Bilag 1

Beskrivelse af Kunden og Kundens IT-miljø

Aarhus Kommunes udvikling, drift og vedligeholdelse af sagsstyringssystem til IT-understøttelse af det sociale område

Vejledning til Tilbudsgiver i forbindelse med besvarelse af bilag 1, Beskrivelse af Kunden og Kundens IT-miljø.

Dette bilag indeholder Kundens anvisninger til bilag 1, Kunden og Kundens IT-miljø. Bilaget vil ikke blive evalueret i forbindelse med tilbudsevalueringen, og skal ikke udfyldes i forbindelse med afgivelse af tilbud.

Dette afsnit slettes ved Kontraktens underskrift.

Indholdsfortegnelse

1. Kundens it-miljø 4
2. Kundens it-strategi og standarder 4
2.1. IT-Strategi 4
2.2. Fysisk Infrastruktur 4
2.3. Logisk infrastruktur 5
2.4. Tjenester 6
2.4.1. NTP Tidssynkronisering 6
2.4.2. DHCP Netværksopsætning 7
2.4.3. DNS Navneopløsning 7
2.4.4. SMTP Mailgateway 8
2.4.5. SNMP Overvågning 8
2.4.6. FTP Filtetransfer 9
2.4.7. LDAP Directory Service / Authentikering af brugere 9
2.4.8. PKI – Certifikathåndtering 10
2.4.9. Radius brugervalidering 11
2.4.10. Internet Gateway 11
2.4.11. Webproxi 12
2.4.12. Print 12
2.4.13. Filsystem 13
2.5. Serverdrift 13
2.5.1. Applikationsservere – Hosted service 13
2.5.2. Applikationsservere - Cloud 14
2.5.3. Systemservere – On premise 14
2.6. Administrativt netværks standarder 14
2.6.1. Directory og rettighedsstyring 14
2.6.2. Desktop 14
2.6.3. Mobiltelefoner / tablets 15
2.6.4. Print 15
2.6.5. Filsystem 16
2.6.6. Kontorplatform 16
2.7. Lokalnetværk 16
2.8. Webplatforme 17
2.9. IT-Sikkerhed 17
2.10. Datakommunikation 17
2.11. Udstyr lokaliseret hos Kunden eller tredjemand 18

1. Kundens it-miljø

I nærværende bilag har Kunden beskrevet sit eksisterende og planlagte it-miljø, eller de dele heraf, som Kunden anser for relevante for Leverandøren i forbindelse med leveringen af Produkter og Ydelser omfattet af nærværende Rammeaftale til Kunden, f.eks. ved specialudvikling.

2. Kundens it-strategi og standarder

2.1. IT-Strategi

Aarhus Kommune anskaffer IT-tjenesteydelser, software- og hardwareleverancer gennem centralt fastlagte udbud, og har fra 2000 målrettet outsourcet sin IT-drift på centralt fastlagte aftalegrundlag samtidigt med, at organisationens IT-driftsenheder i samme periode er reduceret fra 21 til 1, - nemlig det nuværende "Fælles Service" placeret i Borgmesterens Afdeling.

Fælles Service er således fokuseret på fælles digitalisering, IT-support, leverancestyring, infrastrukturudvikling og drift af Infrastruktur.

De decentrale IT-funktioner er fokuseret på afdelingsspecifik digitalisering og produktspecifik support af fagsystemer.

2.2. Fysisk Infrastruktur

Aarhus kommune ejer sin egen CISCO-baserede fiberinfrastruktur, der forbinder de ca. 850 lokationer igennem 53 POP skabe placeret på 10 fiber ringe, der igen er forbundet til en backbone med to redundante knudepunkter. Hertil ca. 70 mindre lokationer opkoblet med ADSL kombineret med Cisco DM-VPN eller TDC's MPLS.

Alle lokationer kan tilbydes alle tjenester og alle netværk igennem denne infrastruktur.

Hele infrastrukturen er i 2015 opgraderet, og har stadig tilstrækkelig kapacitet. Core kapaciteten er p.t. 2*10 Gbit/s og kan udvides til 2*40 Gbit/s.

Lokationer er tilsluttet Core med 1 Gbit/s, større lokationer med 10Gbit/s.

Eksterne driftsoperatører er tilsluttet infrastrukturen enten direkte via kommercielle fiberforbindelser fra TDC og GlobalConnect, med TDC MPLS forbindelser eller med PtP VPN over Internettet. En særstatus har KMD, der er tilsluttet via en proprietær VPN teknologi.

Operatører på WAN infrastrukturen er p.t.:

- TDC / NetDesign: Fysisk fiber
- Netdesign : MAN, WAN, FW, DHCP, NTP, Peering.
- Global Connect: ISP – kapaciteten er p.t. 10 Gbit/s
- Telefoni og bylinjer: Telenor

2.3. Logisk infrastruktur

Aarhus kommunes netværk er opdelt i et antal VRF'er, - der kun har forbindelse med hinanden igennem Firewallregler. Så selvom to VRF'er deler fysisk infrastruktur, er de logisk kun forbundet til hinanden igennem Firewallens regler.

Et særskilt VRF er defineret som "DMZ", hvor ressourcer kan tilgås udefra igennem Firewallen på nattede public IP-adresser, og hvor ressourcerne i DMZ kan få regelbaseret ip-specifik adgang til ressourcer i de interne VRF'er.

De mest betydende VRF'er er:

- Administrativt netværk
  Fælles for hele organisationen. Tilbyder adgang til servere og platforme til alle administrative formål, herunder behandling og opbevaring af følsomme data. Anvendes af domæne pc'er og domæne servere samt managed mobilt udstyr via VPN. Der er ikke adgang til administrativt netværks ressourcer fra andre VRF'er.
- Bygningsteknisk Netværk
  Fælles for hele organisationen. Anvendes til bygningstekniske formål, herunder f.eks. klimastyring, anden proceskontrol, dørlåsesystemer, alarmer og video overvågning. Netværkets ressourcer er som udgangspunkt synlige fra administrativt netværk, - mens administrativt netværks ressourcer IKKE er synlige fra Bygningsteknisk netværk. Der er udstrakt leverandøradgang til Bygningsteknisk netværk.
- Pædagogisk netværk
  Anvendes af magistratsafdelingen for Børn og Unge til undervisningsrelaterede formål på Skoler. Der er som udgangspunkt ikke adgang til Pædagogisk netværk fra andre VRF'er.

- ”Home” netværk
  Fælles for hele organisationen. Tilbyder en simpel, trådløs internetforbindelse til udstyr der via 802.1x teknologi er logget på med brugercredentials fra et kommunalt AD, specifikt oprettede brugercredentials fra en internt vedligeholdt LDAP, eller en MAC-adresse der er registreret på en bruger fra den internt vedligeholdte LDAP. Der er ikke adgang til ressourcer i andre VRF'er fra ”Home”net og ingen tjenester tilbydes udover en webbaseret printservice, der kan udskrive på Kommunens multifunktionsprintere, samt internetadgangen.

- Publikumsnetværket
  Anvendes af Magistratsafdelingen for Kultur og Borgerservice til borgeradgang fra stationære desktops i Bibliotekerne.

- Gæstenet ”SmartAarhus”/”Eduroam”
  Anvendes af kommunens gæster, der kan få etableret en simpel, trådløs internetforbindelse i 9 timer, mod indtastning af credentials (NemID/MitID, SMS kode til mobiltelefon eller lånerkort/sygesikringsbevis). Ingen tjenester tilbydes udover Internetadgangen.

2.4. Tjenester

2.4.1. NTP Tidssynkronisering

Det er afgørende for driftsstabilitet og logning, at alle komponenter i et WAN – på tværs af logiske opdelinger – er ”enige om” hvad klokken er helt præcist. Til den ende har Aarhus Kommune i sit driftsmiljø en NTP-tjeneste, som er tilgængelig fra alle logiske netværk.

Name: 1161-ntp-01.aarhuskommune.local

Address: 10.150.1.100

Aliases: ntp.aarhuskommune.local

Status

NTP-tjenesten er bredt implementeret på de betydende installationer, og der er ikke andre interne NTP-tjenester tilgængelige på WAN. Men det er muligt at anvende NTP synkronisering med eksterne tjenester, og det formodes, at der specielt på VRF for Bygningsteknisk netværk og VRF for direkte Internetforbindelse er udstyr, der enten af historiske eller tekniske årsager anvender eksterne NTP-tjenester.

2.4.2. DHCP Netværksopsætning

Når en enhed tilsluttes WAN'et – enten med trådet Ethernet eller WiFi – tildeles det af DHCP-tjenesten en lokal IP-adresse, IP-adressen på en DNS-tjeneste til resolvering af hostnavne, og IP-adressen for udgående trafik.

Der i Aarhus Kommunes WAN en flerhed af DHCP-tjenester på forskellige platforme, som af historiske eller tekniske årsager betjener dele af, ét eller flere forskellige VRF'er. Der foreligger ikke en samlet dokumentation for DHCP-tjenesten for hele WAN'et og der er ikke en overordnet IP-plan som de arbejder under.

Status

Århus Kommune har et ønske om at konsolidere DHCP-tjenesten og etablere en sammenhængende IP-plan, og projektet er ikke igangsat.

2.4.3. DNS Navneopløsning

Aarhus Kommune har tre niveauer for DNS:

AD: Hvert AD resolverer som udgangspunkt kun sin egen zone i DNS på DC'erne, og forwarder til den fælles DNS.

Fælles DNS: Fælles DNS afvikles på en redundant Microsoft Server platform, og resolverer zoner der ikke findes i eksisterende AD'er eller som af forskellige årsager ønskes resolveret internt, - herunder resolvering til interne IP-adresser i DMZ, så en intern bruger ikke tilgår services i DMZ fra "ydersiden". AD'ernes zoner forwardes til den relevante AD DNS, og public zoner forwardes p.t. til Google.

Name: srvsysdns01.aarhuskommune.local
Address: 10.150.4.201

Name: srvsysdns02.aarhuskommune.local
Address: 10.150.4.202

Public DNS: Aarhus kommune disponerer over ca. 700 public domænenavne, hvor DNS administreres eksternt ved en driftspartner, p.t. E-Brand. Zonerne Aarhuskommune.dk og aarhus.dk er dog placeret i Azure DNS, og administreres af Fælles Service.

Status

Ingen planlagte ændringer

2.4.4. SMTP Mailgateway

Som udgangspunkt anvender medarbejdere i Aarhus Kommune Office365 til afsendelse og modtagelse af Mails. Andre mailsystemer og postklienter understøttes ikke for slutbrugere.

Til systemers afsendelse af mail, hvor gatewayen i Office365 af tekniske årsager ikke kan anvendes, anvendes et sæt redundante on-premise MS Exchange Mailgateways:

Name:	mx-smart.aarhuskommune.local
Addresses:	10.225.7.216
	10.225.7.215
Aliases:	smtp.aarhuskommune.local

Status

Ingen planlagte ændringer.

2.4.5. SNMP Overvågning

Da Aarhus kommune gennem de seneste årtier har haft outsourcet driften af desktops, servere og netværkskomponenter, er der ikke anskaffet overvågningssystemer og -hardware til internt brug. Systematisk overvågning af netværkets komponenter er som arbejdsopgave heller ikke placeret i nogen af Fælles Services funktioner. Overvågning udføres af driftspartnere.

Status

Der forventes at der etableres mulighed for intern driftsovervågning af WAN 'ets komponenter og serverudstyr. Den interne overvågning kan erstatte eller supplere en ekstern overvågning.

2.4.6. FTP Filtetransfer

Der er for 10 år siden etableret en fælles tjeneste til filudveksling på FTP. Tjenesten driftsafvikles på en virtuel Windows 2008R2 server i det outsourcede VM-waremiljø hos Atea, og er baseret på produktet "GoAnywhere" fra Linoma software, men ikke opdateret siden 2012. Der oprettes ikke nye brugere herpå, men de få eksisterende brugere har adgang til at anvende løsningen så længe den virker.

Slutbrugeres behov for Dokumentudveksling med eksterne understøttes strategisk med projektrum i Sharepoint 365 og med individuelt eller fælles OneDrive.

Har en systemejer behov for at hans system har adgang til en ftp-tjeneste, etablerer systemejeren en dedikeret ftp-tjeneste i regie af sit eget system.

Name: **ftp.aarhuskommune.dk**
Address: 10.215.24.27

Status

Fælles FTP-tjeneste er under udfasning, og genetableres ikke.

2.4.7. LDAP Directory Service / Authentikering af brugere

Authentikering af administrative medarbejdere skal ske imod Aarhus Kommunes Azure AD adm.aarhuskommune.dk, og login til nye systemer ske på basis af en "claim" udstedt af Azure AD.

Ansatte I Aarhus Kommune kan også valideres på ldaps opslag i AD adm.aarhuskommune.dk. Skoleelever kan valideres på ldaps opslag i AD bu.pri. Gæstebrugere kan valideres på ldaps opslag i AD homenet.aarhuskommune.dk. Eksterne leverandører af bygningstekniske løsninger kan valideres med ldaps opslag i AD aakiot.aarhuskommune.dk

Domaincontrollere i alle AD'er er driftet on-premise.

Status

Aarhus Kommune ændrer og konsoliderer løbende sin AD portefølje:

- On-premise AD adm.aarhuskommune.dk anvendes primært til legacy systemer. Nye systemer skal anvende AzureAD til authentikering af brugere, så Aarhus Kommune kan betinge udstedelsen af den "claim" som systemet logger brugeren på med af Multifaktor login, Conditional Access m.v.
- On premise AD bu.pri pædagogisk Netværk har en stadigt mindre rolle, da alle elever nu anvender Chromebooks der ikke er domainjoined til bu.pri, og serverporteføljen i bu.pri er vigende.
- De resterende AD'er for IOT, Gæstenetværk og print er under konsolidering til ét on premise AD.

2.4.8. PKI – Certifikathåndtering

Aarhus Kommune certificerer udstyr og applikationer på administrativt netværk med SSL certifikater udstedt af egen PKI, hvor trustalene skal skabes mellem interne enheder.

Root serveren og CA servere er baseret på Microsoft Windows og anvender CA Authorityrollerne i Microsoft AD.

Desktops i domænet adm.aarhuskommune.dk udstyres med maskincertifikater under grundspejlingen.

Mobile enheder udstyres med certifikater via SCEP og Intune enrollment.

Såvel desktops som Mobile enheder anvender certifikatet til bl.a. 802.1x baseret login og AnyConnect VPN tilslutning.

Servere udstyres med certifikat efter behov.

Status

I 1Q 2021 udfases den nuværende Root og dens 6 aktive CA'er, og erstattes af en nyetableret Root med 20 års løbetid og 4 aktive CA'er til hhv. AD autoenrollment, ad hoc enrollment, Intune enrollment af håndholdt udstyr og SCEP enrollment af DMVPN routere.

Aarhus Kommune har et ønske om at etablere autoenrollment af SSL certifikater på alle domainjoined servere, men opgaven er ikke igangsat,

2.4.9. Radius brugervalidering

Radiustjenesten I Aarhus Kommunes WAN er indlejret i Cisco ISE, og anvendes til at validere netværkslogin op imod en flerhed af directories.

Status

Ingen planlagte ændringer.

2.4.10. Internet Gateway

Adgang til Internet sker for alle netværk i Aarhus Kommune igennem 2 redundante Cisco ASA Firewalls.

Cisco 5585–SSP-40 / ASA 9.8(4)26

Et andet redundant sæt Firewalls håndterer indgående VPN baseret på Cisco AnyConnect for slutbrugere, og et antal Site2Site forbindelser til samarbejdspartnere.

Cisco 5525 / ASA 9.8(3)21

Anmodning om portåbninger sker udelukkende igennem changemanagement, og kun få nøglemedarbejdere i Fælles service har adgang til at ændre på Firewallens konfiguration.

Adgangen fra Internettet og ind til de interne netværk er administreret med change management og servere med adgang fra Internet er som udgangspunkt placeret i DMZ.

Adskillelsen af de interne VRF'er er på den udgående firewall primært baseret på interfaces i én samlet kontekst, og administrationen af reglerne på de enkelte interfaces trafik med hinanden har gennem tiden været mangelfuld. Regelsættet der definerer de enkelte interfaces adgang til hinanden, er derfor ustruktureret og vanskeligt at gennemskue.

Der er de seneste år påbegyndt en situationsbestemt etablering af særskilte kontekster, der alene betjener et enkelt VRF.

Status

En samlet revidering af det eksisterende Firewallmiljøs konfiguration gennemføres 1Q 2021.

2.4.11. Webproxi

Der anvendes redundante Citrix Netscalere som legacy webproxi, så webfunktioner placeret på det interne netværk kan udstilles for eksterne brugere. Netscalerne er virtuelle appliances i det outsourcede serverdriftsmiljø hos Atea.

Netscalernes proxifunktion er ofte kombineret med 2-faktor brugervalidering baseret på en løsning fra Signaturgruppen "Loginservice" og/eller ADFS.

Status

Funktionaliteten i Netscaleren kombineret med "Loginservice" kan i mange tilfælde også realiseres i Azure-AD, hvor Conditional Access og en Azure proxitjeneste erstatter Signaturgruppens on-premise løsning. Det forventes at brugen af AzureAD, Conditional Access og Azure Proxi vil tage til, og brugen af Netscaler og Loginservice vige.

2.4.12. Print

Aarhus Kommune anvender en portefølje af multifunktionsprintere fra én leverandør, der vælges igennem periodiske udbud. P.t. har Konica-Minolta leverancen. Multifunktionsprinterne er af historiske årsager typisk placeret i administrativt netværk eller pædagogisk netværk. Routningen af print fra den enkelte arbejdsplads til printeren sker via printservere og systemsoftware leveret af Konica-Minolta.

Servermiljøet for printsystemerne er placeret i et særskilt VRF med sit eget AD print.aarhus-kommune.dk. Det er planen, at såvel printere som printersystemer skal placeres i dette VRF, så muligheden for print er en tjeneste, der er uafhængig af det fagspecifikke VRF brugerens desktop er i.

Status

Migrering af printerne til print VRF'et er påbegyndt

2.4.13. Filsystem

Filshares tilbydes i et DFS-filsystem hos ekstern serverdriftsoperatør. Brugernes personlige filshare (homedir) er omlagt til OneDrive i Office365. Omlægning af afdelingsspecifikke filshares til OneDrive er igangværende.

Status

Ingen planlagte ændringer.

2.5. Serverdrift

2.5.1. Applikationsservere – Hosted service

Driftsarkitekturen, hvor både servere og klienter befinder sig i et internt administrativt netværk bag Aarhus Kommunes firewall, er fælles for en lang række af legacy systemer, - men er **ikke** længere den strategisk valgte driftsarkitektur for nye systemer.

Ca. 300 applikationsservere er virtualiserede og hostes samlet i et outsourcet driftsmiljø, - p.t. et VMware miljø driftet hos ATEA. Der understøttes Win 2012 R2, Win 2016, Win2019 og RedHat Linux. Driftsmiljøet er SPLA licenseret for Operativsystemets vedkommende, mens Microsoft SQL server Std. og Enterprise som udgangspunkt licenseres af Aarhus Kommune selv på særskilt fysisk driftsmiljø hertil.

Herudover hostes et begrænset antal interne applikationsservere af forskellige applikationstekniske eller historisk betingede årsager hos andre driftspartnere, eller ved systemleverandøren.

2.5.2. Applikationsservere - Cloud

Aarhus kommunes strategiske driftsarkitektur for **nye** systemer er:

Authentikering af brugere i AAK Azure AD, med en af AAK defineret MFA
Klienter tilsluttet any-network, men valideret som compliant i AAK Azure MFA
Login med en af AAK udstedt "claim", indholdende brugerens roller / rettigheder
Applikationsservere tilgået over Internettet med tidssvarende kryptering

2.5.3. Systemservere – On premise

Aarhus kommune råder over et redundant virtualiseret serverdriftsmiljø on-premise, hvor systemservere for tjenester (f.eks. DNS, DHCP, SMTP m.v.) og anden funktionalitet (AD, Cisco ISE, SCCM m.v.) på Infrastrukturen afvikles.

Platformen er Cisco ISE Flexpod, og Hypervisoren er VMware.

2.6. Administrativt netværks standarder

2.6.1. Directory og rettighedsstyring

Der anvendes Azure AD samt on premise Microsoft AD 2012 med 4 DC'er. Roller og rettigheder for en administrativ medarbejder, for eksterne brugere og for borgere skal være defineret i AD / Azure AD BTC, og login til et system skal ske på basis af en "claim" udstedet af Aarhus Kommunes AD.

Digitale medarbejdersignaturer for 4-5.000 ansatte i Aarhus kommune administreres og deployeres med "Signaturcentralen" leveret af Signaturgruppen.

2.6.2. Desktop

Alle desktops er managed med Microsoft SCCM. Applikationer deployeres som MSI installationspakker med silent/unattended installation. Antivirus er "Kaspersky". OS er Win 10 Pro.

Der er på administrativt netværk ca. 15.000 Workstations fordelt på et faldende antal bærbare af fabrikat Lenovo, et stigende antal bærbare af fabrikat HP og stationære af fabrikat HP. Porteføljen er konsolideret på forholdsvist få modeltyper, da al arbejdspladshardware er anskaffet inden for de seneste fire år. Der er i 2018 indgået ny aftale på leverance af desktops, hvor produktserien på bærbare er HP. Der vil derfor i en årrække fremover være såvel Lenovo som HP bærbare i produktion.

Desktops tilsluttet eksterne netværk kan tilgå systemer i det interne netværk gennem Cisco AnyConnect VPN. Flere og flere systemer, - herunder Office365 – kan tilgås uden VPN, og det tilstræbes derfor kun at anskaffe nye systemer, der anvender Azure AD som authentikering, og som tilbyder sig som en service på Internet.

2.6.3. Mobiltelefoner / tablets

Porteføljen er spredt på forskellige platforme, og forventes ikke konsolideret.

Der anvendes ca. 45% iPhone, 45% Android og 10% Andet. Tablets til generelt kontorbrug er typisk iPad, mens tablets dedikeret til fagsystemer typisk er Android.

Alle mobiltelefoner og tablets er underlagt device management og deployering baseret på Microsoft Intune deployering.

SIM-kort leveres af én Teleoperatør på indgået aftale herom, - p.t. "Telenor". SIM-kort anvender teleoperatørens APN til Internetforbindelse.

Mobile enheder kan via device management udstyres med Cisco AnyConnect Klient og et brugerspecifikt certifikat. Herved kan apparatet forbindes til administrativt netværk efter behov. Løsningen med VPN opkobling af Mobiltelefoner og Tablets vil løbende blive udfaset til fordel for andre og mere applikationsrettede teknologier, når mulighederne er der.

2.6.4. Print

Ca. 900 Konica-Minolta Multifunktionsprintere, der er managed med Konica-Minoltas produkt "Safe-Q" samt "PaperCut". Printerne understøtter sikker udskrift og follow-me udskrift.

Lokalt tilsluttede printere er tilladte, men understøttes ikke.

Et igangværende projekt konsoliderer printere fra administrativt og pædagogisk VRF i et nyetableret Print-VRF.

Aarhus Kommune er aktuelt i genudbud med printydelser, hvilket forventes at medføre udskiftning af kommunens printere.

2.6.5. Filsystem

Et begrænset antal filshares afvikles i et internt DFS-filsystem. Brugernes personlige filshare (home-dir), samt afdelings eller systemspecifikke filshares er omlagt til OneDrive i Office365.

2.6.6. Kontorplatform

Der anvendes Microsoft Office 365 og Sharepoint 365.

2.7. Lokalnetværk

I kommunens bygninger patches vægstik til specifikke VRF'er i krydsfelter med Cisco switch udstyr.

Aarhus kommune har anskaffet Cisco ISE som standardprodukt til NAC.

NAC på trådet opkobling implementeres løbende på alle lokationer, - typisk i forbindelse med andre changes på det aktive netværksudstyr. Cisco ISE NAC vil på sigt helt erstatte den nuværende binding af switch porten til et bestemt VRF.

I vid udstrækning er de logiske netværk også tilgængeligt trådløst fra de ca. 9.000 Cisco Access points. SSID'er er konsolideret således at langt de fleste netværk tilgås med SSID "Aarhuskommune", der ved hjælp af 802.1x og Cisco ISE sender brugeren til det rigtige VLAN.

I nyt byggeri og større forandringsprojekter vil der blive lagt vægt på dækning med trådløst net, og der vil ikke nødvendigvis være direkte adgang til trådet net fra alle kontorarbejdspladser.

WiFi infrastrukturen består p.t. af :

- Cisco Access Point : En portefølje af Cisco AP'er anskaffet over tid. Serie og Model justeres løbende.
- Cisco Wireless LAN Controller: Nuværende version 8.5.161.0.
- Cisco ISE NAC : Version 2.7.0.356 Installed Patches 1,2

2.8. Webplatforme

Intranet og hjemmeside afvikles i CMS'et "Umbraco". Dokumenthåndteringssystem "e-doc" afvikles i Sharepoint 2010, Collaboration og Projektrum afvikles i Sharepoint Online.

Der er dog ingen vedtagne bindende standarder på WEB-området, og der er derfor også et stort antal mindre og fagspecifikke webløsninger på en betragtelig flerhed af afviklingsplatforme og CMS'er.

2.9. IT-Sikkerhed

Aarhus kommunes IT-Sikkerhedspolitik ligger på **Aarhus kommunes hjemmeside**.

Den tilhørende IT-sikkerhedshåndbog er baseret på DS484, og kan rekvireres fra Aarhus kommune.

2.10. Datakommunikation

Aarhus kommunes strategiske driftsarkitektur er som beskrevet i punkt 2.5.6 at klienter og applikationer kommunikerer via Internettet, med tidssvarende og sikker autentifikation og kryptering.

Men i det omfang der skal etableres lukket datakommunikation med en ekstern driftsudbyder/systemleverandør, sker det under forudsætning af indgået Databehandleraftale og på følgende måder:

- Redundant peering igennem eksisterende kommerciel fiber, - TDC MPLS, Nianet eller GlobalConnect.
- Routning igennem en for udbyderens regning etableret ny kommerciel fiber til Aarhus Kommunes infrastruktur (redundant indgang på hhv. Rådhuset og Grøndalsvej 1, 8260 Viby J.
- Point to Point VPN over AAK's internetforbindelse.

- Individuelt tildelt og personlig VPN adgang for medarbejder(e) hos Leverandøren baseret på Cisco AnyConnect og validering af brugeren med Medarbejder NemID/MitID udstedt af Leverandøren. Bemærk: Brug af "TeamViewer" og tilsvarende kommercielle fjernovertagelsesværktøjer over Internet er **ikke** tilladt på noget udstyr placeret i Aarhus Kommunes netværk.
- SSL kommunikation over Internet fra udstyr placeret i DMZ eller via webproxi for udstyr i interne netværk.

2.11. Udstyr lokaliseret hos Kunden eller tredjemand

1. Legacyløsninger : Hostet i Aarhus kommunes driftsmiljø.

   Omkostningen ved hosting i dette miljø afregnes direkte af operatøren med Aarhus kommune, hvorfor denne omkostning som udgangspunkt skal tillægges den tilbudte pris på en given løsning.

   Som udgangspunkt vil overdragelse, driftsprøve og performancemålinger skulle udføres på de virtuelle servere, som Leverandøren gennem VPN eller tilsvarende får adgang til at udføre sin systemvedligeholdelse og –installation på.

2. Løsninger hostet hos Leverandøren selv, eller ved 3. part på kontrakt med Leverandøren.

   Omkostningen ved denne hosting er typisk indregnet i løsningens tilbudte pris.

   Som udgangspunkt vil performancemålinger skulle udføres i indgangen til Aarhus kommunes infrastrukturs coremiljø, enten via kommerciel fiber, SSL over Internettet eller Point to Point VPN over Internettet.

- Gælder alene for Teknisk netværk:

  Driftsmodel 1 og 2 gælder også for Bygningsteknisk netværk, - men herudover kan leverandøren tilbyde sin løsning opstillet i teknikrum på Aarhus kommunes lokationer. Anvendes denne mulighed er det dog en forudsætning at leverandøren kan etablere en PtP VPN forbindelse hvorigennem udstyret driftes, samt at Aarhus kommune v. Fælles Service Infrastruktur får administratoradgang til de lokalt opstillede systemkomponenter, så de ved akutte driftshændelser kan deaktiveres eller lukkes ned.

  Til Point to Point VPN forbindelsen stiller Aarhus Kommune disse krav:

  - IPSec mode = Standard Site 2 Site (Tunnel mode)
    Authentication mode = Pre-Shared key (20 tegn)
    IKE Phase 1 Capabilities = AES-256
    Encryption = AES-256
    Authentication = SHA1
    DiffelHellmann Group = Dh GROUP 5
    Mode = Main
    Renogotiation = 24H
    IPSec Phase 2 capabilities
    Encryption = AES-256
    Authentication = SHA1
    USE PFS = YES
    Renogotiation = 3600
  - ALLE interne IP adresser på AAK Teknisk Netværk NATTES til et ubrugt Public ip-scope fastsat af AAK

- Som udgangspunkt vil overdragelse, driftsprøve og performancemålinger skulle udføres på det lokalt opstillede udstyr.