Riktlinjer för IT i fastighetstekniska system

INNEHÅLLSFÖRTECKNING

IT för fastighetstekniska system inom Region Skåne måste följa riktlinjer och policys uppsatta av IT organisationen. Denna riktlinje bygger på detta dokument.

Om frågor som inte belyses av detta dokument uppkommer så går det bra att kontakta Regionfastigheters IT kontaktperson it.regionfastigheter@skane.se

Generellt gäller att all installation ska ske på av Region Skåne levererad hårdvara.

1. Klient

Klientlösning ska stödja Region Skånes klientplattform som baserar sig på Microsofts Windows plattform och följer livcykelplanerna för eKlient i Samverkan (Manualer - Öppen info: E-klient - Confluence (atlassian.net)).

Klientlösningen ska stödja den senaste utgivna servicepack från Microsoft och säkerhetspatchar. Region Skåne har som mål att kritiska patchar från Microsoft ska vara installerade inom 48h.

Om klientlösningen nyttjar Microsoft Office ska lösningen stödja samtliga supporterade versioner av Microsoft Office 365.

Antivirusprogram finns idag på samtliga klienter i Region Skånes klientplattform. Klientlösningen ska fungera ihop med idag förekommande antivirusprogram och aktuell releaseversion (t ex F-secure, Microsoft System Center Endpoint Protection, Norton antivirus, Trendmicro, Kaspersky, McAfee).

Klient delen av lösningen som ska köras på användares datorer bör i sin helhet vara webbaserad.

2. Applikation

Leverantören ska tillhandahålla fullständig systemdokumentation som beskriver bland annat integrationer, komponenter med mera.

Installationsförfarande, hårdvarukrav, mjukvarukrav samt krav på nätverk ska vara väl beskrivna.

Det ska tillhandahållas en IT-driftsdokumentation riktad till Region Skånes IT-driftpartner.

Leverantören ska beskriva vilka övriga beroende mjukvaror från tredjeparts (t.ex. lokal javaklient, databasklient, Acrobat reader etc.) som krävs för klientlösningen utöver operativsystemet och webbläsare. Beskriv produkt, version och leverantör.

Klientdelen av lösningen ska vara oberoende av instickspogram eller 3:e parts tillägg såsom Adobe Shockwave, Adobe Flash och Microsoft Silverlight.

Om klientlösningen kräver en lokal installation på PC klienten ska installationsmediet levereras som MSI filer med stöd för MST för konfigurationsförändringar. För detaljer kring krav se EKLIENT I SAMVERKANS PAKETERINGSPOLICY (Manualer - Öppen info: E-klient - Confluence (atlassian.net)

Klientlösningen bör använda AD (Active Directory) för lagring av användarkonton och autentisering bör göras gentemot densamma. Lösningen bör stödja SSO (Single Sign On)

Klientlösningen ska stödja exekvering i plattform för desktop och applikationspublicering genom Citrix Virtual Apps and Desktops av nuvarande och närmast föregående version.

IT-stödet bör uppfylla de krav på tillgänglighet avseende anpassning för personer med funktionsvariationer som verksamheten ställer på det.

Om IT-stödet innefattar tjänster eller produkter som omfattas av EU:s Tillgänglighetsdirektiv, ska dessa uppfylla de krav på tillgänglighet som ställs i förordningen.

Om hela eller delar av IT-stödet omfattas av lagstiftningen för digital tillgänglighet för webbsidor och mobila appar, ska lagstiftningen följas. Detta inkluderar att säkerställa stöd i gränssnittet för användare med olika former av funktionsvariationer, att genomföra en tillgänglighetsanalys innan upphandling, samt att publicera en tillgänglighetsredogörelse inför driftsättning. Observera att lagkraven gäller webbplatsinnehåll, ljud och video, applikationer, och användargränssnitt oavsett om de vänder sig till externa grupper eller interna användare.

Om IT-stödet innefattar tjänster eller produkter som omfattas av EU:s Tillgänglighetsdirektiv, ska dessa uppfylla de krav på tillgänglighet som ställs i förordningen.

Applikationen ska ej kräva lokala administratorbehörigheter.

Användargränssnittet ska ha svenskt och engelskt språkstöd.

Lösningen ska använda svensk teckenuppsättning.

IT-stödet ska ha en flerskiktad (mer än två skikt) och tjänsteorienterad arkitektur. Definitionen av skikt avser lager i applikationsarkitekturen, dvs presentationslager, affärslager och datalager som kan distribueras till olika fysiska noder.

Klientlösningens åtkomst till datalagret ska enbart ske genom tjänstefasader i ett mellanlager för affärslogik mellan klienten och datalagret.

IT-stödet bör inbegripa ett integrationslager på serversidan för integration av IT-stödets externa tjänster.

Leverantören ska tillhandahålla ett gränssnitt för att leverera den av Region Skånes genererade informationen i IT-stödet på ett standardiserat format, exempelvis XML. Informationen ska vara beskriven, dokumenterad och tolkningsbar utan krav på speciellt systemstöd från leverantörer.

Applikationen ska ha stöd för applikationsövervakning genom exempelvis monitorering, händelseloggar, fel-loggar, övervakning av kritiska systemprocesser, batchjobb eller liknande.

IT-stödet ska livscykelhanteras genom nya versioner så att det följer livscykelplanerna för underliggande infrastruktur och programvaror som exempelvis operativsystem, databashanterare, mellanprogramvara eller andra tredjeparts programvaror.

3. Server

Serverdelen av lösningen ska kunna exekveras på en av Region Skånes standardiserade serverplattformar. Dessa är Microsoft Windows Server av nuvarande och närmast föregående version, samt SUSE Linux 15 SP2 eller senare eller Red Hat Linux 8 eller senare.

Leverantören av serverlösningen ska kontinuerligt stödja supportplan från operativsystemsleverantör. Beskriv hur.

Samtliga komponenter i serverdelen av lösningen ska fungera i virtualiserad servermiljö på VMWare vSphere av nuvarande och närmast föregående version och Microsoft Hypervisor av nuvarande och närmast föregående version.

Serverdelen av lösningen ska stödja operativsystemets senaste utgivna servicepack och säkerhetspatchar. Region Skåne har som mål att kritiska säkerhetspatchar ska vara installerade inom 48 h.

Serverdelen av lösningen ska fungera ihop med idag förekommande antivirusprogram och aktuell releaseversion (t ex F-secure, MS ForeFront, Norton antivirus, Trendmicro, Kaspersky, McAfee).

Anbudsgivaren ska beskriva vilka mjukvaror i övrigt som krävs för IT-stödets serverlösning (ex separat databasmotor, integrationsprogramvara etc.) samt versionskrav eller dylikt.

Databas bör stödja MS SQL Server 2018 eller senare.

IT-stödet ska ha en transaktionshantering som medför möjlig säkerhetskopiering i full drift av databas, eventuell applikationsserver som är del av IT-stödet och fullständig konfiguration utan att samtidig tillgång till IT-stödet och dess funktionalitet hindras.

Komponenter i affärslager, integrationslager eller databaslager av lösningen ska kunna köras i en bakgrundsprocess (Windows Service eller liknande), dvs den ska ej kräva en på loggad konsol eller liknande förgrundsprocess på servern.

Server tillhandahålls av Region Skåne, leverantören ska redovisa hårdvarukrav för server.

Serverlösningen för IT-stödet bör gå att skala upp genom att lastdela på flera servrar.

Samtliga skikt i serverlösningen för IT-stödet bör kunna ge feltolerans genom flera servrar. Leverantören ska beskriva hur och eventuella krav på infrastrukturen som ställs från IT-stödet. Leverantören ska inkomma med beskrivningen i anbudet, som en bilaga.

4. Säkerhet

Andra externa anslutningar till Region Skåne än den VPN-tjänst (med tillhörande regelverk och instruktioner) som tillhandahålls av Region Skåne, godkännes ej.

Leverantören ska specificera vilket typ av backup som krävs för att kunna återställa systemet.

Endast av Region Skånes på förhand godkända trafikvägar ska tillåtas till/från samt inom Region Skånes nätverk. Godkännande av trafikvägarna hanteras med hjälp av brandvägg. För respektive trafikväg ska åtminstone ursprung, destination, protokoll och port vara kontrollerade/hanterade.

Applikationer som utvecklas till mobila enheter ska följa livscykeln för respektive mobilt operativsystem (iOS och Android). Detta gäller både för operativsystemversion och versioner av säkerhetsuppdateringar.

Personal och eventuella samarbetspartners ska informeras om sitt ansvar och vara bundna till att rapportera alla informationssäkerhetsincidenter skyndsamt. Informationssäkerhetsincidenter ska rapporteras via fördefinierade kommunikationskanaler i god tid och i enlighet med gällande lagstadgade skyldigheter.

All form av digital kommunikation mellan leverantörens IT-stöd och system i Region Skånes miljö ska initieras från Region Skåne. Dvs ingen kommunikation får lov att initieras från Internet/DMZ direkt in mot RSNET. Ifall en sådan kommunikation är nödvändig så ska Region Skånes relätjänst användas (vilket kräver att 2xSSL med SITHS-certifikat används)

Lösenord, felaktiga lösenord, krypteringsnycklar eller annan känslig information får inte kommuniceras, synas eller överföras i klartext. Informationsöverföring över nätverk ska kunna skyddas från insyn och förvanskning vilket innebär att kommunikation som sker över nätverk mellan olika delar av IT-stödet (ex. mellan klient och server) samt mellan IT-stödet och andra IT-stöd ska kunna krypteras. Gäller även integrationer.

Autentisering av aktörer till IT-stödet ska kunna ske genom en stark autentisering. Leverantören ska på begäran av Region Skåne säkerställa att autentisering för en specifik aktör/roll enbart kan ske genom stark autentisering. Förtydligande: Med stark autentisering avses e-identitetsbaserad multifaktorautentisering där personens identitet ska ha säkerställts på ett tillräckligt säkert sätt (LOA 3) i samband med utfärdande av dennes e-identitet.

Autentisering till IT-stödet på PC-klienter bör kunna ske genom stark autentisering via SITHS-kort/RS-kort som bygger på SITHS-PKI (SITHS CA).

Default-lösenord så som "admin", "password" m.m. ska inte användas.

IT-stödet ska designas, utvecklas och testas i enlighet med ledande branschstandard såsom t.ex. OWASP (för webbapplikationer), Secure coding guidelines och Securtiy Development Lifecycle (SDL, Microsoft).

En av Region Skånes tillhandahållen tidskälla (NTP) ska användas för att synkronisera systemklockorna i alla relevanta informationshanteringssystem för att underlätta spårning och rekonstruktion av aktivitetstidslinjer.

Varje operativsystem ska härdas för att endast tillåta nödvändiga portar, protokoll och tjänster. Härdning ska löpandes uppdateras och konfigureras enligt de

rekommenderade riktlinjer som leverantörer och institut ger ut (t.ex. NIST-guidelines och Microsoft Premier RAP Health Checks).

Policyer och åtgärder ska finnas etablerade för att begränsa och förhindra installation av otillåten programvara på klienter (arbetsstationer, bärbara datorer, mobila enheter m.m.) som används för att hantera eller administrera Region Skånes information, system eller infrastrukturkomponenter.

Det ska finnas etablerade policyer och förfaranden för att stödja processer och tekniska åtgärder som möjliggör skydd av känsliga data som lagras (t.ex. filservrar, databaser, arbetsstationer), används (arbetsminne) och överförs (t.ex. vi systemgränssnitt över nätverk, elektroniska meddelanden).

Leverantören ska följa branschstandard avseende signering och kryptering av data t.ex. Advanced Encryption Standard (AES) och Transport Layer Security (TLS) samt för livcykelhantering av de certifikat och nycklar som används för kryptering, t.ex. NIST SP 800–131 A

Vid nyttjandet av certifikat så ska följande kontroller utföras oavsett om IT-stödet saknar uppkoppling till internet:

- Kontroll av giltighetstid av användarens och/eller funktionens certifikat ska utföras och åtkomst ska endast ges om giltighetstiden för certifikatet ifråga motsvarar tidpunkt för aktuell åtkomst.
- Revokeringskontroll ska göras av användarens och/eller funktionens certifikat och åtkomst ska endast ges om certifikatet i fråga inte har revokerats.
- Kontroll av certifikatutgivaren (CA) av användarens och/eller funktionens certifikat ska utföras och åtkomst ska endas ske ifall utgivaren är en av Region Skåne godkänd CA.

Åtkomst till egenutvecklade program, applikationer, källkod eller någon annan form av immateriellt ägande och användande av proprietär programvara ska begränsat enligt regeln om least privilege.

En process för incidentrapportering och -hantering ska finnas för att mildra effekter, förhindra upprepande och underlätta återgång till verksamhet på normal nivå då någon form av säkerhetsincident skett. Om en extern leverantör hanterar någon del av Region Skånes informationstillgångar ska det finnas rutiner för hur leverantören ska kommunicera och samarbeta med Region Skåne kring incidenter

Leverantören, såväl internt som med externa parter, ska följa en definierad process för att säkerställa kvaliteten för change control, release och test (som t.ex. ITIL) så att enbart auktoriserade, testade och dokumenterade förändringar görs på IT-stödet, underliggande infrastruktur eller dess gränssnitt

Varje användare ska ha ett unikt identifierbart användarkonto och åtkomst och behörigheter ska vara baserade på vad användaren behöver för att kunna utföra sitt arbete. Användare ska inte ha större befogenheter i IT-miljön än vad som behövs för det dagliga arbetet.

IT-stödet ska kunna presentera rapport över vilka behörigheter varje konto har.

Säker identifiering av utrustning (så som infrastrukturkomponenter, arbetsstationer etc.) ska användas för att validera/verifiera riktigheten av utrustning och att utrustningen är känd (t.ex. genom certifikat).

5. Nätverk

Lösningen ska endast kommunicera med hjälp av nätverksprotokoll baserade på TCP/IP. Om andra protokoll krävs ska denna fråga lyftas till Regionfastigheters IT kontaktperson it.regionfastigheter@skane.se

Leverantören ska beskriva vilka portar, kommunikationsvägar samt protokoll som används mellan samtliga ingående komponenter i lösningen i form av en skiss. Det ska framgå av ritningen vart trafik initieras och vilken riktning den går.

Leverantören ska beskriva om lösningen kommer kommunicera via internet.

Leverantören ska säkerställa att ingen nätverksutrustning (ex. switch, router, brandväggar) ingår i leveransen. Det är inte tillåtet att ansluta egna switchar, routers eller brandväggar i Region Skånes nätverk.

Samtliga enheter som ingår i leverans ska ha stöd för ipv4 och bör ha stöd för ipv6.

Om det finns specifika krav på bandbredd och svarstider (t.ex RTD, Jitter, packetloss) mellan några av delarna i lösningen ska leverantören redovisa dessa kraven.

Leverantören ska beskriva om det finns någon utrustning som har behov av multicast i nätverket och mellan vilka enheter denna trafik går.

Enheterna bör stödja WPA2-Enterprise med 802.1X authentication, samt EAP-TLS för autentisering till det trådbundna nätverket.

Enheterna ska stödja autentisering till det trådbundna nätverket med MAC-adress om inte utrustningen kan uppfylla kravet kring 802.1X authentication, samt EAP-TLS för autentisering till det trådbundna nätverket.

Om lösningen kommunicerar via trådlöst nätverk ska lösningen använda Region Skånes befintliga SSID.

Om Enheterna inte kan stödja WPA2-Enterprise med 802.1X authentication och EAP-TLS ska enheterna minst ha stöd för WPA2 Personal. Om det är så att enheten inte klarar WPA2-Enterprise ska detta beskrivas.

Enheter bör stödja WPA2-Enterprise med 802.1x autentisering samt EAP-TLS för autentisering till det trådlösa nätverket.

Utrustningen får inte ställa lägre krav än 67db på primären och 67 db på sekundären

Leverantören ska beskriva om det finns behov samt orsaken till lastballansering av lösningen. Lastballanseringstjänsten tillhandahålls av Region Skåne

Lösningen får inte kräva ett separat vlan.

Region Skåne tillåter ej att leverantör installerar egna fysiska nätverk.

Utrustning som ansluts till nätverk ska klara av att kommunicera men andra nät/subnät (layer3)

Utrustning som ansluts till nätverk ska kunna bli tilldelad IP-adress och DNS-servrar via DHCP, inklusive ”infinitive lease time” om systemet kräver att utrustningen erhåller samma IP-adress på subnätet

Nätverkskortet ska kunna förhandla fram full-duplex via autonegotiation

Utrustning som ansluts bör i framtiden kunna autentisera sig med certifikat via 802.1x

Utrustning som ansluts till nätverk ska kunna skicka och svara på ARP

6. Integration

Leverantören ska beskriva (redogör för gränssnitt) hur koppling mellan IT-stödet och andra fristående komponenter hanteras och vilka möjligheter IT-stödet erbjuder.

IT-stödets integrationsarkitektur ska stödja följande standarder för tjänsteorienterad integration: Soap 1.2, Rest (https), HL7, OPC UA eller WDSL 2.0

För webbapplikationer bör autentiseringen bygga på de nationella säkerhetstjänsterna och användning av protokollet SAML WEB SSO.

IT-stödet bör kunna integrera till av Region Skåne tillhandahållet externt användarregister för autentisering och styrning av behörigheter.

IT-stödets externa integrationsgränssnitt bör vara dokumenterade enligt branschstandard. Dokumentationen bör innehålla Anrops och svars exempel

Det ska vara möjligt att avropa tekniskt stöd för anslutning och integration till IT-stödets externa integrationsgränssnitt inom avtalet.

7. Övrigt

Leverantören ska erbjuda support och användarstöd via telefon, e-mail, webbsida eller liknande för felanmälan, rådgivning kring IT-stödets användning eller tekniska frågeställningar och problem.

Fysiska lås (USB, RS232) m.fl är ej tillåtna

Testdatabaser innehållandes personuppgifter eller uppgifter av annan känslig natur får ej lämna Region Skånes infrastruktur. Endast fiktiv eller godkänt avidentifierad information får lämnas ut för att hanteras i leverantörers test- och utvecklingssystem.

Leverantören ska kunna redogöra för hur de och dess underleverantörer hanterar personuppgifter samt var dessa lagras. Vid behov ska PUB-avtal upprättas och i detta måste det:

- Framgå uttryckligen att svensk lag gäller för behandlingen av personuppgifter.
- Finnas en garanti att uppgifter inte används för några andra ändamål än desom krävs för att leverera tjänsten som har avtalats.
- Säkerställas att underleverantörer hela tiden är redovisade och att nya underleverantörer ska redovisas i förtid.

- Möjliggöra frånträde från avtal om en underleverantör anlitas och som inte accepteras av Region Skåne (detta innebär att det måste finnas en faktisk möjlighet att frånträda avtalet)
- Säkerställas att molnleverantören tillåter en säkerhetsuppföljning av en utomstående och pålitlig part.
- Framgå att personuppgiftsbiträdet har ett skadeståndsansvar gentemot den personuppgiftsansvarige (Region Skåne)
- Säkerställa att behörighetssystem upprätthålls och att spårbarhet för åtkomst (loggning) sker.
- Finnas garantier för att uppgifter som Region Skåne har för avsikt att radera faktiskt raderas inom en viss tidsperiod.
- Möjliggöras för att Region Skåne att ha åtkomst till loggar och andra uppgifter för egen uppföljning.