Bilag 2 Kundens it-miljø

**Indholdsfortegnelse**

[1 Indledning 5](#_Toc486001221)

[2 Afgrænsning mellem Kundens it-miljø og Leverandørens Leverance 5](#_Toc486001222)

[Appendiks A Kundens it-miljø 7](#_Toc486001223)

[1 Kundens it-miljø 7](#_Toc486001224)

[1.1 Beskrivelse af Kundens IT - organisation 7](#_Toc486001225)

[1.2 IT infrastruktur 7](#_Toc486001226)

[1.2.1 Datacentre 7](#_Toc486001227)

[1.2.2 Netværk 8](#_Toc486001228)

[1.2.3 Internet forbindelser 8](#_Toc486001229)

[1.2.4 VLAN 9](#_Toc486001230)

[1.2.5 Firewall 9](#_Toc486001231)

[1.2.6 Netværksovervågning 9](#_Toc486001232)

[1.2.7 VPN adgange 9](#_Toc486001233)

[1.3 Servere 9](#_Toc486001234)

[1.3.1 Virtuelle servere 9](#_Toc486001235)

[1.3.2 Operativsystemer 10](#_Toc486001236)

[1.3.3 Databaser 10](#_Toc486001237)

[1.3.4 Antivirus 10](#_Toc486001238)

[1.3.5 Mailsystem 10](#_Toc486001239)

[1.3.6 Domænestruktur 10](#_Toc486001240)

[1.3.7 Domæneopbygning 10](#_Toc486001241)

[1.4 Arbejdsstationer 10](#_Toc486001242)

[1.4.1 Hardware 10](#_Toc486001243)

[1.4.2 Operativsystem 11](#_Toc486001244)

[1.4.3 Browser 11](#_Toc486001245)

[1.4.4 Kontorpakke 11](#_Toc486001246)

[1.4.5 Antivirus 11](#_Toc486001247)

[1.5 Unified Communications 11](#_Toc486001248)

[1.6 Mobiltelefoner og tablets 11](#_Toc486001249)

[1.7 Administration af mobile enheder 12](#_Toc486001250)

[1.8 Folketingets cloud-løsning 12](#_Toc486001251)

[1.9 Folketingets DMZ 12](#_Toc486001252)

[1.10 Systemintegration 12](#_Toc486001253)

[1.11 Særlige forhold for installation på PCer. 12](#_Toc486001254)

[Appendiks B Leverandørens krav til kundens it-miljø 13](#_Toc486001255)

[1.12 Leverandørens krav til it-miljøet 13](#_Toc486001256)

**Bilag**

Appendiks A Kundens it-miljø

Appendiks B Leverandørens krav til kundens it-miljø

***Vejledning til tilbudsgiver***

*Denne vejledningstekst og øvrige vejledningstekster i bilaget slettes forud for kontraktindgåelse.*

*Nærværende bilag specificerer Kundens it-miljø og Leverandørens Krav hertil og det i bilaget angivne supplerer Kontraktens bestemmelser herom.*

*Tilbudsgiver skal udfylde bilagets Appendiks B i overensstemmelse med vejledningen til bilaget.*

*Tilbudsgiver skal i Appendiks B specificere, hvilke krav der stilles til Kundens it-miljø, såvel under udviklings- og implementeringsforløbet som i vedligeholdelsesperioden. Tilbudsgiver skal angive de krav til dimensionering og kapacitet (herunder eventuelle kapacitetsudvidelser ved mængdeforøgelser), der er nødvendige med henblik på opfyldelse af kravene i Kontrakten, herunder de i bilag 6 angivne servicemål.*

*Tilbudsgivers krav til Kundens it-miljø skal beskrive, hvad der som minimum kræves. Tilbudsgiver kan i det omfang, at det vurderes relevant, opstille supplerende anbefalinger til it-miljøet, herunder forslag til udviklingstiltag. Sådanne anbefalinger må dog ikke have betydning for Leverandørens opfyldelse af Kontrakten.*

*I bilagets afsnit 2 er beskrevet den nærmere afgrænsning mellem Kundens it-miljø og Leverancen, der leveres af Leverandøren under Kontrakten.*

*For specifikke krav til tilbudsgivers beskrivelse henvises til vejledning til Appendiks B.*

*Herudover er det ikke hensigten, at tilbudsgiver skal foretage yderligere tilføjelser eller ændringer til bilaget. Såfremt tilbudsgiver alligevel foretager tilføjelser eller ændringer, henvises der til udbudsbetingelsernes punkt 9 vedr. evaluering af tilbud, hvoraf det fremgår, at* *det vurderes i hvilket omfang med hvilket indhold, at vilkårstekst, der ikke er markeret som mindstekrav, imødekommes, idet det vurderes positivt, såfremt den angivne vilkårstekst imødekommes, da denne vilkårstekst udtrykker ordregivers forretningsmæssige ønsker til vilkår, som er indeholdt i de enkelte dokumenter. Derudover skal tilbudsgiver være opmærksom på det nedenfor anførte vedrørende mindstekrav.*

***Særlige forhold vedr. mindstekrav og grundlæggende elementer***

*Bilaget indeholder alm. vilkårstekst. En del af denne vilkårstekst kan udgøre mindstekrav. Mindstekrav er angivet i bokse og mærket med ”****mindstekrav****” eller ”[****MK****]”.*

*Sådanne mindstekrav* ***skal*** *opfyldes. Opfyldes et mindstekrav ikke, betragtes tilbuddet som ikke-konditionsmæssigt og vil som følge heraf blive afvist.*

*Tilbudsgiver skal være opmærksom på, at tilføjelser eller ændringer i vilkårstekst kan kollidere med mindstekrav, selv om tilføjelserne eller ændringerne foretages uden for de steder, der er markeret som mindstekrav.*

*Tilbudsgiver skal ligeledes være opmærksom på, at tilføjelser eller ændringer til vilkårstekst kan udgøre ændringer til grundlæggende elementer med den følge, at tilbuddet vil blive afvist som ukonditionsmæssigt.*

*Afvigelser over for vilkårsafsnit i et bilag skal markeres med ændringsmarkering (”Track Changes”) eller på anden måde tydeligt fremhæves.*

*Dette afsnit under overskriften ”Vejledning til Tilbudsgiver” vil ikke indgå i den endelige Kontrakt.*

*Tilbudsgivers udfyldelse af dette bilag med krav til Kundens it-miljø vil blive vurderet under underkriteriet ”Systemets kvalitet” i overensstemmelse med det angivne i udbudsbetingelserne punkt 9.1.1.*

# Indledning

Bilag 2 indeholder en beskrivelse af Kundens it-miljø samt Leverandørens evt. krav hertil.

Kundens it-miljø er beskrevet i bilag 2, Appendiks A.

Leverandøren har i bilag 2, Appendiks B beskrevet evt. krav til Kundens it-miljø som forudsætning for at opfylde kravene i kontrakten.

# Afgrænsning mellem Kundens it-miljø og Leverandørens Leverance

Leverandørens Leverance, som nærmere beskrevet i bilag 3 skal omfatte applikationen og evt. middleware som er nødvendigt for afviklingen af applikationssoftware. Kunden anskaffer og installerer selv hardware og basisprogrammel, jf. nedenstående figur. Kunden har ansvaret for drift, herunder patching af hardware og basisprogrammel. Leverandøren har ansvaret for vedligehold af applikationen og eventuel middleware, herunder patching. Dette skal ske i tæt samarbejde med Kunden.

**Middleware** omfatter applikationsservere, webservere mv.

**Basisprogrammel** omfatter Operativsystemersåsom f.eks. MS Windows samt databaseprogrammel såsom f.eks. MSSQL og Sharepoint Online.

Kunden varetager selv backup.

Leverandøren er forpligtet til at vejlede Kunden om de nærmere forhold vedr. installation af Kundens it-miljø.

Bilag 2, Appendiks A Kundens it-miljø

# Appendiks A Kundens it-miljø

# Kundens it-miljø

Beskrivelse af kundens It-miljø omhandler det miljø, Leverancen skal fungere i samspil med.

## Beskrivelse af Kundens IT - organisation

Folketingets It-organisation er delt i to særskilte enheder under Vicedirektøren for Service- og Administrationsafdelingen.

* ITU, der står for udvikling af fortrinsvis parlamentariske specialapplikationer og hjemmesider samt applikationsdriften af disse.
* ITS, der står for brugersupport samt drift og udbygning af hele It-infrastrukturen – dvs. servere, netværk, storage og klienter – både PC og mobilenheder.

Vedligehold og videreudvikling af intranet-applikation vil blive forankret i ITU.

ITS vil administrere servere, basisprogrammel og sikkerhed på intranettet herunder daglig administration af Folketingets AD (Active Directory).

## IT infrastruktur

### Datacentre

Folketinget drifter IT i 3 datacentre, placeret i forskellige bygninger og etager. Der er fiberforbindelser mellem de 3 datacentre.

I alle 3 datacentre findes der ledig plads i eksisterende serverracks, hvis der skal monteres fysiske servere.

### Netværk

Folketingets netværk er baseret på en CISCO infrastruktur, med en backbonestruktur bestående af 2 backboneroutere placeret i 2 af datacentrene. Disse er dels koblet til et L2 netværk, der driver tilgangen til VMware-servere og storagesystemer, dels et L3 distributionsnet bestående af 3 switche, der igen servicer krydsfelterne.

Alle fysiske netværksporte, på nær porte i datacentre, er beskyttet med 802.1x.

Det trådløse netværk består af 2 CISCO WLAN controllere i cluster. Der benyttes følgende SSID´er:

* WLANI (hidden SSID) Internt netværk med 802.1x beskyttelse. Benyttes KUN af domænejoinede PC´er.
* FTiPHONE – WPA beskyttet. Benyttes til mobiltelefoner af husets faste brugere.
* Christiansborg\_press – WPA beskyttet. Benyttes af pressemedarbejdere til disses PC`er og andet udstyr.
* Christiansborg\_guest – Åbent netværk med en ”Accept-page”. Benyttes af gæster.

Det trådløse netværk er under omlægning for så vidt angår placering og antal af accesspunkter, så der kan opnås fuld dækning på 5 GHz båndet på Christiansborg og tilhørende bygninger.

### Internet forbindelser

Folketinget benytter 2 internetoperatører.

Telia, der leverer en redundant fiberforbindelse fra 2 af datacentrene. Denne forbindelse benyttes for den trafik der er initieret fra Folketinget samt mailtrafik. Det er denne forbindelse der gennem firewalls giver adgang til det interne netværk. Det er også denne fiberforbindelse der er bære for al internettrafik fra de trådløse netværk, som tilbydes i Folketinget. Telia fiberforbindelsen er delt ud i 3 særskilte net, FT-internet, Streaming og Public. Det er Public-nettet der benyttes til trafik fra SSID FTiphone.

NIANET, der leverer en enkeltstående forbindelse til 1 datacenter. Denne forbindelse bruges som adgangsforbindelse fra omverden, til de websites og services Folketingets stiller til rådighed for offentligheden.

Kapaciteten på Teliaforbindelsen er 800 Mbit og NIANET er 1 Gbit.

### VLAN

Der bruges VLAN i netværket til at adskille datatrafik. Nye VLANs oprettes efter behov.

### Firewall

Alle internetforbindelser er beskyttet med firewalls. For Telia-nettet Public, der benyttes af mobiltelefonerne, er der i dag en enkeltstående firewall.

Mobiltelefoner er koblet op på SSID FTiPHONE og har direkte adgang til internettet via firewallen. De har ingen direkte adgang til det interne produktionsnet. Der er således ingen forskel på, rent adgangsmæssigt, om en mobiltelefon befinder sig på det trådløse netværk i Folketinget, et andet sted eller på 4G-netværk.

For det interne produktionsnetværk, hvor servere og PC´er er tilsluttet, gælder det at al internettrafik går gennem PROXY-servere med skanning af indhold for malware inden trafikken går videre til firewallen. Har en serverapplikation et behov for direkte internetkommunikation uden om PROXY-server kan der åbnes for dette, med mindre det konflikter med Folketingets it-sikkerhedspolitik.

### Netværksovervågning

Netværksenheder overvåges med Solarwinds Orion.

### VPN adgange

Der er adgang via VPN for PC´er installeret og udleveret af Folketinget til Folketingsmedlemmer og ansatte.

For leverandører gives der RDP-adgang til udvalgte servere fra forhåndsaftalte IP-adresser. Adgangen kræver 2-faktorvalidering i form af en SMS-kode.

## Servere

### Virtuelle servere

Folketinget etablerer som udgangspunkt udelukkende virtuelle servere, der er ganske få fysiske tilbage.

Det virtuelle miljø er baseret på VMware og er baseret på en stretched Cluster opsætning.

Som udgangspunkt etablerer vi ikke fysiske servere, med mindre der er et velargumenteret specificeret krav.

### Operativsystemer

Folketinget installerer som udgangspunkt kun Microsoft Windows Server 2012 R2 Standard, eller nyere, med mindre der er et velargumenteret specificeret krav til andet. Licensmæssigt er det omkostningsfrit for Folketinget at gå op til Datacenter versionen på virtuelle servere. På fysiske vil det være en meromkostning for Folketinget hvis typen går over Standard.

### Databaser

Folketinget anvender som udgangspunkt Microsoft SQL Server 2012 std, eller nyere.

### Antivirus

Alle servere og klienter kører har Antivirus agent installeret med opdatering og overvågning fra en central server.

Undtagelser for indstillinger laves ikke med mindre der er et velargumenteret specificeret krav.

### Mailsystem

Folketingets mailsystem er baseret på Exchange 2010, med en Outlook 2013 Klient. I enkelte tilfælde benyttes Outlook Web App til webmail adgang.

### Domænestruktur

Folketinget har en enkelt domænestruktur med on-premise domain-controllere med mulighed for logonvalidering gennem Azure AD.

### Domæneopbygning

Folketingets domæne er baseret på Windows Server 2012 og functional level 2012.

## Arbejdsstationer

### Hardware

Folketinget benytter i dag Laptops med minimum i5 processor og 8 GB RAM

### Operativsystem

Windows 10

### Browser

Standard browser er Internet Explorer 11, men Folketinget accepterer at bruge andre browsere såfremt dette er nødvendigt til enkelte applikationer, der benyttes af få udvalgte brugere. Øvrige browsere der er installeret er Google Chrome og Edge.

### Kontorpakke

Office 2013 er standard. I enkeltstående tilfælde kan det accepteres at benytte Office 2016 eller Office 365.

### Antivirus

Der er installeret antivirusagent på samtlige arbejdsstationer.

## Unified Communications

Folketinget har pt. ikke installeret UC, men har en strategi om at installere Microsoft Skype for Business. Det er ikke afgjort om der vil blive tale om en On-premise eller cloud løsning. Folketinget har licensmæssigt Skype for Business med i licensaftalen fra Microsoft, der er en Secure Productive Enterprise E3, som er bestående af Windows, Mobility og Office 365 E3. Aftalen dækker samtlige brugere i Folketinget. Folketingets licenspartner er Crayon.

## Mobiltelefoner og tablets

Folketinget benytter Apple iPhones som smartphone. Pt. benyttes modellerne iPhone 5S, 6 og 6S. Alle brugere får udleveret en iPhone, hvilket vil sige knap 1200.

Medlemmerne samt en række ansatte i Folketingets administration, i alt knap 350, har tillige fået udleveret en iPad af typerne iPad2/32GB, iPad4/32GB, iPad air/32GB, iPad air2/64GB og iPad air2/128GB.

## Administration af mobile enheder

Microsoft Intune er under indfasning som MDM-system til administration af mobile enheder. Det forventes at samtlige mobilenheder er tilsluttet MDM inden sommeren 2018.

## Folketingets cloud-løsning

Folketinget har ”Secure Productive Enterprise E3”-licensaftale der giver adgang til brug af Sharepoint, både som Cloud og on-prem for 1250 brugere. Aftalen giver brugerne ret til at tilgå Sharepoint-løsninger og desuden også indeholder rettigheden til at tilgå underliggende Windows servere. Ligeledes giver SPE licensen rettighed til at installere ubegrænset Sharepoint servere, så længe at de ansatte, der tilgår serverne er SPE licenseret. Folketinget har endvidere 1250 CAL licenser til de ansatte – også i det tilfælde en løsning baseres på SQL Server / CAL licenseringen. Vælges SQL Server / CAL og ikke core licenseringen, skal de eksterne brugere have en SQL CAL.

## Folketingets DMZ

Folketinget har forskellige DMZ/Netværkszoner, og servere placeres så der opnås størst mulig isolation mellem internetkoblede klienter og data.

## Systemintegration

Folketinget anvender i vidt omfang udveksling af data mellem de forskellige applikationer. Dette sker som oftest ved, at de enkelte systemer gennem webservices udstiller events som opfanges og sendes som meddelelser til de systemer, der måtte gøre brug af dem.

Som message-broker anvendes Microsoft Biztalk.

Er der i forbindelse med en event brug for ekstra data fra kildesystemet, vil Biztalk eller modtagesystemet tilgå kildesystemets API for at hente de nødvendige data.

I forbindelse med nyanskaffelser af systemer, der skal indgå i dataudveksling med andre systemer, vil Folketinget sikre sig, at systemet kan udveksle data på ovennævnte måde.

## Særlige forhold for installation på PCer.

Brugerne har ikke administrative rettigheder på deres pc-arbejdsplads, hvorfor eventuelle komponenter, der ikke kan installeres i brugerkontekst, skal leveres i et format, f.eks. MSI-pakke, der kan installeres med Microsoft Configuration manager.

**Bilag 2, Appendiks B Leverandørens krav til kundens it-miljø**

# Appendiks B Leverandørens krav til kundens it-miljø

## Leverandørens krav til it-miljøet

*[Udfyldes af tilbudsgiver*

*Tilbudsgivers beskrivelse skal indeholde følgende:*

* *Detaljerede krav til hardware og programmel (omfattende operativsystemer, basissoftware og databaser for produktions- og testmiljø til Leverancen.*
* *Tilbudsgivers forventninger til ændringsbehov i vedligeholdelsesperioden for, at opdateringer af systemet vil kunne anvendes]*