# Kravsspecifikation
# for
# BTN-VRF

| Dato | Forfatter | Firma | Version | Handling |
|---|---|---|---|---|
| 25-05-2021 | AZ33430 | Aarhus Kommune | 0.0 | Oprettet |
| 26-05-2021 | AZSBAI9 | Aarhus Kommune | 0.1 | Tilføjet punkter under kravspecifikation |
| 22-05-2025 | AZSBAI9 | Aarhus Kommune | 0.2 | Rettelser og opdateringer af dokumentet |
| 20-06-2025 | AZSBAI9/ AZ33430 | Aarhus Kommune | 0.3 | Tilrettet alle afsnit ift. AaE/AaK |
| 03-10-2025 | Ejendomme + FIDI | Aarhus Kommune | 0.4 | KS fra Ejendomme og FIDI |
| | | | | |
| | | | | |

## Resumé

Dette dokument omhandler obligatoriske generelle krav til administration og benyttelse af og opkobling til det Bygningstekniske Netværk herefter benævnt BTN-VRF. Denne kravspecifikation tager sit udgangspunkt i Aarhus kommunes IT-Politik for BTN-VRF som er udarbejdet af Fælles IT og Digitalisering (FIDI) i samarbejde med Sikringsydelser.

BTN-VRF er et netværk (VRF) som er tilbudt og driftet af Fælles IT og Digitalisering, og hvis formål er at være et fælles kommunalt netværk som kommunens magistratsafdelinger skal benytte til opkobling af tekniske enheder ud fra nærmere bestemte kriterier.
Behovet for generelle krav til BTN-VRF er opstået på baggrund af et ønske i Aarhus Kommune om standardisering af tekniske krav.

Der opleves en tilvækst og øget variation i bygningstekniske installationer, hvilket betyder at indkøb, kontrahering, systemejerskab, applikationer, sikkerhedshåndtering mv. samlet set er kompleks. Formålet med standardisering af krav er, at de rette krav stilles, og at driftshåndteringen bliver mere sikker og effektiv og samtidig nedbringe såkaldt teknisk gæld.

Nærværende kravspecifikation er blevet til i samarbejde mellem FIDI og Sikringsydelser til gavn for Aarhus kommune. Med vedtagelse af denne kravspecifikation er det obligatorisk, at magistratsafdelinger som opkobler, ændrer, køber eller installerer sikringsydelser eller tilhørende leverancer følger nærværende krav til netværk og deres systemer hhv. platforme samt stiller tilhørende design- og produkt/leverandørkrav mv. Kravspecifikationer kan generelt findes på Aarhus Kommunes intranet under ”Sikringsydelser” eller på kommunens hjemmeside under ”Krav til tekniske installationer”.

# Indhold

# 1. Indledning

Aarhus Kommune fastlægger igennem dette dokument en kravspecifikation for BTN-VRF, hvorved Kommunen vurderer dels de nuværende tekniske systemer dels italesætter risici ved forskellige skadescenarier og muliggør prioriteringer.
Succeskriteriet for denne kravspecifikation er, at bestillere i Aarhus Kommune vælger og indbygger tekniske løsninger, som opfylder Aarhus Kommunes krav på området. Et afledt succeskriterie er at begrænse antallet af hændelser og skader og dermed nedbringe mulig skade. Heraf følger, at når BTN-VRF benyttes muliggøres overvågning, og dermed tidligt hæmme og melde, og dermed vil have en nedbringende virkning.

Formålet med at benytte et BTN-VRF er at give bygningsejer eller dennes repræsentant, mulighed for at følge og opstille fælles regler som virker på tværs af Kommunen, og dermed mulighed for at opstille en standardiseret tilgang til opkobling til BTN.
Ved benyttelse af BTN-VRF kan der dokumenteres hændelser, som finder sted i det overvågede område fx igennem observation, verifikation og identifikation. BTN-VRF er ikke lovreguleret men er med til at sikre fx GDPR.

BTN-VRF benyttes blandt andet i forbindelse med følgende sikringssystemer:

- Tv-overvågning (TVO)
- Automatisk indbrudsalarmering (AIA)
- Adgangskontrol (ADK)
- Automatisk brandalarmering (ABA)
- Bygningers tilstandskontrol (BMS/CTS)

BTN-VRF benyttes blandt andet i forbindelse med følgende tekniske systemer:

- Overfaldsalarmer
- Kassesystemer
- Billetsystemer
- Vejrtjenester
- Trafik
  Listen er ikke udtømmende

# 2. Begreber

## 2.1. Aarhus Kommunes Organisation

Magistratsafdeling
Aarhus Kommune er udover borgmesterens afdeling opdelt i 5 Magistratsafdelinger:

- 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.

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.

Institution/enheder
En forvaltning kan drive en eller flere Institutioner/enheder, der yder en specifik kommunal service eller sikrer et tilbud til borgerne.

### 2.2. Aarhus Kommunes IT-Net, 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 for Fælles IT og Digitalisering i borgmesterens afdeling udgør Kommunens fællesfunktion på IT-området og rådgiver om og drifter kommunens it-infrastruktur, herunder BTN-VRF.

Afdelingen Ejendomme i Teknik og Miljø udgør Kommunens fællesfunktion på ejendomsområdet og rådgiver om - og varetager vedligehold og genopretning af klimaskærm, tekniske anlæg og udenoms arealer for hovedparten af de kommunale bygninger. Derudover håndteres og rådgives om byggetekniske- og planmæssige forhold samt service og drift.
I Aarhus Kommune stilles der krav om varetagelse af systemejerskab på sikringstekniske anlæg. Systemejerskab reguleres af Governance for Systemejerskab og tilhørende bilag. Som en direkte følge deraf varetages administration af BTN-VRF af systemejere.
Hver magistratsafdeling administrerer og håndterer en række bygninger, og håndterer ejer/lejer-, drifts-, vedligeholdelses- og serviceansvar for disse bygninger, samt om- til- og nybyggeri.

## 3. Definitioner

Aarhus Kommunes anvender definitioner for brugen af BTN-VRF, herunder hvilke typer af enheder der må tilsluttes og hvilke netværkskommunikationer der tillades og ikke tillades. Desuden er det i Aarhus kommune (AaK) besluttet at alle enheder der tilkobles BTN-VRF skal være registreret internt i AaK, knyttet til en systemejer i AaK, et

godkendt system og netværksgodkendes fx via Cisco ISE, således ikke godkendte netværks opkoblede enheder udelukkes for tilslutning.

# 4. Roller

## 4.1. Driftsoperatør, systemejer, systemleverandør

**Driftsoperatøren af det logiske netværks infrastruktur** er i Aarhus Kommune "It-infrastruktur" i Borgmesterens afdeling, eller det firma, der har en driftsaftale med Fælles Service. Driftsoperatøren/"It-infrastruktur" leverer drift af LAN og WAN, servere, print og arbejdspladser.

Driftsydelsen aftages af **Systemejere.** Systemejerens primære funktion er ansvar og økonomisk beslutnings kompetence, 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 og support, for rettighedsstyringen, for overholdelsen af interne retningslinjer og lovkrav, for dialogen med alle interessenter for dokumentation og for systemets rettidige udfasning. Systemejeren varetager desuden den fulde administration af BTN-VRF, herunder hvilke typer af enheder der kan godkendes, kontrolleres og tilsluttes og fastlægger derigennem systemets tilgængelighed og funktionalitet, og er ansvarlig for databehandleraftaler til driftsoperatør og vagtoperatør som er tilsluttet BTN-VRF.

En **systemleverandør**, er en leverandør af den systemtekniske installation eller ydelse, og vil typisk have den tekniske dialog om 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 lagrede data fra et system, 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 for BTN-VRF

Eksternt firma er af Fælles IT og Digitalisering udpeget til at overvåge den logiske og fysiske sikkerhed i og omkring BTN-VRF, og kan dermed fungere som vagtoperatør. Vagtoperatørens ydelse er derfor afhængig af BTN-VRF nettets tilgængelighed og funktionalitet, og Vagtoperatøren er derfor en væsentlig interessent for Fælles IT og Digitalisering og Systemejeren. Vagtoperatøren har behov for at kunne tilgå lagrede data i alle servere på BTN-VRF, og operatørens adgang hertil skal reguleres af en databehandleraftale. I normal arbejdstid kontaktes Fælles IT og Digitalisering på 89 40 11 11.

### 4.3. IT-Sikkerhedsområdeansvarlig

Aarhus Kommune håndterer de forhold der vedrører Persondatalovgivningen i en særskilt IT-Sikkerhedsorganisation. Fx. sager vedr. aktindsigt og Borgerens rettigheder til egne data og udlevering af logdata - herunder BTN-VRF-data.
Den IT-Sikkerhedsområdeansvarlige[1] for en organisatorisk enhed, hvor der anvendes BTN-VRF er derfor en væsentlig interessent for Fælles IT og Digitalisering, idet den IT-Sikkerhedsområdeansvarlige - bl.a. ud fra adgang til BTN-VRF-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 BTN-VRF-nettet. Den IT-Sikkerhedsområdeansvarliges adgang til data kan tildeles fra sag til sag af den for BTN-VRF nettets respektive systemejer.

### 4.4. Administrative institutionsledere

Et BTN-VRF benyttes typisk i én, flere eller alle bygningerne i en institution, og den administrative institutionsleder, eller den teknisk ansvarlige i Ejendomme, er derfor en vigtig interessent for Systemejeren, da den administrative institutionsleder er den primære aftager af det konkrete BTN-VRF's leverance.
Den administrative institutionsleder, eller den teknisk ansvarlige i Ejendomme, er også en vigtig interessent for den IT-sikkerhedsområdeansvarlige, idet dialog om en eventuel politianmeldelse på basis af misbrug initieres af den administrative institutionsleder.

### 4.5. Teknisk Servicemedarbejder

Den tekniske servicepersonale på en AaK-lokation har behov for at kunne tilgå indkøbte tjenester som serviceres via BTN-VRF, men har ikke nødvendigvis behov for at kunne tilgå lagrede personlige data. Begrænsninger reguleres af Systemejeren.

## 5. Ikke funktionelle krav til leverandør, entreprenør og rådgivere, afklares inden udbud

### 5.1. Persondataforordningen (GDPR)

GDPR foreskriver, at der ved relevant forespørgsel er udleveringspligt for Aarhus Kommune. Udleveringspligten gælder adgang til lagrede data.

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

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

Databeskyttelsesrådgivning:
Som følge af databeskyttelsesforordningen har Aarhus Kommune en databeskyttelsesrådgiver (DPO)[2], som varetager: Underretning og rådgivning om behandling af personoplysninger og de medfølgende forpligtelser; Overvågning af overholdelse af forordningen, anden EU-ret og national ret om databeskyttelse og overvågning af politikker om beskyttelse af personoplysninger. I tvivlsspørgsmål kan DPO'en rådgive om konsekvensanalyser.

Aktindsigt og mistanke om kriminel hændelse:
Systemejeren for BTN-VRF skal kunne tildele en Systemejer, IT-områdeansvarlig og/eller en institutionsleder tidsbegrænset læse - og kopierings adgang til relevante data for et fælles system i en given periode. Dette sker på baggrund af en autentificering via et teknisk-AD, som kun benyttes til systemer der serviceres via BTN-VRF, som sikrer at brugeren er den person som brugeren udgiver sig for at være.

Anmeldelse:
Det er Fælles IT og Digitaliserings rettighed at anmelde brud på BTN-VRF inden ibrugtagning. Systemejeren har formelt ansvaret for at sikre, at der forefindes metoder og processer for registrering af anmeldelser, men alle med en AZ-ident har et ansvar for at indmelde et brud på BTN-VRF.

## 5.2. Beskrivelse af BTN-VRF-behov

Ved etablering og benyttelse af BTN-VRF skal det overholde Governance. Årsagen er, at mulighederne for funktionalitet og rolleinddeling i et BTN-VRF-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 måtte ønske BTN-VRF skal hjælpe med at løse.

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

- Institutionstypen
- Sikringsniveauet
- Institutionens generelle risikoprofil

[2] E-mail: databeskyttelsesraadgiver@aarhus.dk

- Forventning til uønskede personers midler og motivation for at omgå adgangskontrolsystemet

Behovsvurderingen skal også på et overordnet niveau beskrive BTN-VRF-rolle i institutionens samlede sikringsløsning, eller hvordan BTN-VRF-nettet indgår i institutionens samlede sikringsløsning.

## 5.3. Funktionsgruppe: Fælles Sikringssystemer

Ved valg af endelig løsning som skal opkobles på BTN-VRF skal det som minimum afklares hvilke forhold som kan have indflydelse på BTN-VRF - herunder:

- Oppetid
- Overvågning
- Organisation
- Nød drift og aktiv stillingtagen til plan for beredskab
- Kontaktpersoner
- Detailprojektering af det samlede anlæg, inkl. udarbejdelse af installationstegninger der viser komponentplacering og kabeltræk, tilslutningsdiagrammer og nødvendige blokdiagrammer samt beregning af netværksbelastning.
- Levering og installation af de tilbudte komponenter.
- Idriftsætning og funktionsafprøvning af de opkoblede enheder/systemer.
- Datablad med komplet stykliste og opsummering af samtlige enheder med angivelse af fabrikat, model, type, version samt leverandør.
- Dokumentation, og installationserklæring skal leveres i trykt form samt på digitalt medie jfr. kommunens retningslinjer til Digital aflevering.

Listen er ikke udtømmende.

## 5.4. Change management

Change management er et digitalt internt sagsforløb, i Aarhus Kommunens ServiceNow instans, som beskriver den ønskede reaktion i tilfælde af en planlagt hændelse registreret på BTN-VRF. Herunder reaktion ved integration af BTN-VRF i andre systemer.
En Change Management sag initialiseres enten af systemejeren eller af Fælles IT og Digitalisering. En Change kan være opdatering / opgradering af fx switche, infrastruktur eller opdatering af en given tjeneste på en specifik systemydelse som leveres via BTN-VRF. Relevante aktører / leverandører / Aftagere af tjenesten kan via Change Manager informeres. SinglePoint of Contact vil altid være Change Manager.

**Incident management**
Ved drift-forstyrrelser, nedbrud, cyber angreb mv. der kan ramme systemer og / eller selve BTN-VRF-segmentet i AaK oprettes der, via Fælles IT og Digitalisering, en Incident management, så der registreres tiltag, impact som efterfølgende kan danne grundlag for afrapportering ved større hændelser.

### 5.5. Sikringsniveau

I forbindelse med afdækning og beskrivelse af brugerbehovet for BTN-VRF, bør det overvejes, hvilket sikringsniveau man ønsker at opnå. Der kan, af et forsikringsselskab, af bygningschef, igennem risikostyringsprogrammet eller af en bygningskonsulent, være defineret et ønsket risikoniveau for lokaletypen eller -funktionen, bygningen eller ejendommen. Som vejledning til at finde dit sikringsniveau er der på Forsikring & Pensions hjemmeside et værktøj til bestemmelse af sikringsniveauet for en institution som hedder ”Find dit sikringsniveau”.

### 5.6. Beskrivelse af ydelsesgrænser

Det anbefales generelt, at ydelsesgrænser imellem bruger- og sikringsbehov, teknologiske ønsker, bygherrer, rådgiver, service-provider og entreprenør nøje beskrives inden igangsætning af et projekt.
Udgifter til den nødvendige infrastruktur, IT- kabling, switche som vurderes nødvendige for tilslutning til BTN-VRF skal afholdes af projektet og medtages i tilbuddet. Fælles IT og Digitalisering og Sikring ydelser skal altid inddrages i denne proces, da der kan være andre interessenter der også er aftagere tjenester på infrastrukturen i den samme bygning / lokation. Der er igennem kommunens udbud valgt specifikke leverandører til IT-kabling som ikke nødvendigvis er de samme som leverandører som har vundet generelt el / elektriker arbejde via udbud. Valg af leverandør af IT-kabling skal altid rekvireres og afklares via Fælles IT og Digitalisering og hertil oprettet Bestillingsformular i Aarhus Kommunes ServiceNow system. En bestilling i ServiceNow kan kun initialiseres af en kommunal medarbejder og aldrig af en leverandør. Der foreligger separat kravspecifikation på IT-kabling i Aarhus Kommune som leveres af Fælles IT og Digitalisering.
Aarhus kommune forbeholder sig retten til at projektere og etablere nødvendigt IP-netværk fra BTN-VRF nettets switch til net distributørens kantrouter for transmission.

## 6. Krav til leverancen

### 6.1. Datasikkerhed og standarder

Ved ibrugtagning af, og drift og indkøb til BTN-VRF skal følgende krav stilles til leverancen:

- Installerede anlægsdele, komponenter mv. skal være standardvarer, som skal kunne anskaffes uafhængigt af entreprenøren
- Ved valg af komponenter skal det sikres og dokumenteres ved leverandør, at disse som minimum er lagervare og kan supporteres i mindst 2 år, fra installationen er idriftsat og godkendt og Kommunen
- Leveres der en sikringsydelse er der krav om minimum ISO9001 godkendelse

- Netværksopkoblede enheder skal opfylde og understøtte 802.1x og DHCP-tildeling af IP-adresse som konsekvent styres af Systemejer af BTN-VRF. Netværks opkoblede enheder må aldrig tilsluttes i serieforbindelse, hver enkelt enhed skal have eget dropstik som tilsluttes direkte i AaK (kommunal) switch. Der må ikke benyttes switche, routere og lign. indbygget i en løsning
- Enheder må aldrig kunne initialisere en separat VPN-opkobling, ej heller kunne tilgås udefra via af AaK' ikke godkendte opkobling. TeamViewer, "Tosy-Box" ol. produkter accepteres ikke og understøttes ikke
- En Leverandør må aldrig opsætte egne switche, routere, gsm modem etc. På kommunens netværk, ej heller indirekte igennem tekniske enheder
- Alle netværk opkoblede enheder skal, hvis enheden udbyder et netværksbaseret interface (fx. https), skal som minimum være beskyttet af login og password som ikke er default indstillinger og sådanne logins skal fremsendes til Systemejer. Systemejer har til enhver tid ret og pligt til at kunne ændre sådanne login oplysninger. Enheder skal altid have installeret den seneste firmware fra leverandør ift. Sikkerhedspatches. Det er leverandørs forpligtigelse at informere systemejer i AaK, når der foreligger en firmware opdatering der er releasede fra leverandør til den enkelte netværksenhed
- Systemejer af BTN-VRF forbeholder sig retten til at frakoble / u-autorisere netværksopkoblet enheder der ikke er opdateret eller skønnes at kunne udgøre en sikkerhedsrisiko. Det er den enkelte systemejer af et givent system der har ansvaret for at udrede og optimere en sådan enhed i samråd med leverandøren, for systemejers betaling
- Godkendte systemer / enheder vil kunne tilgås via kommunens egen godkendte adgangs løsning, hvor adgangen er personlig og tilknyttet den enkelte brugers personlige NEMID. En tildelt adgang må aldrig overdrages til 3.mand. Adgangen er ikke et krav der kan stilles fra leverandør – men kan tilbydes hvis en sådan adgang er nødvendig ved drift, support etc. Typen af tilbudt adgangsløsning kan til enhver tid ændres af AaK. Evt. Ændring af adgangsmetode og en leverandørs evt. Udgifter hertil er kommunen uvedkommende
- Adgang til systemer kan ikke stilles som et krav fra leverandør eller slutbruger. En indkøbt ydelse / leverance må ikke være afhængig af udefra kommende uautoriseret adgang, hverken via et eksternt system (f.eks. en cloudløsning) eller via en enkelt person. Inden indkøb af systemer skal rettigheder og nødvendige netværksressourcer afklares i samråd med BTN-VRF-ejer (Sikringsydelser i Aarhus Ejendomme) og godkendes af denne
- Der er obligatorisk at kontakte sikringsydelser og Fælles Service via ServiceNow allerede i designfasen.

## 6.2. Ejendomsret

Alle installerede BTN-VRF-net og systemer skal som udgangspunkt være ejede, dvs. Aarhus Kommunes ejendom efter installation. Der må således ikke installeres leaset udstyr. Hvis der er knyttet software licenser til et givent produkt skal disse udleveres til

Aarhus Kommune på forlangende, hvis disse er nødvendige for support, drift og sikkerhedsopdateringer / sikkerheds audits.
I bygninger der ikke ejes af Aarhus Kommune, skal Kommunen have fuld brugsret og være systemejer og bestyrer af BTN-nettet som hvis der var tale om ejerskab.

Adgangskoder og logins til alle opsatte netværksenheder og system komponenter er Aarhus Kommunes ejendom. Koder skal altid oplyses ved systemets idriftsættelse og kunne ændres af Kommunens systemejer. Det er systemejers og leverandør forpligtigelse altid have sådanne logins registeret i et beskyttet register.
Er disse af eller anden årsag ikke registreret, eller er det ikke de rette koder der er noteret, skal installatør til en hver tid udlevere dem uden beregning.
Dette glæder alle koder der giver adgang til netværk, porte, switche, masterkode, servicekode, login til pc/server, login til software etc. Og licenser.

### 6.3. Lovgrundlag og gældende forskrifter

BTN VRF-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
- Den til enhver tid gældende EU-forordning, direktiver, dekreter mv.

Herudover er følgende standarder gældende i nyeste version:

- Gældende bygningsreglement
- Arbejdstilsynets gældende forskrifter og meddelelser mv.
- Fælles IT og Digitalisering og digitaliserings (FIDI) IT-politik, som bl.a. er beskrevet i nyeste version af "Kundens IT-miljø" (rekvireres hos FIDI Kundens It-Miljø (EMN-2023-008178))
- BTN-kabling er underlagt kravspecifikation for IT-kabling, og de tilhørende dokumenter.

## 7. Funktionelle krav til BTN-systemer

Aarhus kommune har en fælles platform til opkobling på BTN-VRF.
Hvis det i et konkret udbud vurderes nødvendigt at etablere opkobling på dette Fælles BTN-VRF, skal systemejeren og sikringsydelser i ejendomme for det pågældende bygningstekniske netværk inddrages i de designmæssige krav.
Hvis løsning er Server afhængig skal denne oprettes og driftes på AaK egen infrastruktur. AaE tilbyder en virtuel server platform i kommunens eget interne miljø. En af

leverandør leveret fysisk server tillades ikke. Som udgangspunkt leveres der en standard windows2022 server platform som er domainjointet til BTN-VRF tekniske AD.

## 7.1. Krav om administration af BTN-VRF

Enheder skal altid godkendes og registreres inden tilslutning af den kommunale systemejer. Godkendelse af tilslutning af udstyr foretages kun af Sikringsydelser i Ejendomme. Sikringsydelser (systemejer af BTN-VRF) forbeholder sig retten til at afvise udstyr der ikke kan godkendes eller ikke opfylder de tekniske krav jf. pkt. 7.2 og 7.3
Systemkomponenter skal placeres på Aarhus Kommunes bygningstekniske netværk, der er et lukket særskilt BTN-VRF i Aarhus Kommunes IT-infrastruktur, hvorfra der kun er adgang til andre netværk igennem kommunens firewall til andre AaK VRFs. Regler herfor styres konsekvent af Systemejer på BTN-VRF i samråd med Fælles IT og Digitalisering.
Leverandør må aldrig opsætte og tilslutte eget VPN eller netværks udstyr, lokale switche, acces points etc. på kommunens IT-infrastruktur. Enheder der er en del af det leverede system må aldrig kunne agere som en netværkskomponent: wi-fi acces point, router eller lign. En netværksopkoblet enhed skal udelukkende kommunikere via netværket via IP-trafik internt i Aarhus Kommune til / fra enheder, server i det samme system. Hvis en opsat enhed laver støj eller påvirker driften af andre systemer forbeholder Aarhus Kommune sig at frakoble sådanne enheder fra netværket.

## 7.2. Opkobling til Aarhus Kommunes Fælles BTN-VRF

Tilkobling til det kommunale BTN-VRF (det bygningstekniske net i AaK) skal altid foregå via kontakt til sikringsydelser i Ejendomme. Inden tilslutning / installation fremsendes MAC adresser på ønsket tilkoblet udstyr. Efter modtagelse registreres de enkelte enheder i AaK og der returneres besked til leverandør omkring registrering og tildelt IP-adresse. Enheder skal som udgangspunkt sættes til DHCP. Der må ikke benyttes eksterne DNS server adresser på udstyret. DNS, Gateway tildeles via DHCP. Hvis udstyr ikke kan håndteres DHCP oplyses IP-adresse, Subnet, Gateway og DNS til installatør.
Der må ikke tilsluttes lap tops, servere og lign til det tekniske net. Kun godkendte registrerede enheder må tilsluttes.
Enheder kan/må ikke tilsluttes via Wi-Fi men skal altid være tilkoblet via LAN kabling.

## 7.3. Tekniske specifikationer

Enheder skal understøtte og overholde 802.1x og DHCP-protokol. Firmware skal altid være seneste releasede version hvis det ikke påvirker drift.
Sikkerhedspatches til udstyr og software skal altid være opdaterede. Det påhviler leverandøren at informere om og installere sikkerhedspatches hvis det ikke påvirker driften negativt. Det skal altid afklares med systemejeren inden en opdatering igangsættes.

Enheders netværks opsætning:

- Enheder skal opsættes til DHCP

- Enheder må først tilsluttes når enhedernes MAC adresser er registreret og reserveret i AaK interne systemer af system ejer. Hvis enheder er tilsluttet inden klar melding fra systemejer i AaK, er det leverandørs pligt og u. omkostning for AaK at ændre opsætning på enhederne til det foreskrevne. Tildeling af IP-adresser styres af AaK
- Der må ikke benyttes Ipv6 på enheder (hvis installeret, skal det deaktiveres)
- Enheder der ikke understøtter 100 Mbits eller derover, må og kan ikke tilsluttes. (fx. ældre enheder som kun understøtter 10 Mbits kan ikke tilsluttes)
- Enheder skal understøtte DHCP protokollerne BOOTP eller Windows DHCP
- Enheder skal understøtte 802.1x protokollen således AaK´s netværksudstyr kan autentificere den enkelte enhed. Hvis enheden teknologisk ikke kan understøtte denne protokol, kan der gives dispensation herfor
- Hvis enheder bruger PoE fra AaK's switche skal der inden tilslutning afklares om der skal opsættes ekstra bestykning af switche pga. PoE strømforbrug. Switche må kun bestilles, indkøbes og opsættes af AaK netværksleverandør. Enheden skal opsættes så den svarer på ICMP (ping) forespørgsler.

Certifikater på tjenester:
Hvis en webbaseret løsning udbydes af et givent system, Skal dette understøtte https på port 443 og have et af AaK udstedt Certifikat installeret.
Http (usikker) tillades ikke.
Certifikater leveres som PFX-certifikater og er Root godkendt intent i AaK af egen CA Root udsteder og opdateres automatisk på den enkelte server herefter. Levetiden for et af AaK udstedt certifikat er 12 mdr.
Hvis løsning skal opdateres manuelt via af andre certifikattyper – skal leverandør foreså eksport til fx PEM-format og installation / opgradering af dette på den udstillede tjeneste. Der må aldrig benyttes "selfsigned" certifikater på en webtjeneste. Det påhviler leverandør at opdatere certifikatet i samarbejde med systemejeren i AaK inden udløb eller ved opdatering uden ekstra omkostninger da dette ses som en del af driften af det leverede system.
Alle netværks opkoblede enheder skal, hvis enheden udbyder et netværksbaseret interface (fx. https), som minimum være beskyttet af login og password som ikke er default indstillinger og sådanne logins skal fremsendes til Systemejer.
Systemejer har til enhver tid ret og pligt til at kunne ændre sådanne login oplysninger.
Enheder skal altid have installeret den seneste firmware fra leverandør ift. Sikkerhedspatches. Det er leverandørs forpligtigelse at informere systemejer i AaK, når der foreligger en firmware opdatering der er releasede fra leverandør til den enkelte netværksenhed.

# 8. BTN-udstyr i Aarhus Kommunes IT-driftsmiljø

## 8.1. Netværk og tjenester på netværk

Der understøttes som udgangspunkt IKKE site2Site til leverandør medmindre der ikke er mulighed for at hoste tjenester internt på kommunens infrastruktur, herunder serverplatform. Det prioriteres at en løsning kan hostes på kommunens egen virtuelle server platform.

Enheder der er tilkoblet AaK BTN-VRF, må og kan ikke multicaste trafik til/fra hinanden. En leveret løsning må derfor ikke være afhængig af brugen multicast på netværket.
Der kan etableres intern adgang til andre interne netværk i Aarhus Kommunes infrastruktur, gennem firewallregler hvis AaK skønner dette er nødvendigt for drift af systemet. Det er kun AaK der bestemmer, opsætter og vedligeholder disse regler.

Leverandøren kan få adgang til udstyret på BTN-VRF via:

- Personlig 2 faktor adgang til kommunens udstillede RDS-tjeneste
- Det er altid AaK og dennes systemejer der tildeler og administrere en sådan adgang og bestemmer hvilke tjenester / applikationer der tilbydes via RDS tjenesten. Fildeling tilbydes som udgangspunkt ikke, men kan deles via kommunens OneDrive / SharePoint miljø, hvis systemejer aktivt deler adgangsregulerede mapper til formålet til den enkelte ansatte ved en leverandør. Adgang til delte mapper autentificeres via Microsoft 2 faktor.
- Forudsætning for adgang til kommunens miljø er at hver enkelt medarbejder ved leverandør, der tildeles adgang, har egen mobiltelefon som understøtter Microsofts Autentifikations app og at den enkelte person kan verificere sig med personligt NEMID.
- RDS-tjenesten skal ses som en virtuel "jump host" hvor der tildeles adgang til specifikke applikationer og / RDP til specifikke servere. Filer der benyttes / gemmes på RDS tjenesten må aldrig være en del af det enkelte systems drift – da disse filer ikke gemmes og periodisk slettes fra den enkelte brugers profil på RDS-tjenesten. Filer der er nødvendige for drift på en server / et system skal derfor gemmes i det givne system og ikke på RDS-tjenesten. RDS-tjenesten skal forstås ligesom en leverandørs Workstation hvor der ligger data der ikke er en del af / afhængig et givent systems fortsatte drift. En leverandør kan ikke installere software på RDS-tjenesten.
- Filer er gemmes på tildelte shares til RDS-tjenesten fra en given systemserver gemmes på denne.

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. Afsender mail må kun være en dertil oprettet aarhus.dk mail og skal rekvireres af systemejer i Aarhus Kommunes ServiceNow hvis løsning skal kunne sende e-mail. Der må ikke benyttes andre smtp / mail servere.

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 minimum 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.
Aarhus Kommune kan til enhver tid afbryde net forbindelsen til et eller flere netkomponenter, ifm., fejlsøgning eller pga. sikkerhedsmæssige tiltag. En leverandørs evt. Ekstra omkostninger heraf er AaK uvedkommende. Dog forsøges det altid at informere leverandør om sådanne changes inden de foregår.

## 8.2. Servere og Workstations i Aarhus Kommunes driftsmiljø

Servere:
Skal en server driftsafvikles i Aarhus Kommunes netværk, placeres den, afhængigt af hvilke data der håndteres og lagres på den, i BTN-VRF eller i administrativt netværk.
Servere er virtuelle og driftsafvikles på Aarhus Kommunes VM-ware platform. Aarhus Kommune understøtter pt. Windows Server 2019 og 2020.

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.
Servere der hostes af AaK og er en del af et BTN-system, virtuelt eller fysisk, i Aarhus Kommune skal inden konfiguration / opsætning af software applikationer m.v. domain joines til AD AAKIOT.AARHUSKOMMUNE.DK
Adgangsstyring administreres af BTN systemejer. For at opnå adgang er det et krav at leverandørens personale er oprettet til førnævnte opkoblingsmetode
Det er ikke tilladt at installere 3.parts fjernadgang på servere eller enheder tilsluttet eller hostede i AaK infrastruktur
- (fx TeamViewer, Dameware etc.) Det er ej heller tilladt at installere fjernadgang på lokale controllere / servere.
Hvis sådanne (lokale) servere er en nødvendighed for sikker drift eller systemets bestykning skal sådanne ligeledes tilmeldes og rettighedstyres via AD - AAKIOT.AARHUSKOMMUNE.DK
Direkte Fjernadgang til server kan kun opnås via RemoteDesktop adgang som rettighedsstyres igennem Azure og AD - AAKIOT.AARHUSKOMMUNE.DK

Hvis der ikke er mulighed for at hoste på kommunes infrastruktur og hostes server eksternt ved leverandør er det et krav at:

- Leverandør beskriver og indestår for adgangsstyring/kontrol til server, både fysisk og virtuelt.

- server er beskyttet for unødig adgang
- Leverandør på anfordring fremsender lister over hvilke brugere / kommunalt ansatte / medarbejdere der pt. Har adgang til systemet.
- Leverandør kan redegøre for backup af systemet hvis dette er en del af den bestilte leverance.
- Administration og opsætning af servere / udstyr ved leverandør skal overholde nyeste ISO27001 krav og de seneste krav for Aarhus kommunes Fælles IT og Digitalisering Governance for GPDR med adgangskontrol styring mv.

Software dongels understøttes ikke på kommunens virtuelle servere. Secure USB-enheder og software dongels understøttes ikke via RDS tjenesten. Evt. installationer / opgraderinger på en specifik server skal altid aftales med systemejer i AaK med tilhørende servicevindue der meldes ind internt i en change management. Installation af software skal som udgangspunkt altid ske på servers D drev da C drev er reserveret til operativsystemet på server.
Alle servere følger Microsoft patch og antivirus management som automatisk installeres. Der må aldrig installeres 3. parts antivirus og software patches på serverne uden aftale med systemejeren. Hvis et givent system ikke er kompatibelt med seneste software, patches fra Microsoft, påhviler det leverandør at tilvejebringe opdateret software der er kompatibelt med Microsoft patches.
Virtuelle servere sikkerhedskopieres 1 gang i døgnet via fuldt snapshot af serveren. Der foretages ikke inkrementel eller enkelt fil/mappe backup af server. Det kan derfor ikke forventes at der kan restores fx. en enkelt fil på en virtuel server men i stedet restores server til det seneste snapshot hvor evt. ændringer der er foretaget efter dette snapshot ikke kan gendannes. En evt. restore af en server initialiseres altid af systemejeren i AaK.
Ved major nedbrud / incident på en given server restores server til sidst kendte virkende snapshot. En leverandørs evt. Ekstra Udgifter afledt heraf er aarhuskommune uvedkommende. Det påhviler leverandør af få et givent system i drift så hurtigt som muligt sammen med systemejer efter et major incident / nedbrud.

Licenser på Servere og installerede systemer skal altid udleveres til og ejes af Aarhus Kommune. Hvis en løsning kræver Microsoft SQL-tjeneste, skal licens til denne medleveres ved leverance. Aarhus kommune har interne SQL-hotel løsninger hvor flere databaser deler samme host, som kan tilbydes til en løsning. Enkeltstående SQL-instanser må som udgangspunkt ikke benyttes medmindre system ikke understøtter andet.
Ved et licens audit kan leverandør faktureres for evt. Manglende licenser hvis disse ikke er leveret med det specifikke system. Dette gælder for alle software løsninger der måtte kræve en licens. Hvis en software / licens udbyder pålægger gebyr / bøde for manglende licens faktureres denne til leverandøren. Operativsystem licens til kommunens egne virtuelle servers operativsystem leveres og betales af AaK.
Det påhviler altid leverandør at levere opdaterede licenser hvis det er nødvendigt for et systems drift, hvis disse er tidsbegrænsede. Leverandør skal levere sådanne licenser minimum 14 inden udløb af eksisterende licens. Det påhviler leverandøren at kontrollere evt. Udløbsdato af licenser.

Workstations:
Der kan ikke tilsluttes en leverandørs Workstations, lap tops og lign. til BTN-VRF. Medarbejdere i Aarhus Kommune, der med klientprogrammel til Workstations skal tilgå tjenester i BTN-VRF, gør det fra deres administrative Windows11 pc tilsluttet administrativt netværk. En leverandør må aldrig installere klient software på en kommunal administrativ PC.
Installation af et evt. 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. Systemejer i AaK skal i så fald bestille en sådan software installation til klienter internt i AaK. Klienter der benytter JAVA understøttes som udgangspunkt ikke pga. Licensregler.
Leverandøren kan jf. pkt. 8.1 tilgå tjenester på BTN-VRF via egen Workstation opkoblet via RDS webtjeneste og via eget internet. Det afklares altid med systemejer hvilke tjenester der tilbydes og måtte være nødvendige for drift af et givent system.

## 9. Service og Vedligeholdelse

Leverandøren 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.

Service skal kunne fravælges efter garantiperiodens udløb.

## 10. 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:

- Betjeningsvejledning som muliggør betjening med et minimum af betjenings-fejl. Betjeningsvejledningerne skal udformes under hensyntagen til brugernes adgangsrettigheder
- Beskrivelse af de hensyn, brugeren skal tage for at minimere antallet af fejl-alarmer
- Anlægsdokumentationen skal udleveres til bygherre/bygningsejer

*Dokumentation skal afleveres i henhold til Aarhus Kommunes IKT-paradigme*[3]
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 fx Revit-tegninger) i henhold til Aarhus Kommunes IKT-paradigme, til enten Aarhus Kommunes FM-system eller arkivserver/projektweb[6].

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

Anlæggene skal være af en sådan kvalitet og robusthed at uhensigtsmæssige nedbrud som manglende forbindelse som skyldes systemtekniske forhold.

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