet eller af en bygningskonsulent, være defineret et ønsket risikoniveau for lokaletypen eller -funktionen, bygningen eller ejendommen.

På Forsikring & Pensions hjemmeside findes et værktøj til bestemmelse af sikringsniveauet for en institution, som hedder "Find dit sikringsniveau". Sikringsniveauet er et udtryk for den risiko, man gerne vil nedbringe med AIA.

Der er i alt seks sikringsniveauer, og hvert niveau beskriver nøje, hvilke krav der er til elektronisk alarmovervågning. Sikringsniveau 10 er det laveste niveau, og sikringsniveau 60 er det højeste.

⁵ <http://www.forsikringogpension.dk>



5.5. Beskrivelse af ydelsesgrænser

26. januar 2022
Side 12 af 28

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 åbningskontakter til døre og vinduer leveres under anden entreprise, så de monteres fra fabrikken.

Specielt anbefales det at tage kontakt til bygningsafdelingerne, MTM-Ejendomssystemer og til 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, skal afholdes af AIA-projektet og medtages i tilbuddet.

Aarhus Kommune forbeholder sig retten til at projektere og etablere nødvendigt IP-netværk fra AIA-systemets switch til net-distributørens kantrouter for transmission af evt. videosignal til Aarhus Kommunes kontrol-/vagtcentral(er).

6. Krav til leverancen

Ved indkøb af AIA-anlæg skal følgende krav opfyldes:

6.1. Datasikkerhed og standarder

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

- Alle service-, master- og administrationskoder/passwords skal vederlagsfrit udleveres til systemejeren
- AIA-systemer skal uden begrænsninger kunne serviceres af anden ISO 9001 AIA-certificeret installatør i henhold Forsikring & Pensions⁶ retningslinjer
- Installerede anlægsdele, komponenter mv. skal være standardvarer, som skal kunne anskaffes uafhængigt af AIA-entreprenøren
- AIA-centraler og øvrige komponenter skal være klassificeret i den udstyrsklasse der stilles af Forsikring & Pension i sikringsniveauerne eller tilsvarende i henhold til de europæiske standarder for alarmudstyr Jf. AIA-kataloget

⁶ <https://www.forsikringogpension.dk/>



26. januar 2022
Side 13 af 28

- AIA-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 "Installations- erklæring"⁷
- AIA-leverandør/installatør skal være ISO9001 godkendt

Anvender AIA-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.

AIA-entrepriser skal udføres af certificerede og dermed af faglært personale med relevante kompetencer.

6.2. Ejendomsret

Alle installerede AIA-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 AIA-anlægget, som hvis der var tale om ejerskab.

Koder til anlægget skal være registreret ved kontrol/-vagtcentralen, de er Aarhus Kommunes ejendom. Er disse af eller anden årsag ikke registreret, eller er det ikke de rette koder der er noteret, skal installatøren til en hver tid udlevere dem uden beregning.

Dette glæder alle koder der giver adgang til anlægget, masterkode, servicekode, login til pc/server, login til software etc.

6.3. Lovgrundlag og gældende forskrifter

AIA-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)
- Persondataforordningen

⁷ Se Bilag 1



- Anlægget skal opfylde bygherrens og Aarhus Kommunes øvrige politikker samt Forsikring og Pensions' forskrifter for AIA.

26. januar 2022
Side 14 af 28

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:

- Nyeste AIA-katalog⁸, fane 00 til fane 180, Forsikring & Pension
- Lov om vagtvirksomhed
- 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"
- AIA-kabling skal udføres iht. Aarhus kommunens "Kravspecifikation for IT-kabling" og tilhørende dokumenter.

7. Funktionelle krav til AIA-systemer

Aarhus Kommune har fælles administrative platforme for opkobling af AIA-systemer. Hvis det i et konkret udbud vurderes nødvendigt at etablere en opkobling på disse Fælles systemer til AIA, skal systemejeren for det pågældende bygningstekniske netværk inddrages i de designmæssige krav.

AIA-systemer skal, som udgangspunkt af bygningsejeren/bygherre, registreres i Aarhus Kommunes FM system. De oplysninger, som skal registreres, er alle data, som er nævnt i Installationserklæringen⁹: bruger, installationstidspunkt, installationstype, antal enheder, tegninger med placeringer.

⁸ <http://www.forsikringoopenion.dk>

⁹ Se Bilag 1



26. januar 2022
Side 15 af 28

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:

- Godkendte AIA-produkter: Se Forsikring og Pensions hjemmeside¹⁰
- Certificering af AIA-virksomheder: Indbrudsalarmanlæg, Kravsspecifikation - GES-2014-00273 Dok ID 344343 eller nyere.

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

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

De enkelte AIA-systemer projekteres teknisk af rådgiver eller den bydende virksomhed samt eventuelt i samarbejde med MTM-Ejendomssystemer, så AIA fabrikantens forskrifter er opfyldt sammen med de opgavespecifikke og aktuelle krav til de sikringskategorier, som ønskes. Ved integration i andre sikringsystemer skal der projekteres ud fra Forsikring & Pensions Suppleringskataloger 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.

¹⁰ <http://www.forsikringogpension.dk>



8. AIA-udstyr i Aarhus Kommunes IT-driftsmiljø

26. januar 2022
Side 16 af 28

8.1. Netværk og tjenester på netværk

AIA-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 NATning 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.

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.

26. januar 2022
Side 17 af 28

8.2. Servere og Workstations i Aarhus Kommunes driftsmiljø

8.2.1. Servere

Skal en AIA-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.

Alle medarbejdere i Aarhus Kommune, der med klientprogrammet til Workstations skal tilgå servere eller enheder i Bygningstekniske netværk, gør det fra deres administrative Windows10 pc tilsluttet administrativt netværk.

Installation af klientprogrammet skal ske med Aarhus Kommunes SCCM softwaredistributionssystem, og klientprogrammet 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

26. januar 2022
Side 18 af 28

8.3.1 I AIA-enheden

Lagres data i selve AIA-enheden, skal data – både når de beror i AIA-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 med databehandlingsaftale som 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 under transporten fra sensor 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

AIA-anlæg skal projekteres i henhold til Forsikring & Pensions AIA-Katalog, fane 030, og installeres af en Forsikring & Pension registreret og certificeret installatør.

9.1. Ny installation (arbejdets omfang)

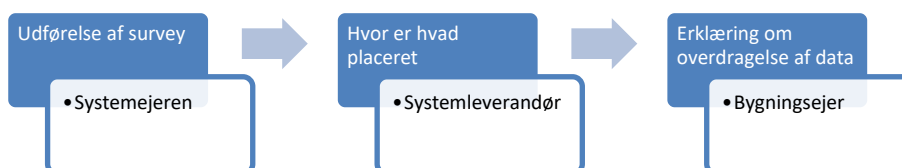
Indbrudsalarmanlæg, der er projekteret og installeret – i henhold til AIA-kataloget fra Forsikring & Pension - har det formål, at de automatisk skal registrere indbrud eller forsøg på indbrud så tidligt som muligt. Indbrudsalarmanlægget skal herefter afsende alarm til en kontrol-/vagtcentral, så en reaktion kan iværksættes og eventuelle følgeskader begrænses.

Under AIA-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 AIA-system. Adgang til lokationer aftales med projektlederen for projektet og brugerne af bygningen/bygningsejeren. Alle forhold omkring leveringstid og dokumentation aftales med bygningsejers projektleder.

Det er entydigt, det er installatøren, der er ansvarlig for og forestår alle installations- og montagearbejder på det lokalt tilbudte AIA-anlæg. Herunder forestår alle ydelser, der er nødvendige for den fulde konditionsmæssige udførelse og implementering samt test af det tilbudte AIA-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 AIA udføres et survey, hvor udstyrets 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



9.2. Udvidelse af anlæg

26. januar 2022
Side 20 af 28

Udvidelse af anlæg, hvor centraludstyret ikke længere er registreret hos Forsikring & Pension, kan ske med komponenter, der på installationstidspunktet for udvidelsen er registreret, hvis de fungerer sammen med eksisterende centraludstyr. Hvis det ikke er muligt, skal centraludstyret udskiftes.

Et AIA-anlæg bevarer sit sikringsniveau ved eventuelt brugerskifte til ny institution med samme krav til sikringsniveau. Hvis der efterfølgende stilles krav om et højere sikringsniveau, skal hele anlægget opfylde kravene på det pågældende tidspunkt. AIA-anlæg, der indeholder komponenter, der ikke længere er registreret hos Forsikring & Pension, kan ikke flyttes til anden adresse.

10. Service og Vedligeholdelse

AIA-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.

Efter garantiperiodens udløb - hensigtserklæring:

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

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

Serviceaftalen skal til en hver tid kunne opsiges af Aarhus Kommune, med maksimalt tre måneders varsel, og eventuelt tilgodehavende ved forudbetalt abonnement skal refunderes til Aarhus Kommune.

11. Garanti og kvalitet

Der skal som minimum gives en toårig totalgaranti på alt udstyr, programmel, komponenter og installationsarbejdet, 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:

26. januar 2022
Side 21 af 28

- Betjeningsvejledning, som muliggør betjening med et minimum af betjeningsfejl. Betjeningsvejledningerne skal udformes under hensyntagen til brugernes adgangsrettigheder, idet der henvises til Forsikring & Pension GES-2016-00172 Dok ID 372582 fane 060, Adgangsrettigheder – og AIA-katalog 2016, Fane 30 Anlægsprojektering.
- Beskrivelse af de hensyn brugeren skal tage til f.eks. detektorer med henblik på at minimere antallet af fejlalarmer.
- Anlægsdokumentationen skal udleveres til bygherre/bygningsejer, jævnfør punkt 50, i kravsspecifikationerne vedrørende certificering af AIA-installatørvirksomheder eller i overensstemmelse med EN 50131-1, jf. TS-50131-7.

Anlæggene skal være af en sådan kvalitet og robusthed, at u hensigtsmæssige nedbrud som manglende AIA-signal/visning, som skyldes systemtekniske forhold, maksimalt må udgøre 0,001% af samtlige driftstimer. AIA-systemets opetid 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-paradigme¹¹

For alle byggesager foregår aflevering af D&V materiale i MainManager. Ved nyetablering af anlæg, i større byggesager til en samlet udbudssum over 5 mio. kr., hvor der indgår bygningstekniske IT-netværk, stilles der krav om BIM-projektering.

Alt dokumentation skal leveres i elektronisk form af upload (PDF-dokumenter samt min. CAD-, Visio- eller BIM modeller som f.eks. Revit-tegninger) i henhold til Aarhus Kommunes IKT-paradigme, til enten Aarhus Kommunes FM-system eller arkivserver/projektweb⁶.

Følgende filformater anvendes i udvekslingen:

- Ikke redigerbare filer leveres i PDF-format og IFC for BIM modeller
- Redigerbare BIM-filer levers i originalformat samt låst neutralformat

¹¹ Informations- og kommunikationsteknologi. Link: <https://www.aarhus.dk/virksomhed/leverandoeer-til-os/krav-til-leverandoeer-af-bygge-og-anlaegsprojekter/ikt-bim-cad-og-dokumentation/>



12. Bilag 1 – AIA Installationserklæring

Erklæringen kan rekvireres som Word dokument på Ejendommens intranetportal under Ejendomssystemer.

26. januar 2022
Side 22 af 28

AIA-INSTALLATIONSERKLÆRING

ANLÆGSEJER/-BRUGER		ISO 9001-CERTIFICERET VIRKSOMHED	
Navn		Firmastempel	
Adresse		Installationsansvarlig	
Postnummer	By	F&P-registreringsnr.	
Driftsansvarlig	Telefon		

STAMOPLYSNINGER	
Installationsadresse	Adresse, postnummer og by
Installationsnummer	
Ejerforhold - Er anlægget:	<input type="checkbox"/> Ejet <input type="checkbox"/> Lejet/leaset eller lignende
Installationsstatus	<input type="checkbox"/> Nyinstallation <input type="checkbox"/> Udvidelse <input type="checkbox"/> Ændring/Dokumentation

VIRKSOMHEDENS SIKRINGSNIVEAU
Anfør sikringsniveau og sikringsform (S, C eller O) for de berørte områder i bygningen, f.eks. udstillingsbåle, butik, lager på 1. sal, serverrum, lokale 10.4 etc. Se et eksempel på udfyldning af skemaet i vejledningen side 3.

Sikringsniveau	Sikringsform	Beskriv bygningens eller lokalets art og beliggenhed

SIKRINGSRAPPORT OG TEGNINGER	
Er der udarbejdet sikringsrapport af forsikringselskabet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nej
Er der udarbejdet tegninger med grænseflader for det/de fastlagte sikringsniveau(er)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nej

FORSIKRINGSSELSKAB OG KONTAKTPERSON	
Forsikringselskab og evt. kontaktperson	Policensnummer

Undertegnede forsikringstager bekræfter ved min underskrift hermed, at ovenstående stamoplysninger, baseret på de af forsikringselskabets fastsatte sikringsniveauer, er korrekte. Endvidere forpligtes jeg ligeledes ved min underskrift at sikre, at installationsomfanget eller AIA-anlæggets funktion ikke forringes ved bygnings- og indretningsmæssige ændringer. Endeligt er jeg blevet gjort opmærksom på, at ethvert sikringsniveau også stiller krav til den mekaniske sikring.

Dato	Anlægs ejerens/brugerens underskrift

INSTALLATIONSOPLYSNINGER	
Installation udført iht. Forsikring og Pensions AIA-katalog og "kravspecifikationer - Certificering af AIA-installationsvirksomheder"?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja
Er salg, projektering og installation foretaget af personale med dokumenteret kendskab til AIA-anlæg?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja
Aftale med kontrolcentral?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja, hvilken? <input type="text"/>
Type af alarmoverførsel til KC?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja, hvilken? <input type="text"/>
Aftale med certificeret vagtfirma?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja, hvilken? <input type="text"/>
Alarmverifikation (V-AIA)?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja, hvilken? <input type="text"/>
Evt. integration med andre anlæg?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja, hvilken? <input type="text"/>
Har forsikringselskabet stillet krav om supplerende sikring?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja, se bilag: <input type="text"/>
Er der anvendt underleverandør?	<input type="checkbox"/> Nej <input type="checkbox"/> Ja, skriv navn og certifikatnr.: <input type="text"/>
Dato	Underskrift af ISO 9001 AIA-certificeret virksomhed

AFLEVERING AF ANLÆG (Sikringsniveaues krav til mekanisk sikring er ikke omfattet af denne erklæring)	
Anlægget er solgt og installeret således at det overholder:	<input type="checkbox"/> Forsikring & Pensions sikringsniveauer og kravspecifikation for AIA-installatørvirksomheder
Dokumentation afleveret til kunde:	<input type="checkbox"/> Brugermanual <input type="checkbox"/> Placeringstegn <input type="checkbox"/> Systemdiagram <input type="checkbox"/> Systemdele <input type="checkbox"/> Drifts- og vedligeholdelsesvejledning
Træning/undervisning	<input type="checkbox"/> Bruger <input type="checkbox"/> Superbruger
Afprøvning	<input type="checkbox"/> Afprøvning i.f.m. idriftsættelse
Mangelliste	<input type="checkbox"/> Nej <input type="checkbox"/> Ellers dateret: <input type="text"/>

DRIFT	
Vedligeholdelseskontrakt	<input type="checkbox"/> Ingen <input type="checkbox"/> Helårige* <input type="checkbox"/> Interval <input type="checkbox"/> Fuld service og vedligeholdelse <input type="text"/>
*) I henhold til Forsikring & Pensions AIA-katalog fane 120 skal anlægs ejer/bruger indgå eftersynsaftale med registreret AIA-installatør	

Hermed bekræftes rigtigheden af ovenstående oplysninger.		Hermed bekræftes, at aflevering er godkendt, og at der er rådgivet om ovenstående.	
Dato	Certificeret AIA-installatør	Dato	Anlægs ejer/lejer



13. Bilag 2 – Ydelsesgrænser

26. januar 2022
Side 23 af 28

IT-indholdet i sikringsinstallationer øges markant, og udviklingen vil 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 faser¹² svarende til et normal 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 Ejendommens 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

¹² Hjælpeskemaet kan ikke benyttes som hovedfaser ifm. rådgivning jfr. ABR §11



Fase 1: Projektering

26. januar 2022

Side 24 af 28

nr.	Ydelse	Bygherre				Entreprenører				Service - providere		Rådgiver		
		Projektsansvarlig	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 - Initiierer

O - Orienteres

U - Udfører



Fase 2: Projektstart

26. januar 2022
Side 25 af 28

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



Fase 4: Aflevering og drift

26. januar 2022

Side 27 af 28

nr.	Ydelse	Bygherre				Entreprenører				Service - providere		Rådgiver		
		Projektsansvarlig	Sikringsansvarlig	IT-ansvarlig	Andet	Managementsystem	Sikringsanlæg	IT kabling	IT udstyr	Telefon	Internet	Projektleder	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													
	Dokumentation 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/driftprøvningsperiode	U	U	U								I		
30	Afhjælpning af fejl og mangler					U	U	U	U			I		G
31	IT (fejltrening)					U	U	U	U			I / G		
	NETVÆRK (LAN/WAN)													
	Fejltrening af installation og opsætning fra fase 3					U	U	U	U			I/G		
	HW													
	Fejltrening af installation og opsætning fra fase 3					U	U	U	U			I/G		
	SW													
	Fejltrening af installation og opsætning fra fase 3					U	U	U	U			I/G		
	DATASIKKERHED													
	Fejltrening af installation og opsætning fra fase 3					U	U	U	U			I/G		
32	Afslutning af testperiode/endelig idriftsættelse (fejltrettet 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	Evaluerings	D	D	D			(D)		(D)			I	D	
39	Slurrapportering	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				



Fase 5: 1 & 5-års gennemgang

26. januar 2022
Side 28 af 28

nr.	Ydelse	Bygherre				Entreprenører				Service - providere		Rådgiver		
		Projektsvarlig	Skrivingsvarlig	IT-ansvarlig	Andet	Managementsystem	Skrivingsanlæg	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	
	Viruskanner: 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 service rapporter	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	