Systembeskrivelse for Simployer

Driftsplattform

Infotjenester AS (heretter kalt ITAS) drifter i dag HMS-systemer, personalsystemer, personal/lederhåndbøker og andre systemer for mer enn 1000 kunder, hvorav noen er av Norges største selskaper.

ITAS benytter Embriq AS som driftspartner. Dette er en samarbeidspartner med en av landets mest moderne datasentraler i fysisk sikrede lokaler, og våre servere er beskyttet for brann ihht. klasse C1 med redundante aggregater for strøm og kjøling. Embriq har sertifiserte spesialister som bistår med daglig drift og preventivt vedlikehold av operativsystem, brannmur, antivirus og maskinressurser.

Tjenesten består blant annet av:

- Leie av servere og maskinvare
- Vedlikehold av maskinvare samt oppgraderinger av BIOS/Firmware
- Overvåking av maskinvare og operativsystemer (24/7)
- Oppdatering av antivirus-programvare
- Sikkerhetskopiering

Driftspartner kjører offsite sikkerhetskopiering hver natt av samtlige kundedatabaser. ITAS kan på konsulentbasis legge tilbake backup dersom kunden etterspør dette.

ITAS sine underleverandører er ITAS sitt ansvar.

For en detaljert beskrivelse av servicenivå og kvalitet i tjenesten henvises det til gjeldende SLA (Service Level Agreement) og databehandleravtale. ITAS kan tilby graderte nivåer både på SLA og databehandleravtale.

Teknisk oppbygging

Teknisk oppbygging består av en klassisk tre lags struktur, standardisert på Microsoft sine produkter med Microsoft SQL-server, Microsoft Internet Information Server og Microsoft .Net rammeverk som hovedelementer.

Produktet er en ren webapplikasjon som leverer ren HTML til kundens nettleser, og bruker ikke proprietær teknologi på klientsiden (for eksempel Flash).

Kundedata

Hver kunde hos ITAS har sin egen fysiske database. Det vil si at data fra forskjellige kunder aldri blandes i felles databaser.

Tilgang til kundedata

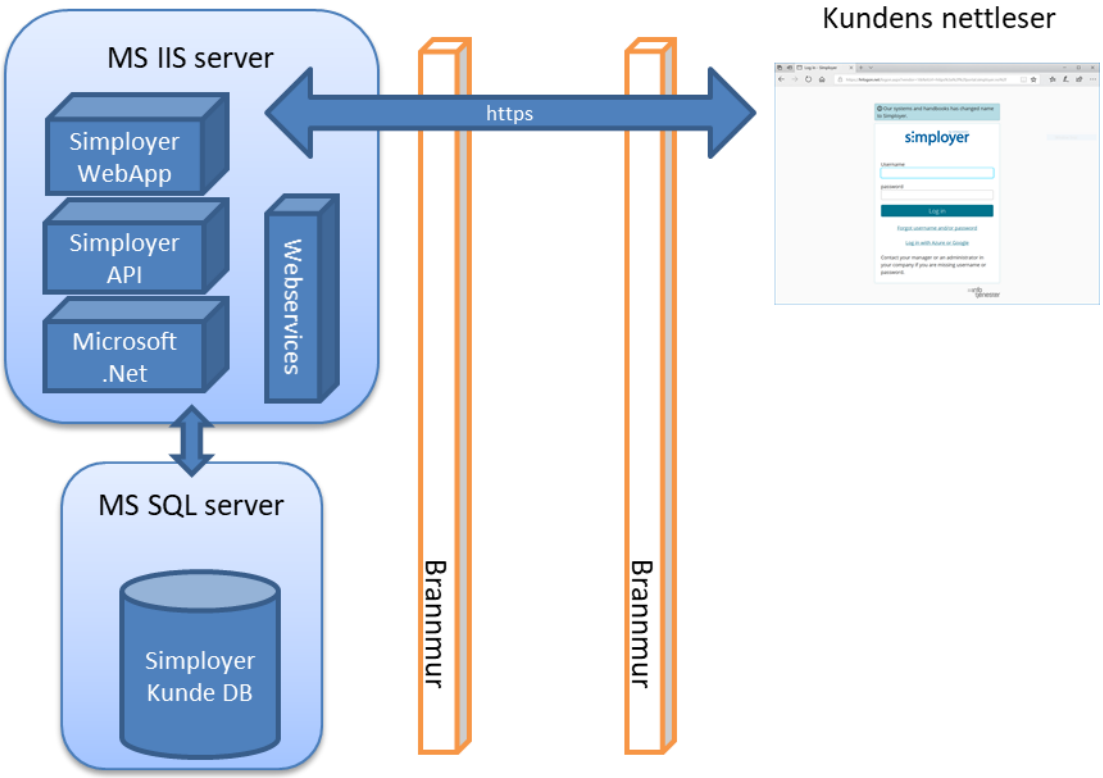
ITAS skiller mellom to forskjellige statuser, «ikke publisert» og «publisert». I en fase hvor kunden tar i bruk systemet og arbeider med å sette det opp, vil statusen være «ikke publisert». I denne fasen vil utvalgte personer hos ITAS ha tilgang til kundens data, slik at kunden enkelt kan få assistanse.

Når systemet er ferdig satt opp, publiseres løsningen. Da vil samtidig alle personer hos ITAS automatisk bli utestengt fra kundens system, og kan ikke lenger logge seg inn i dette. Hvis kunden allikevel ønsker å gi ITAS

tilgang, kan kunden gjøre dette fra systemet. Det kan da gis en tidsbegrenset adgang til en bestemt person hos ITAS.

Kryptering

All kommunikasjon der kundedata flyter over internett er kryptert med SSL (https). ITAS benytter sertifikater fra DigiCert og Commfides.



Systemkrav

Nettleser av nyere versjon som beskrevet i gjeldende SLA (Service Level Agreement)

Standard webtilgang (https på port 443) til aktuelt domene hos ITAS eller ITAS sin underleverandør.

Det er ingen spesielle krav til datamaskinen eller operativsystem.

Moduler

Simployer er et modulbasert personalsystem hvor kunden selv velger hvilke moduler man vil kjøpe. For en

beskrivelse av de forskjellige modulene henvises det til hjemmesiden på https://www.infotjenester.no/hrm-system/

Personalarkiv

Alle applikasjoner fra ITAS som håndterer kundens data har et felles personalarkiv i bunnen. Personalarkivet inneholder informasjon om kundens brukere, og ivaretar sikkerhet og autentiseringsmekanismer.

Integrasjon

Simployer kan integreres med de fleste systemer. For en detaljert beskrivelse av integrasjonsmulighetene henvises det til Simployer sin Wiki på http://wiki.infotjenester.no/display/HRES/Integrasjonsmatrise.

Sikkerhet og personvern

ITAS prioriterer bestandig sikkerhet og personvern når vi utvikler applikasjoner, og vi avtalefester med våre kunder hvilket servicenivå og sikkerhetsregime vi skal levere. Dette reguleres av gjeldende SLA og databehandleravtale.

For generell informasjon om personvern henvises det til Simployer sin Wiki på:
http://wiki.infotjenester.no/display/SOP/Personvern

For generell informasjon om sikkerhet henvises det til Simployer sin Wiki på:
http://wiki.infotjenester.no/display/SOP/Sikkerhet

Standard autentiseringsmetoder

BrukerID og passord

En bruker må være registrert i personalarkivet. Innlogging foregår ved å oppgi brukerid/passord på en tradisjonell innloggingsside. Det er krav til passordstyrken.

Azure Active Directory

Dersom organisasjonen har synkronisert lokal Active Directory med Microsoft Azure (benytter Office 365), så kan Azure AD benyttes til autentisering i håndbøkene. Brukere kan således benytte sin egen jobbkonto for å få tilgang.

Microsoft ADFS

Dersom organisasjonen har satt opp infrastruktur for ADFS (Active Directory Federated Services), kan man benytte ADFS for å autentisere brukere i håndbøkene. Brukere kan således benytte sin egen jobbkonto for å få tilgang.

Google-konto

Personalarkivet har et felt på brukeren hvor man kan definere brukerens Google ID (vanligvis GMail adressen). Dersom dette feltet er definert, kan brukeren logge seg på Simployer via sin Google ID.

Rettigheter

Som standard i Simployer har brukeren lese- og skriverettighet til data om seg selv. De samme rettighetene gjelder for brukerens nærmeste leder. Det finnes imidlertid unntak fra denne regelen hvor brukeren ikke har skriverettighet (f.eks. informasjon om egen stilling), og det finnes unntak hvor brukeren ikke har leserettighet (f.eks. i oppfølging av sykefravær).

Simployer har en hierarkisk avdelingsoppbygging som gjenspeiler kundens organisasjon, og rettigheter arves oppover i hierarkiet.

Roller

Simployer har også en fleksibel rollemodell hvor man kan sette dedikerte roller på tvers av hierarkiet. Hvilke roller som er tilgjengelig er avhengig av hvilke moduler man har kjøpt. For en detaljert beskrivelse av rollene i Simployer henvises det til dokumentasjonen på https://simployersupport.phb.no/