# It arkitektur- og sikkerhedskrav

## Løn og personalesystemsudbud

Region Midtjylland 2010

.

# 1 Indledning

## *1.1 Versionshistorie*

| Version | Dato | Ansvarlig | Status | Beskrivelse |
|---|---|---|---|---|
| 1.0 | 2010-05-04 | HENSTI | Lukket | Definition af minimumskrav |

## *1.2 Formål*

Dette dokument beskriver overordnede krav til It arkitektur- og sikkerhed, i forbindelse med udbud af nyt Løn og personalesystem i Region Midtjylland.

De opstillede krav er kategoriseret efter RM IT's kategorisering og kan derfor redaktionelt placeres anderledes i det endelige udbudsmateriale. I det omfang at HR ønsker det må kravenes ordlyd tilpasses, men essensen af kravene kan kun ændres med It-arkitektur og sikkerheds accept.

Kravene er formuleret på et overordnet niveau. Detaljeret specifikation af den eksisterende infrastruktur er ikke taget med i kravene, da løsningen forventes implementeret så langt ude i fremtiden at detaljerede krav til infrastruktur endnu ikke kan defineres. Krav stillet i dette dokument bygger på de kendte langsigtede beslutninger der er truffet om Region Midtjyllands it-infrastruktur.

## *1.3 Afgrænsning*

Krav, der kan udledes direkte af lovkrav, de jure og de facto standarder, er ikke specificeret i detaljer.
Såfremt der i forbindelse med projektering og installation af den beskrevne løsning udkommer nye love og/eller standarder som erstatninger for de anførte, skal de(n) nye standard anvendes.

## *1.4 Referencer*

### 1.4.1 Persondataloven

### 1.4.2 Sundhedsloven

### 1.4.3 Arkitekturprincipper for Sundhedsområdet

### 1.4.4 DS484:2005

# 2 Arkitektur og standarder

Da der fra HR's side ønskes en totalleverance, ønskes følgende generelle betragtninger beskrevet

## *2.1 Integration*

2.1.1 Leverandør skal redegøre for i hvilket omfang det er muligt at interagere med systemet via et API eller afgrænsede services på en måde der gør at skrivning og læsning af data til systemet kun sker med overholdelse af de regler der er defineret i systemets forretningslogik og generelle konfiguration.

2.1.2 Leverandør skal redegøre for dokumentation og tilgængelighed af support i forbindelse med API eller afgrænsede services, hvor Region Midtjylland eller tredje part måtte forestå udvikling eller implementering med andre systemer der skal interagere med

2.1.3 Leverandør skal redegøre for hvilke kommunikationsmetoder systemet kan anvende til system til system kommunikation

2.1.4 Leverandør skal redegøre for hvilke kommunikationsmetoder systemet kan anvende til kommunikation til og fra personer

2.1.5 Leverandør skal redegøre for mulighed for at anvende Region Midtjyllands CPR service.

Region Midtjylland foretager identitetsstyring via BSK som håndterer information om alle brugere, grupper og overordnede roller i regionen. Det drejer sig om ansatte samt personer i et ansættelseslignende forhold. Der ønskes fuld anvendelse af alle relevante data fra BSK.

Data fra BSK kan enten tilgås live via en webservice eller via løs kobling, hvor data synkroniseres med passende mellemrum.

2.1.6 Alle stamdata om brugere og roller i systemet skal vedligeholdes via Region Midtjyllands brugerstamdatakatalog. Det drejer sig om alle stamdata der ikke er unikke for systemet. Som et minimum er der tale om gruppetilhørsforhold, roller, brugernavn og adgangskode.

### *2.1 Infrastruktur*

2.1.1 Der skal kunne anvendes DNS til serveradressering.

2.1.2 Der skal anvendes fully qualified domain names til adressering.

2.1.3 Klienter skal kunne anvende DHCP.

2.1.4 Der skal kunne anvendes IP kommunikation mellem servere og klienter

2.1.5 Tilbudsgiver redegør for hvordan systemet håndterer de sikkerhedsmæssige aspekter omkring håndtering af kommunikation med klienter

### *2.2 Klient og periferi udstyr*

Systemet skal kunne anvendes på Region Midtjyllands standard klient platform. Da der forventes at ske betydelige ændringer på denne platform inden leverance fremsættes der en række generelle krav til klientmiljøet.

2.2.1 Applikationer skal kunne afvikles uden lokale administrative rettigheder

2.2.2 Tilbudsgiver skal redegøre for kendte konflikter med middleware som SUN Java, Microsoft.NET ol.

2.2.3 Tilbudsgiver skal redegøre for hvordan klient software kan afvikles på en Microsoft Windows platform til PC. – min. Win. XP sp3, herunder også krav til installeret middelware eller runtime environments.

2.2.4 Såfremt middleware eller runtime environment anvendes, det kunne f.eks. være SUN Java elle Microsoft .NET, skal der redegøres for hvordan dette miljø til enhver tid kan opretholde den højest mulige sikkerhedsmæssige standard. Herunder hvordan Tilbudsgiver stiller sig til rådighed i forbindelse med sikkerhedsmæssigt funderede opgraderinger af miljøet.

2.2.5 Applikationer, det være sig både webbaserede og lokalt installerede skal kunne afvikles med alle nuværende og kommende anbefalede security patches og updates fra Microsoft.

2.2.6 Tilbudsgiver redegør for krav til installation af tredjepartssoftware på klienter.

2.2.7 Tilbudsgiver skal redegøre for hvorvidt alle systemroller har fuld funktionalitet fra alle installerede versioner og/eller webbaserede versioner af systemet

2.2.8 Enhver bruger der anvender systemet skal være entydigt identificerbar og enhver handling udført fra lokal eller webbaseret klient skal kunne relateres direkte til den udførende bruger ud fra log data.

2.2.9 Tilbudsgiver beskriver muligheden for at afvikle hele systemet eller dele her af via applikations virtualisering, desktop virtualisering og lignende client side virtualiseringsmetoder. (Citrix, terminal services, VDI ol.)

### *2.3 Krav i øvrigt*

2.3.1 Tilbudsgiver skal acceptere, at der skal antivirusprogram valgt af Region Midtjylland på alle enheder på netværket, samt at der løbende udrulles sikkerhedspatches.

2.3.2 Region Midtjylland definerer overvågningsmetoder for klienter og infrastruktur generelt.

2.3.3 Alle arbejdspladser skal kunne installeres med udrulningsværktøj, installation skal derfor kunne håndtere uden brugerinteraktion.

2.3.4 Eksisterende print infrastruktur baseret på Microsoft software skal kunne anvendes

# 3 Sikkerhed

## *3.1 Generelt*

Systemet skal leve op til danske (og internationale) standarder for sikkerhed og overholde krav til sikkerhed og adgangskontrol i standarder på sundhedsområdet.

## *3.2 Adgangskontrol og rettighedsstyring*

Systemets adgangskontrol og rettighedsstyring bør baseres på rolle og organisatorisk enhed med mulighed for individuel tildeling af rettigheder.

3.2.1 Det skal til enhver tid sikres og dokumenteres, at brugerne har adgang til relevante data/funktioner og kun disse. Tilbudsgiver skal beskrive, hvorledes adgangskontrollen er indrettet samt dokumentere, at den lever op til gældende love og regler, (Persondataloven og lovgivning på sundhedsområdet, herunder lov om patienters retsstilling) og redegøre for, hvorledes den administreres.

3.2.2 Der skal være adgangssikkerhed på bruger- og brugergruppeniveau. Visse stamdata på f.eks. organisation, ansættelse m.v. kan kun ændres af autoriseret personale

3.2.3 Tilbudsgiver skal levere redskaber til opfølgning på sikkerheden (logning, præsentation af logs, analyse af logs, hvor der laves analyse af handlingsmønstre for at afdække eventuelt misbrug).

3.2.4 Der skal være passende forholdsregler ved uautoriseret adgang til systemet. Herunder mulighed for at genererer en liste over fejlslagne adgangsforsøg baseret på et brugerdefineret tidsinterval.

3.2.5 Der skal redegøres for muligheden for rollebaseret adgangsstyring.

## *3.3 Ejendomsret til data*

3.3.1 Tilbudsgiver skal redegøre for ejendomsretten til data i systemet som Region Midtjyllands ansatte eller andre betroede personer har produceret.