Beslut om baskrav vid upphandling av system och tjänster med IT-komponenter

Beslut

Linköpings universitet (LiU) beslutar att fastställa baskrav vid upphandling av system och tjänster med IT-komponenter. Baskraven utgör en katalog över möjliga IT-krav att ställa och ska användas i samband med upphandling och annan anskaffning av system och tjänster med IT-komponenter.

Skäl till beslut

Enligt Linköpings universitets riktlinjer för IT-säkerhet (LiU-2018-01814) ska krav på informationssäkerhet ställas för att säkerställa efterlevnad av tekniska aspekter i riktlinjerna. Genom väl övervägd tillämpning av baskraven vid upphandling och anskaffning av system och tjänster med IT-komponenter säkerställs att riktlinjer för informationssäkerhet efterlevs samt att aspekter kring användarvänlighet, effektivitet och kompabilitet vid integration med universitetets övriga IT-miljö beaktas.

Handläggningen av beslutet

Detta beslut har fattats av IT-direktör Joakim Nejdeby efter föredragning av systemingenjör Johannes Hassmund.

Joakim Nejdeby

Johannes Hassmund

Kopia till:
Upphandlingsenheten
Universitetsledningen
Dekaner

Kanslichefer
Prefekter
Adm chefer
UDL
Universitetsbiblioteket
Internrevisionen
Fackliga företrädare
LiU-Nytt
Regelsamlingen

Baskrav vid upphandling av system och tjänster med IT-komponenter

Sammanfattning

Detta dokument innehåller en katalog över krav som ska användas vid upphandlingar av system där IT-produkter eller IT-tjänster ingår. Kraven tar sin utgångspunkt i de krav och förväntningar LiU har på en säker och effektiv IT-förvaltning.

Närmare läsanvisningar och information om tillämpningen av katalogen återfinns i avsnitt 1. Avsnitt 2 och framåt innehåller konkreta krav.

Eftersom kravställning av denna typ av system ofta är mycket komplex, särskilt i de fall det upphandlade systemet interagerar med andra system, är det viktigt att IT-avdelningen alltid är med och utformar kraven i varje upphandling.

Detta dokument ersätter inte en dialog med IT-avdelningen och kan inte användas i sin helhet i ett förfrågningsunderlag. Ett urval måste göras eftersom dokumentet annars innehåller motstridiga krav.

Katalogen innehåller, förutom allmänna krav, krav på informationssäkerhet. För dessa krav är katalogen att betrakta som en interimslösning till dess att en process för informationssäkerhet i upphandlingar är fastställd. Arbete med detta pågår.

Denna version av katalogen är fastställd 2018-10-31. Katalogen revideras med ett intervall om ett till två år.

Historik

2015-06-02	Första versionen
2016-10-17	Reviderad version. Förtydliganden bl.a. kring tillgänglighet, kryptografiska metoder, och inverkan av informationsklassning.
2016-12-15	Klargöranden om hur dokumentet ska användas.
2018-10-31	Större revision framförallt utifrån Riktlinjer för informationssäkerhet dnr LiU-2018-01814.

Innehåll

1 Introduktion

Detta dokument innehåller från avsnitt 2 och framåt en katalog över IT-relaterade krav som ska användas vid upphandlingar av system där IT-produkter eller IT-tjänster ingår.

Katalogen är baserad på Riktlinjer för informationssäkerhet vid Linköpings universitet (Dnr LiU-2018-01814), Beslut om stärkt informationssäkerhet på LiU (Dnr LiU-2014-00052), samt erfarenhet från tidigare upphandlingar och system.

Samtliga krav är obligatoriska om annat ej anges. Vissa krav styrs dock av informationsklassning på den information systemet ska hantera, medan andra krav valfritt kan tillämpas baserat på aktuellt behov. Utöver kraven i katalogen kan andra IT-relaterade krav behöva ställas. Flera avsnitt i katalogen innehåller vägledning kring detta.

Katalogen ersätter inte en dialog med IT-avdelningen. Notera att dokumentet inte kan användas i sin helhet i ett förfrågningsunderlag eftersom det innehåller motstridiga krav och information som inte är riktad till anbudsgivare.

IT-avdelningen ska rådfrågas i samtliga upphandlingar där IT-produkter eller IT-tjänster är en komponent. Eftersom kravställning av i dessa upphandlingar kan vara mycket komplex ska kontakt med IT-avdelningen tas i god tid.

1.1 Informationsklassning

Inför varje upphandling bör en inventering göras av vilka informationstillgångar det upphandlade verktyget eller systemet kommer att hantera. Dessa informationstillgångar klassificeras sedan enligt universitetets ledningssystem för informationssäkerhet. Klassningen ligger till grund för att avgöra vilka krav i denna katalog som kan uteslutas.

Kontakta gärna universitetets IT-säkerhetsgrupp för att få hjälp att genomföra inventering och informationsklassning.

1.2 Avstämning med IT-säkerhetsgruppen under kravställning

Under arbete med kravställning i berörda upphandlingar ska användningen av denna kravkatalog stämmas av med IT-avdelningen. Undantagsvis kan IT-avdelningen efter sådan avstämning meddela att vissa obligatoriska krav kan justeras eller utelämnas helt.

1.3 Särskilda anvisningar avseende molntjänster

Om upphandlingen innefattar molntjänst och denna kommer att bearbeta information klassad med **höjd konfidentialitet**, **höjd riktighet**, **höjd tillgänglighet** eller **känsliga personuppgifter** så ska avstämning göras med universitetets informationssäkerhetssamordnare **innan** upphandlingen inleds.

1.4 Typografiska konventioner

Ej obligatoriskt

I katalogen finns anteckningar som anger när krav inte är obligatoriska. Detta indikeras genom en marginalnotering (exempel till vänster).

I ett flertal krav ska leverantören redogöra för hur man uppnår exempelvis önskat skydd. Detta indikeras genom en fetmarkering av uppmaningen samt markering med symbol enligt nedanstående exempel:

Beskriv hur önskat skydd uppnås.

Särskilda instruktioner till läsaren, som inte är en del av kravformuleringarna, presenteras i tabellform enligt nedan:

Exempel på information till läsaren

Denna ruta innehåller detaljerad information om hur och när krav tillämpas eller annan information som särskilt bör beaktas i katalogens användning. Denna typ av text ska **inte** tas med i förfrågningsunderlag.

1.5 Begränsningar

Juridiska krav som påverkar IT, exempelvis regleringar rörande arkivering, patientdata och liknande hanteras inte i denna katalog. Krav som rör hantering av personuppgifter hanteras delvis. Se LiU:s riktlinjer för personuppgiftsbehandling för ytterligare information om personuppgiftsbehandling.

1.6 Giltighetstid

Kravkatalogen ses över löpande. Den senaste versionen av katalogen finns tillgänglig på webbsidan nedan:

https://insidan.liu.se/informationssakerhet/kravkatalog

2 Klienters IT-miljö

2.1 Krav avseende webbaserade system

Obligatoriska endast om systemet som avses är webbaserat (gäller samtliga krav under 2.1).

Tillämpning av krav avseende webbaserade system

System bör normalt stödja både traditionella klientdatorer och mobila enheter. Om systemet inte behöver stödja mobila enheter kan kraven nedan anpassas så att Android och iOS inte nämns.

2.1.1 Stöd av webbläsare

Webbaserade system ska under hela avtalsperioden fungera med nedanstående webbläsare och plattformar:

- Edge (Windows)
- Chrome (Windows, MacOS, Linux, Android)
- Firefox (Windows, MacOS, Linux)
- Safari (MacOS, iOS)

2.1.2 Stöd för löpande uppgradering av webbläsare

Leverantören ska säkerställa att systemet löpande fungerar med den vid varje tillfälle gällande (det vill säga den senaste) versionen av webbläsarna enligt krav 2.1.1. LiU uppgraderar webbläsare i takt med att nya versioner blir tillgängliga.

2.1.3 Plugins i webbaserade system

Systemet får inte ställa krav på plugins i webbläsare. Systemet ska fungera med webbläsare enligt 2.1.1 med standardinstallation. Detta innebär att systemet till exempel inte får kräva webbläsarplugin för Java, Flash, Silverlight, ActiveX eller liknande.

2.1.4 Inställningar i klienters operativsystem

Webbaserade system ska under hela avtalsperioden fungera utan särskilda inställningar eller säkerhetspolicys på klienten. Detta innebär att systemet ska fungera med webbläsare enligt krav 2.1.1 på nyinstallerad dator eller enhet utan vidare justeringar.

2.2 Klientbaserade komponenter

Tillämpning av klientbaserade komponenter

Krav under rubrik 2.2 tillämpas om systemet innehåller komponenter bestående av fristående programvaror tänkta att installeras på användares klienter.

Programvaror som ska köras av en mycket stor mängd användare bör finnas tillgängliga på samtliga plattformar som stöds vid LiU (se 2.2.2).

Om programvaran rör en mer specifik användargrupp väljs lämpliga operativsystem som ska stödjas. I dessa fall måste krav 2.2.1 till och med 2.2.4 anpassas.

2.2.1 Säker leverans av klient

Tillämpning av säker leverans av klient

Detta krav kan tillämpas om klientprogramvaran ska användas av en begränsad grupp användare. I så fall kan flera efterföljande krav strykas i och med att klienten kommer att köras i leverantörens miljö.

Ej obligatoriskt.

Om en så kallad klient används inom lösningen, ska leverantören tillhandahålla en säker och tillförlitlig leverans av denna klient, till exempel genom användning av Citrix Metaframe.

2.2.2 Plattformar som ska stödjas

Eventuell klientprogramvara ska fungera på minst följande operativsystem:

- Windows (10)
- OS X (10.12 och senare)
- Ubuntu Linux (16.04, 18.04)
- CentOS / RHEL (version 6 och 7)

Klientprogramvaran ska under avtalsperioden löpande underhållas så att den fungerar med minst de två senaste versionerna av Windows 10, OS X, Ubuntu Linux LTS och CentOS / RHEL.

2.2.3 Mobila plattformar som ska stödjas

Ej obligatoriskt om mobila plattformar inte ska stödjas eller om lösningen används av en homogen grupp användare.

Eventuell programvara för mobila plattformar (appar) ska fungera på minst följande system:

- iOS (11 och 12)
- Android (8.x - 9.x)

Programvaran ska under avtalsperioden löpande underhållas så att den fungerar med minst de två senaste versionerna av iOS, och Android.

2.2.4 Paketering av programvara

Programvaror ska kunna paketeras för automatiserad installation. Detta innebär att installation programvaror ska kunna genomföras i bakgrunden och utan interaktiv inblandning av användaren eller tekniker. Även eventuell licensaktivering ska kunna ske i bakgrunden.

- Program avsedda att köra på Windowsklienter ska kunna MSI-paketeras.
- Program avsedda att köras på MacOS ska kunna paketeras som .PKG-filer.
- Program avsedda att köras på Ubuntu ska kunna paketeras för installation med dpkg.
- Program avsedda att köras på CentOS/RHEL ska kunna paketeras för installation med rpm.

2.2.5 Krav på underliggande operativsystem

Löpande patchning av operativsystem och andra programvaror (webbläsare, Java, Adobe Flash och liknande) ska tillåtas och får inte utgöra ett hinder för användning av programvaran.

2.2.6 Kodsignering

Programvaran ska vara signerad med ett certifikat utfärdat av en betrodd utgivare. Det ska inte krävas installation av ytterligare rotcertifikat i klienten för att validera signaturen.

2.2.7 Kompatibilitet med säkerhetsmekanismer

Programvaran ska gå att använda utan begränsningar även om Applocker, device guard, eller Emet används (gäller enbart Windows). Programvaran ska vara kompatibel med Windows Defender och System Center Endpoint Protection.

2.2.8 Administratörsbehörigheter

Programvaran ska inte kräva att användaren har särskilda behörigheter, till exempel administratörsbehörigheter, på datorn där den körs.

2.2.9 Installationsplats

Programvaran ska installeras på operativsystemets normala plats(er). Programvaran ska inte installeras i användarens profilkatalog.

2.2.10 Säkerhetsinställningar

Programvaran ska inte kräva undantag i säkerhetsinställningar i operativsystem. Det innebär till exempel att det inte får krävas gammal programvara, inställningar av betrodda webbplatser, undantag i säkerhetsprogram eller liknande.

2.2.11 Servertjänster

Om en tjänst har som primärt syfte att agera server ska detta istället paketeras som en serverlösning.

Programvara som körs på klienter ska fungera som kravställt utan att ta emot inkommande anslutningar via nätverket.

2.2.12 Distanssupport

Om leverantören erbjuder distanssupport ska supporten använda en av LiU:s IT-avdelning godkänd programvara.

3 Användarhantering och inloggning

Tillämpning av användarhantering och inloggning

Normalt ska krav 3.2 tillämpas på system som riktar sig till flertalet medarbetare.

Krav 3.3 är främst tillämpbart på klientbaserade system utan egen lösenordsdatabas, som gör automatisk inloggning (vanligt på t.ex. telefoner och läsplattor) och inte har en egen användardatabas.

Krav 3.4 bör förekomma endast i undantagsfall, och aldrig i system som riktar sig till flertalet medarbetare eller studenter vid LiU.

För vissa mer komplexa system kan det vara nödvändigt att använda flera krav. Till exempel kan 3.2 tillämpas på normalanvändare, 3.4 tillämpas på expertanvändare och 3.3 tillämpas på access från mobila klienter.

Det kan även finnas fall, framförallt i särskilt känsliga system, där andra former av tvåfaktorautentisering kan krävas. **Rådgör alltid med IT-avdelningen i dessa frågor.**

3.1 Personliga användarkonton

Användarkonton ska vara personliga.

3.2 Federerad inloggning (SSO)

Utesluter normalt 3.4 och kan utesluta 3.3. Se vägledningen ovan.

Användare ska logga in i systemet genom LiU:s ADFS (SSO) som kan använda tvåfaktorautentisering. Autentisering ska kunna ske såväl med AD vid LiU som Azure AD.

3.3 Tillämpningsspecifika lösenord

Utesluter normalt 3.4.

System som sparar inloggningsuppgifter (t.ex. e-postklienter, IM-klienter eller liknande) och därmed inte har stöd för tvåfaktorautentisering ska kunna använda tillämpningsspecifika lösenord som genereras av Active Directory.

3.4 Lokal användardatabas

Ska normalt inte användas. Utesluter normalt 3.2 och 3.3. Se vägledningen ovan.

Systemet ska hantera användare genom lokal användardatabas. Inloggning får inte göras genom uppslag mot LiU:s användarkatalog exempelvis genom bindning mot AD eller LDAP. Användaridentiteten ska inte likna LiU-ID eller e-postadress.

3.4.1 Lösenordslängd

Systemet ska inte tillåta lösenord kortare än 10 tecken. Systemet ska tillåta godtyckliga lösenordslängder mellan 10 och 64 tecken. Systemet får tillåta lösenord som är längre än 64 tecken.

3.4.2 Överföring av lösenord

Lösenord ska överföras säkert. Lösenord får inte överföras okrypterat vilket exempelvis innebär att de inte får skickas via e-post.

Beskriv hur lösenord överförs.

3.4.3 Lagring av lösenord

Lösenord för lokal användardatabas ska lagras kodade på ett icke reversibelt sätt.

Beskriv hur lösenord lagras.

Undantag

Undantagsvis kan det av tekniska skäl vara nödvändigt att tillåta lagring av lösenord på ett reversibelt sätt (till exempel i klartext). Kontakta IT-säkerhetsgruppen för rådgivning.

3.4.4 Lösenordsåterställning

Lösenordsåterställning ska göras på ett säkert sätt (till exempel genom engångskod).

Beskriv hur lösenordsåterställning sker.

3.4.5 Användares möjlighet att byta lösenord

Användare ska kunna byta lösenord; antingen genom att själva välja ett nytt lösenord eller genom att systemet slumpar ett nytt lösenord åt användaren.

3.4.6 Periodiska lösenordsbyten

Periodiska lösenordsbyten ska **inte** krävas.

Ej obligatoriskt.

3.4.7 Lösenordskomplexitet

LiU ska kunna ange en policy för komplexitet på lösenord (till exempel antal tecken och antal teckenklasser som måste ingå, förbud mot upprepning av tidigare använda lösenord).

3.5 Tvåfaktorsautentisering

Ej obligatoriskt.

Tvåfaktorautentisering ska användas vid inloggning i systemet.

Beskriv vilka metoder för tvåfaktorautentisering som erbjuds.

3.6 Auktorisering

Tillämpning av auktorisering

Auktorisering kan ske på olika sätt beroende på hur systemet interagerar med LiU:s infrastruktur. System som autentiserar genom ADFS eller tillämpningsspecifika lösenord ska använda auktorisering via AD-grupper.

I övriga system behöver kravet anpassas till den specifika upphandlingen.

3.6.1 Auktorisering av användare ska ske via AD-grupper

Auktorisering av användare ska kunna ske genom användning av grupper i LiU:s Active Directory. Grupptillhörighet ska alltså kunna styra rättigheter i systemet. Systemet ska ha stöd för nästlade grupper. Grupptillhörighet kan ges genom attribut i inloggningstoken, uppslag på LiU:s AD, eller API-anrop mot LiU:s Azure AD.

3.6.2 Granskning av behörigheter

Endast tillämpbart då krav 3.6.1 inte används för samtliga användare.

LiU ska kunna begära ut en rapport över samtliga användare med anknytning till LiU samt deras behörigheter i systemet.

3.7 Begränsning av åtkomst till valda IP-adresser

Ej obligatoriskt.

Åtkomst av systemet ska endast kunna ske från av LiU angivna IP-adresser eller nätverk.

3.8 Lista över användare

LiU ska kunna begära ut lista över samtliga användare med anknytning till LiU. Listan ska innehålla koppling till antingen LiU-ID eller e-postadress vid LiU.

3.9 Tillfälligt stänga konto

Leverantören ska kunna stänga användarkonton tillfälligt på LiU:s begäran, alternativt ska det finnas ett gränssnitt där LiU kan genomföra sådan stängning.

3.10 Radering av konto

Leverantören ska kunna radera konton på LiU:s begäran, alternativt ska det finnas ett gränssnitt där LiU kan genomföra sådan radering.

4 Allmänna säkerhetskrav

4.1 Korrekt tid

Detta krav bör utgå vid upphandling av system som kör på LiU:s datorer (klienter eller servrar), men det är viktigt vid upphandling av system som kör på specialdatorer eller hos leverantören. Andra meningen i kravet kan utgå om man vet att systemet inte kommer att köra på LiU:s datorer.

System och tjänster som ingår i anbudet ska under hela avtalsperioden ha korrekt tid, till exempel genom att använda NTP för tidssynkronisering. System som kör på LiU:s datorer (klienter och servrar) och använder systemets klocka anses uppfylla detta krav.

4.2 Backuper

4.2.1 Backuper

Leverantören ska ta backup på data i systemet minst en gång per dygn till en plats som är fysiskt skild från den där driften av huvudsystemet sker, eller på annat sätt säkerställa motsvarande eller högre nivå av datasäkerhet.

Beskriv rutiner.

4.2.2 Tid för återläsning

Tillämpning av tid för återläsning

Anpassa tidsgränserna till behoven i det aktuella systemet.

Vid normalt driftsavbrott ska systemet kunna återställas inom 4 timmar. Vid större händelse ska katastrofåterställning kunna ske inom 24 timmar.

4.2.3 Test av katastrofåterställning

Leverantören ska kunna återställa tidigare version av systemets data. Leverantören ska ha rutiner för att säkerställa att sådan återställning kan genomföras framgångsrikt.

Beskriv rutiner.

4.2.4 Skydd av backuper

Backuper ska skyddas mot otillbörlig tillgång och förändring.

4.3 Lagring av data

4.3.1 Krypterad lagring

Endast obligatoriskt om systemet hanterar information klassad med **höjd konfidentialitet** eller **känsliga personuppgifter**.

Data ska lagras krypterat. Krypteringsnycklar ska vara skyddade från obehörig åtkomst.

4.3.2 Destruktion av lagringsmedia

Leverantören ska ha säkra rutiner för radering eller destruktion av lagringsmedia då media som innehållit LiU:s uppgifter avyttras eller skrotas. Rutinerna ska även tillämpas efter att avtal med LiU avslutats eller upphört att gälla. Som lagringsmedia räknas alla former av fysiskt media, även papper.

Beskriv rutiner för destruktion av lagringsmedia.

4.4 Kommunikationssäkerhet

Tillämpning av krav 4.4.1 och 4.4.2

Krav 4.4.1 ska användas som systemet överför **särskilt skyddsvärd information**. Krav 4.4.2 kan användas om systemet endast överför information som inte är särskilt skyddsvärd. Om man på förhand vet vilken information som systemet hanterar som är **särskild skyddsvärd** kan kravet preciseras så att kryptering endast krävs för denna information.

4.4.1 Kryptering av överförda data

Information som sänds över nätverk ska vara krypterad med vedertagen säker metod, till exempel TLS 1.2 eller senare.

4.4.2 Kryptering av överförda data

Leverantören ska redovisa vilka typer av data som kan komma att överföras okrypterat samt motivera varför kryptering av sådana data inte är nödvändigt. Eventuell krypterad överföring ska göras med vedertaget säkra metoder, till exempel TLS 1.2 eller senare.

4.4.3 Certifikatvalidering

Vid användning av krypterad överföring ska det finas skydd mot så kallade ”man-in-the-middle”-angrepp, till exempel genom validering av server- eller klientcertifikat.

Beskriv mekanismerna för att förhindra ”man-in-the-middle”.

4.4.4 Osäkra protokoll

Tillämpning av osäkra protokoll

Listan nedan bör anpassas till respektive upphandling. Vid upphandling av system som integrerar med skrivare bör exempelvis LPD läggas till. Notera att de protokoll som anges i det här dokumentet alltid ska vara med i kravet.

Systemet ska inte använda SMB version 1, autentisering med NTLM-hash, NetBIOS eller andra protokoll med kända sårbarheter eller autentisering i klartext.

4.5 Säkerhet i webbaserade system

4.5.1 Åtkomst med https

Webbtjänsten ska vara åtkomlig med användning av https.

4.5.2 Åtkomst med http

Anrop med http ska inte vara möjlig. Omdirigering till https vid anrop med http är tillåtet och bör ske.

4.5.3 Tillåtna protokoll

Vid användning av https ska TLS 1.2 eller senare användas då aktuella versioner av Internet Explorer, Edge, Chrome, Safari eller Firefox används.

4.5.4 Förbjudna protokoll

Det ska inte vara möjligt att anropa tjänsten med nedanstående protokoll:

- SSL (version 1–3)
- TLS version 1.0–1.1

TLS 1.0–1.1 måste förbjudas endast om **särskild skyddsvärd** information förekommer.

4.5.5 Tillåtna kryptografiska metoder

Webbtjänst åtkomlig genom användning av https ska ges lägst rating B enligt Qualys SSL Labs ”SSL Server Test” under hela avtalsperioden.

Kommentar till kravet tillåtna kryptografiska metoder

Webbtjänst som är åtkomlig med https måste konfigureras så att en väl avvägd kombination av kryptografiska metoder tillåts. Denna avvägning är under ständig utveckling i takt med att sårbarheter upptäcks och nya versioner av webbläsare släpps. IT-säkerhetsgruppens definition av en väl avvägd kombination är metoder som resulterar i lägst betyg B i testet som nämns i kravet. Testet finns för närvarande åtkomligt på https://www.ssllabs.com/ssltest/analyze.html

4.5.6 Härdning av webbtjänster

Om en tjänst ska integreras i LiU:s egen infrastruktur behöver tjänsten klara av att fungera på system som härdats, genom bland annat owasp top 10.

Tjänsten ska vara skyddad mot sårbarheterna i owasp top 10[1]. Denna lista av de tio vanligaste hoten mot webbtjänster uppdateras i takt med att nya sårbarheter blir vanligare. Tjänsten ska under avtalsperioden löpande underhållas så att den uppfyller kraven i takt med att owasp top 10 uppdateras och när förändringar görs i tjänsten. Dessa åtgärder berör inte enbart den utvecklade tjänsten utan även omkringliggande system som driver tjänsten, exempelvis webbservrar och databaser.

Bifoga en rapport om tester gjorts mot owasp top 10 eller motsvarande.

4.5.7 Domänadress för webbaserade system

Undantag kan godkännas av universitetets informationssäkerhetssamordnare.

Webbaserade system ska vara åtkomliga på domänadress som slutar på .liu.se. Omdirigering från liu.se-adress till externt domännamn anses inte uppfylla detta krav.

4.6 Certifikathantering

4.6.1 Giltighet av certifikat (TLS)

Certifikat för TLS ska i förekommande fall hållas uppdaterade under hela avtalstiden. Certifikat ska förnyas innan de förfaller.

[1] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

4.6.2 Utfärdande av certifikat under domänen liu.se

Certifikat för tjänster med domänadress som ägs av LiU (bl.a. alla domänadresser som slutar på .liu.se) ska utfärdas av LiU CA (genom Sunet TCS). Eventuell kostnad för dessa certifikat betalas av LiU.

4.6.3 Utfärdande av övriga certifikat

TLS-certifikat för webbtjänster ska i förekommande fall vara utfärdade av betrodd utgivare. Det ska inte krävas installation av särskilt rotcertifikat i webbläsare eller operativsystem.

4.7 Skydd mot intrång och skadlig kod

Systemet ska vara skyddat mot intrång och skadlig kod (exempel: regelbunden patchning, brandvägg, IPS, förvaltningsrutiner m.m.).

Beskriv skydd samt rutiner för patchning.

4.8 Hantering av IT- och informationssäkerhetsincidenter

Leverantören ska ha rutiner för hantering av informationssäkerhetsincidenter. Vid leverans ska leverantören uppge kontaktuppgifter för incidenthantering (minst e-post och telefonnummer).

4.8.1 Svarstider

När LiU kontaktar leverantören i frågor rörande IT- och informationssäkerhet ska ett första svar vara LiU tillhanda inom en arbetsdag från det att en fråga initieras.

4.9 Rapportering av IT- och informationssäkerhetsincidenter

Informationssäkerhetsincidenter som berör eller involverar LiU ska rapporteras till av LiU utsedd kontaktperson.

Kommentar till kravet

Normalt ska universitetets IT-säkerhetsgrupp ingå bland dessa kontaktpersoner. Då används funktionsadressen: abuse@liu.se

4.10 Åtgärdande av sårbarheter

Leverantören ska skyndsamt åtgärda sårbarheter avseende IT-säkerhet. Allmänt kända sårbarheter (sårbarheter som exempelvis publicerats på publika Internetforum) ska åtgärdas inom högst en månad. Sårbarheter som påtalats för leverantören men som inte är allmänt kända ska åtgärdas inom högst 3 månader.

4.11 Formella säkerhetskrav

Tillämpning av formella säkerhetskrav

Dessa krav tillämpas baserat på skyddsbehov för det aktuella systemet. Notera att dessa krav särskilt riskerar att vara konkurrenshämmande om de inte tydligt kan motiveras.

Kraven 4.11.1 och 4.11.2 kan tillämpas var för sig eller utelämnas helt beroende på behov.

Krav 4.11.3 tillämpas endast om behovet går att motivera (till exempel om det finns avtal med forskningsfinansiär som kräver certifiering).

Ej obligatoriskt.

4.11.1 Löpande säkerhetsrevisioner

Leverantören ska genomföra regelbundna säkerhetsrevisioner med hjälp av extern, oberoende, part. LiU ska få ta del av rapporter från dessa revisioner.

4.11.2 Säkerhetsrevision på LiU:s begäran

LiU ska kunna begära att leverantören genomför säkerhetsrevision av en från leverantören extern och oberoende part. Kostnader för den externa partens arbetsinsatser bekostas av LiU.

Ej obligatoriskt, ska motiveras för att användas.

4.11.3 Certifiering enligt ISO 27001

Leverantören ska vara ISO 27001-certifierad.

Endast obligatoriskt om systemet inte är placerat vid LiU och hanterar **särskilt skyddsvärd** information.

4.11.4 Driftsmiljö

Leverantören ska ha en driftsmiljö som lever upp till de krav på sekretess, tillgänglighet och riktighet som LiU ställer. Inbrottsskydd ska vara minst motsvarande SSF 200, skyddsklass 2 med inbrottslarm motsvarande SSF 130 larmklass 2.

Redogör för hur driftsmiljön är utformad.

5 Loggning och behandlingshistorik

5.1 Format på loggfiler

Förekommande loggfiler ska föras i textformat som är lämpligt för maskinell bearbetning. Som sådant format räknas exempelvis JSON, XML, syslog, CSV. Binära eller proprietära format är godtagbara endast om leverantören löpande kan tillhandahålla en fullständig specifikation av loggformatet.

Beskriv format för loggdata.

5.2 Tidsangivelse i loggdata

Förekommande logghändelser ska loggas med datum (år, månad, dag) och tid (timme, minut, sekund och tidzon). Logghändelser får även loggas med högre tidsprecision. Tidsangivelser ska vara korrekta och synkroniserade mellan alla komponenter som genererar händelser.

5.3 LiU:s möjlighet att ta del av loggar

Möjlighet ska ges för LiU att maskinellt och med automatik ta del av loggdata. Nedanstående metoder är exempel på godtagbara metoder:

- Kontinuerlig överföring med syslog eller annan icke proprietär metod
- Dumpar av loggfiler partitionerade med i intervall om 5–30 minuter. Varje fil ska vara tillgänglig i minst 24 timmar och hämtas med exempelvis SFTP eller liknande teknik.

Nedanstående metod att ta del av loggdata uppfyller inte kravet:

- Webgränssnitt där loggar kan sökas ut.

Beskriv hur kravet uppfylls.

5.4 Redovisning av förväntad mängd loggdata

Leverantören ska redovisa förväntad mängd genererade loggdata (mätt i byte).

Ange ungefär hur mycket loggdata förväntas per dygn.

5.5 Händelser som ska loggas

Tillämning av händelser som ska loggas

Punkterna ”skapande”, ”visning”, ”förändring”, och ”borttagning” av uppgifter är obligatoriska endast för **särskilt skyddsvärd information**. Om man på förhand känner till vilken information som berörs kan kravet preciseras genom att ange detta. Övriga punkter bör alltid tillämpas. Det kan även vara relevant att logga ytterligare händelser, beroende på vad som upphandlas.

Följande händelser ska loggas:

- Inloggningar och inloggningsförsök
- Utloggningar
- Tillägg av användare
- Borttagning av användare
- Förändringar av behörigheter
- Skapande av uppgifter
- Visning av uppgifter
- Förändring av uppgifter
- Borttagning av uppgifter

Loggning krävs endast för händelser i det upphandlade systemet. Loggning krävs inte för händelser i LiU:s system, såsom förändringar av medlemskap i grupper som ligger till grund för behörigheter.

5.6 Information som ska loggas

Följande uppgifter ska loggas:

- Typ av händelse
- Tidpunkt för händelsen
- Subjekt (användare eller system) som initierade händelsen
- Uppgift som påverkades av händelsen

För autentisering till servertjänst ska anslutande IP-adress loggas. Om det är möjligt att korrelera loggposter med tillhörande autentisering är det inte nödvändigt att logga subjekt i varje post.

5.7 Skydd av loggar

Loggar ska skyddas mot obehörig åtkomst. Om loggar inte överförs kontinuerligt (enligt krav 5.3) så ska skyddet också avse obehörig förändring,

Beskriv hur loggdata skyddas.

5.8 Gallring av loggdata

Loggar ska sparas minst 6 månader och högst 18 månader. Loggar som är äldre än 6 månader kan gallras vid godtycklig tidpunkt, dock senast efter 18 månader.

Kravet på att spara loggar kan uppfyllas genom att överföra loggdata till Linköpings universitet. Rensning kan då ske omgående eller vid annan tidpunkt, dock senast inom föreskriven tid.

Kommentar till kravet gallring av loggdata

Krav ska ställas på den minsta respektive längsta tid loggdata ska sparas. Exakta tidsgränser bör bedömas utifrån en avvägning av skyddsbehov kontra integritetsaspekter. Det kan för vissa system finnas särskilda lagkrav som måste beaktas.

Enligt LiU:s dokumenthanteringsplan dnr LiU-2018-01356 ska loggar sparas i minst 6 och högst 18 månader med gallring någon gång däremellan.

6 Särskilda krav avseende tillgänglighet

Tillämpning av särskilda krav avseende tillgänglighet

Krav för tillgänglighet är obligatoriska endast för system som behandlar informationstillgångar klassificerade med **höjd** riktighet eller **höjd** tillgänglighet.

Tidsgränserna i kraven i detta avsnitt är endast att betrakta som rekommendationer. Gränserna kan justeras både uppåt och nedåt baserat på de behov som föreligger.

Notera att det är **nödvändigt** att definiera vad tillgänglighet innebär för att dessa krav ska vara meningsfulla. Definitionen av tillgänglighet måste utgå från verksamhetens behov; det är i grunden inte en IT-fråga. Exempelvis är det knappast tillräckligt att det går att ansluta till en tjänst om man inte även kan använda den till något. Definitionen måste vara mätbar, så att man kan följa upp systemets eller tjänstens tillgänglighet.

6.1 Tillgänglighet

Systemet ska vara tillgängligt minst 99,7% av tiden, mätt över perioden 07:00-18:00 under årets samtliga vardagar. Servicefönster ska normalt läggas 17:00-07:00 vardagar, eller på helger. På förhand avtalade servicefönster ingår inte i beräkningen av tillgänglighet.

Beskriv rutiner och servicefönster.

6.2 Övervakning

Leverantören ska ha aktiv driftövervakning av ingående systemdelar. Vid driftsstörningar längre än 10 minuter, oavsett tidpunkt, ska ett meddelande skickas till av beställaren utsedda kontaktpersoner.

Beskriv hur meddelanden skickas.

7 Rättsliga krav

7.1 Gällande lagstiftning

Leverantören ska följa all gällande lagstiftning och andra tillämpliga regleringar, inklusive EU:s dataskyddsförordning, med avseende på den information de behandlar och de tjänster de erbjuder.

7.2 Incidentrapportering

Ej obligatoriskt för system som drivs av LiU.

Linköpings universitet omfattas av obligatorisk IT-incidentrapportering enligt MSBFS 2016:2. Leverantören ska antingen rapportera allvarliga IT-incidenter till LiU samt bistå vid upprättande av incidentrapport till MSB, alternativt själv rapportera IT-incidenter till MSB i enlighet med MSBFS 2006:2 9 §. I det senare fallet ska incidentrapporten även skickas till LiU.

8 Användbarhet

Tillämpning av användbarhet

Användbarhet är en viktig aspekt i många system, men också en som kan vara svår att kravställa. I system där användbarhet är en viktig aspekt, kan en utvärdering av användbarheten ingå i utvärderingen av anbuden, men då behöver man på förhand ta fram en utvärderingsmetod.

För webbaserade system kan man hämta krav från webbriktlinjer.se.

8.1 Språk

Tillämpning av språk

Dessa krav är tillämpbara på system eller delar av system som har en bred användarbas. System eller delar av system som används av en mindre grupp användare kan ha andra krav (exempelvis kan man ställa krav på att den användartillriktade delen av ett system ska ha både svenskt och engelskt utförande, men acceptera att till exempel administratörsgränssnitt bara finns på engelska).

8.1.1 Översättningar

Ej obligatoriskt.

Systemet ska finnas i svenskt och engelskt utförande.

8.1.2 Språkinställningar (klientbaserade komponenter)

Klientbaserade komponenter med stöd för fler än ett språk ska välja det språk klientsystemet (till exempel Windows) är inställt på. I det fall klienten inte har en språkinställning, eller är inställd på ett språk systemet inte klarar, ska i första hand engelska och i andra hand svenska användas.

8.1.3 Språkinställningar (webbaserade system)

Webbaserade system med stöd för mer än ett språk ska välja språk efter:

- I första hand användarens inställning i webbtillämpningen. Sådan inställningsmöjlighet ska finnas.
- I andra hand webbläsarens språkinställning (accept-language).
- I sista hand standardinställning i systemet.

Det ska vara möjligt för användare att välja språk i systemet. Det ska vara möjligt för systemadministratör eller systemförvaltare att ange standardinställning.

8.2 Tillgänglighet

Tillämpning av tillgänglighet

Krav på tillgänglighet styrs av bland annat lagen om offentlig upphandling (6 kap 1 §), arbetsmiljölagen (2 kap 1 §), diskrimineringslagen (1 kap 1 §, m.fl.), och förordning om de statliga myndigheternas ansvar för genomförandet av handikappolitiken.

Dessa krav bör anpassas till varje enskilt system eftersom IT-branschen har stor utvecklingspotential när det gäller tillgänglighetsfrågor. Exempelvis kan det i vissa fall vara bättre att sänka kraven och istället kräva alternativa lösningar för funktionshindrade. Samtidigt är kraven inte på något sätt orimliga (WCAG 2.0 har till exempel varit en standard sedan 2008).

8.2.1 Allmänna krav på tillgänglighet

Tillämpning av allmänna krav på tillgänglighet

EU-riktlinjen som refereras till förväntas införlivas i svensk lagstiftning. Kraven är mycket omfattande, och kan vara svåra för en leverantör att sätta sig in i, så det är lämpligt att gå igenom kraven och reproducera de som är tillämpbara på systemet som upphandlas.

Systemet ska uppfylla samtliga krav i europeisk standard för krav på tillgänglighet i offentlig upphandling av IT (EN 301549).

8.2.2 Tillgänglighet i webbaserade system

Webbaserade system ska uppfylla kraven i WCAG 2.0 (ISO/IEC 40500:2012), nivå AA eller bättre. Vid automatisk validering får fel förekomma endast om de inte inverkar på systemets tillgänglighet.

Bifoga en valideringsrapport som visar att kravet uppfylls. Vid avvikelser ska **leverantören motivera varför dessa inte inverkar på systemets tillgänglighet.**

8.2.3 Tillgänglighet i mobila gränssnitt

Tillämpning av tillgänglighet i mobila gränssnitt

Riktlinjen som refereras till är relativt omfattande och kan innehålla punkter som inte är relevanta i vissa system, till exempel om systemet ska användas av en begränsad expertgrupp. Det är lämpligt att ta ut de specifika krav som är relevanta i respektive upphandling.

Systemet ska följa samtliga riktlinjer i ”riktlinjer för tillgänglighet i mobilgränssnitt” och ”riktlinjer för mobilnavigering” från funka.nu.

8.3 Prestanda

Tillämpning av prestanda

Det är viktigt att kravställa prestanda på systemet. Det går inte att ange några generella krav, utan dessa måste anpassas till respektive system och dess funktioner. De krav som följer är exempel.

8.3.1 Övergripande prestanda

Den tekniska lösningen ska utformas och dimensioneras av leverantören för att klara den totala volymen användare och data utan att belastningen i ingående system påverkar användarna negativt. Tid för uppkoppling, sökning, bildväxling etc. får inte upplevas som orimlig, maximalt 2 sekunder från sökning till svar.
I de fall hela eller delar av lösningen ska integreras i LiU:s IT-miljö ska leverantören ta hänsyn till eventuella begränsningar som finns i denna.

8.3.2 Prestanda på webbsidor

Samtliga webbsidor ska ritas upp på under en sekund på en typisk arbetsdator. Det innefattar tillräckligt mycket innehåll att användaren upplever att webbsidan är användbar, det vill säga även laddning av till exempel data i urvalslistor som krävs för att använda sidan.

8.3.3 Prestanda på sökningar

Sökningar efter enkla begrepp ska slutföras på under två sekunder.

9 E-post

9.1 Avsändaradresser

Vid upphandling av system som förväntas skicka e-post med avsändaradress under liu.se ska normalt en utpekad domän, för närvarande partner.liu.se, användas. Önskas adresser direkt under liu.se måste IT-avdelningen måste detta godkännas av IT-direktören innan förfrågningsunderlaget färdigställs.

9.1.1 Avsändare under liu.se

System eller tjänster som skickar e-post med adresser som slutar på .liu.se ska använda en av IT-avdelningen utpekad underdomän och adress.

9.1.2 Servrar för e-post

Detta krav **måste** vara med om man förväntar sig att e-post ska skickas med avsändare på formen *avsändare*@liu.se. Uppfylls detta krav inte kan det vara tekniskt omöjligt att säkerställa tillförlitlig leverans av e-post. Notera att användning av sådan adress ska godkännas av IT-direktören innan förfrågningsunderlaget färdigställs.

Om avsändaradress på formen *avsändare*@liu.se används ska e-post skickas genom av LiU utpekade e-postservrar med av LiU utpekade protokoll och mekanismer för autentisering.

9.2 Tillförlitlig leverans

E-post som är nödvändig för tjänsten ska skickas på ett sådant sätt att de går att särskilja från all annan e-post, i syfte att säkerställa att de passerar LiU:s e-postfilter. Särskiljning kan till exempel göras på avsändande server, avsändaradress, eller fast innehåll i meddelandet. Leverantören ska inför driftsättning kunna redogöra för hur denna e-post kan särskiljas.

9.3 Massutskick

Många tjänsteleverantörer vill göra massutskick i samband med lanseringen av tjänsten, och ibland under tjänstens leverans. Dessa utskick ska följa LiU:s regelverk och principer.

9.3.1 Genomförande av massutskick

Detta krav är endast tillämpligt om leverantören gör massutskick (utskick till ett stort antal användare vid LiU). Massutskick ska planeras och genomföras i samråd med LiU. Inga utskick ska göras utan att tidpunkt, innehåll, och utformning har godkänts av IT-direktören.

9.3.2 Prenumerationer på massutskick

Detta krav är endast tillämpligt om leverantören gör massutskick (utskick till ett stort antal användare vid LiU) som inte är nödvändiga för tjänstens funktion, till exempel nyhetsbrev. Massutskick som inte är nödvändiga för tjänstens funktion ska endast skickas till de mottagare som prenumererar på dem.

9.3.3 Initiala prenumerationer

Detta krav är endast tillämpligt om leverantören gör utskick som går att prenumerera på, exempelvis massutskick som inte är nödvändiga för tjänstens funktion. LiU ska kunna anvisa vilka användare som ska vara prenumeranter på utskick innan det första utskicket genomförs.

9.3.4 Möjlighet att stoppa utskick

Leverantören ska ha möjlighet att på LiU:s begäran stoppa planerade utskick.

9.4 Skyddsvärd information

Om man på förhand vet att systemet behandlar **särskilt skyddsvärd** information bör detta krav preciseras genom att ange vilken information det gäller.

Information som LiU bedömer är av konfidentiell art, känsliga personuppgifter, eller uppgifter med särskilda integritetskrav bör inte skickas via e-post. Om sådan information ändå skickas via e-post ska den krypteras med mottagarens nyckel (som för användare vid LiU utfärdas av LiU) i formatet S/MIME.

10 Integrationer

Tillämpning av integrationer

System som ska hämta data från, skicka data till, eller på annat sätt integreras med LiU:s andra system, till exempel HR, ekonomisystem, kontohantering, eller liknande, måste kravställas utifrån ett integrationsperspektiv.

Denna kravställning kan vara komplex och ska därför göras i samråd med IT-avdelningen.

Nedan följer ett exempel på hur sådana krav kan vara formulerade.

10.1 Integration med annan programvara

Tillämpning av integration med annan programvara

Listan över specifika program kan anpassas om integrationen endast används av en homogen grupp. Kraven kan vidare vara olika för läsning och generering av filer.

10.1.1 Hantering av Office-filer

Om lösningen hanterar Office-filer (Word, Excel) ska dessa kunna genereras och/eller läsas med följande programvara:

- Microsoft Office 2010 till 2016
- Office 365
- LibreOffice 5.x

Lösningen ska under avtalsperioden löpande underhållas så att den fungerar med versioner de av Microsoft Office som har mainstream eller extended support, samt senaste versionen av LibreOffice.

10.1.2 Hantering av PDF-filer

Om lösningen hanterar PDF-filer ska dessa kunna genereras och/eller läsas med följande programvara:

- Adobe Acrobat Reader DC på Windows och OS X
- Foxit Reader (enbart Windows)
- Evince (enbart Linux)

Lösningen ska under avtalsperioden löpande underhållas så att den fungerar med den senaste versionen av ovanstående program.

10.1.3 Integration med Office-program

Om lösningen integrerar med Office-program, ska den kunna integreras med de av följande program som är tillämpliga:

- Microsoft Exchange 2016 (e-post, kalender, tasks, mm).
- Microsoft Exchange Online (e-post, kalender, tasks, mm).
- Microsoft Office 2013 och 2016 (makron, plugins, e-post, kalender, tasks, mm).
- Skype for business (chat, röstsamtal, videosamtal mm) eller dess efterföljare.
- Office 365

Lösningen ska under avtalsperioden löpande underhållas så att den fungerar med den senaste versionen av ovanstående program eller dess efterföljare.

10.1.4 Integration med skrivarsystemet

Anpassa detta krav till aktuellt utskriftssystem.

Systemet ska stödja befintlig utskriftslöning på LiU. För närvarande använder LiU Papercut.

10.2 Integration med andra system

Tillämpning av integration med andra system

Dessa krav är endast tillämpbara om det är avsett att systemet ska inhämta information från LiU:s andra system (HR, ekonomi, mm) eller lämna information till dessa. Kontakta IT-avdelningen för stöd med formulering av krav för just detta system.

Utveckling av integrationer kan innebära en merkostnad. Om dessa är en option, begär att utvecklingen prissätts separat.

10.2.1 Allmänna krav

Leverantören ska kunna tillhandahålla ett tekniskt gränssnitt för integtaion. Gränssnittet ska kunna hantera ett eller flera av följande protokoll och tekniker: REST, WCF, SOAP, SFTP, SMB3, Microsoft SQL, Microsoft Azure SQL, CosmosDB, Blob Storage, Microsoft Azure ServiceBus (Queue och/eller Topic). Gränssnittet skall vara fullständigt dokumenterat, och dokumentationen göras tillgänglig för LiU.

Data- och överföringsformat ska vara fullt dokumenterade och använda öppen standard. All överföring av data och filer till andra system ska kunna ske med en säker krypterad överföring, till exempel genom https, sftp eller krypterad smb3.

10.2.2 Händelsestyrda integrationer

Ej obligatoriskt, men avsteg ska godkännas av IT-avdelningen.

Integrationerna ska vara händelsestyrda både in (de processas direkt vid anrop/överföring) och ut (anrop/överföring påbörjas direkt vid en händelse i systemet).

10.2.3 Batchintegration

Alla förändringar (nya, ändrade, raderade data) under ett av LiU angivet tidsintervall (inom överenskomna gränser) ska antingen kunna skickas till, eller vara möjliga att hämtas av, LiU:s integrationsplattform, på ett format som är anpassat för maskinell behandling. Formatet ska vara fullt dokumenterat.

10.2.4 Utläsning av data

LiU ska ha möjlighet att få en utläsning av all LiU-ägd data samt eventuell annan tillhörande data som behövs för att tolkning (t.ex. centrala/gemensamma listor) ur systemet. Eventuell historik ska inkluderas. Datat ska vara på ett format som är anpassat för maskinell bearbetning och är fullständigt dokumenterat. Systemleverantören kan antingen tillhandhålla detta på LiU:s begäran eller tillgängliggöra det via ett tekniskt gränssnitt.

11 Systemlivscykel

Krav på systemlivscykeln beror i stor utsträckning på vilken typ av system som upphandlas. Kraven är olika på system som drivs av LiU och system som drivs av en extern part.

Dessa krav ska utformas i samråd med IT-avdelningen.

11.1 Införande

11.1.1 Migrering från befintliga system

Tillämpning av migrering från befintliga system

Kravet på migrering från tidigare system är obligatoriskt endast om det finns information i ett tidigare system som ska behållas. Som alternativ till kravet kan man även komma överens med IT-avdelningen om andra lösningar, till exempel arkivering av data. Hanteringen av befintlig information ska dock på något sätt adresseras i upphandlingen.

I utvärderingen bör man be leverantören prissätta införandeprojektet så att minst 10 testmigreringar ingår. De ska även prissätta ytterligare testmigreringar utöver de första 10.

Leverantören ska ombesörja migrering av data från befintliga system till den nya lösningen. Antalet migreringar/testmigreringar ska inte vara begränsat.

11.1.2 Övriga krav

Kraven vid införande av systemet varierar från system till system. För system som ska drivas vid LiU kan man behöva ställa krav på utbildning av teknisk personal (leverantören ska tillhandahålla utbildning på plats), konsultstöd på expertnivå, rådgivning vid införande kring såväl enkla aspekter som ”best practice”, samt hjälp med anpassningar av produkten och/eller LiU:s miljö.

Om LiU ska ansvara för support till slutanvändare krävs utbildning av LiU:s tekniker samt erforderliga behörigheter och verktyg för uppgiften. I korthet behövs ett helt batteri produktnära tjänster.

Notera även att om systemet använder LiU:s infrastruktur (till exempel nätverk eller datorhallar) kan det finnas tekniska begränsningar som måste kravställas. Detta ska göras i samråd med IT-avdelningen.

För system som ska användas av många personer på LiU kan informations- eller utbildningsmaterial krävas.

11.2 Förvaltning

För många system är det viktigt att ha en leverantör som tar ett löpande ansvar för leveransen. Därför bör man överväga att kravställa till exempel regelbundna möten, möjligheter till vidareutveckling, kontinuerlig dialog eller liknande. Man kan också tänka sig att be leverantören beskriva sitt långsiktiga åtagande, och poängsätta leverantörernas olika beskrivningar.

11.2.1 Assuranskrav

För LiU-övergripande verksamhetskritiska system, till exempel ekonomisystem, HR-system, studiedokumentation, bör assuranskrav ställas, till exempel kring systemutvecklingens livscykel, arkitektur och design, installation och drift, administrativa rutiner, systemintegrationstest, riskanalys och sårbarhetsanalys. Ta kontakt med IT-säkerhetsgruppen för utformning av dessa krav.

11.2.2 Övriga krav

Kraven på förvaltning av systemet varierar från system till system. För system som inte drivs av LiU ska krav ställas på leverantörens svarstid och på spårbarhet av ärenden. För stora system, som används av många personer, bör man kräva att leverantören regelbundet rapporterar kring användning, problem, ärenden och liknande.

Normalt krävs en svarstid kortare än vad som anges i SLA för svar till användarna, eftersom denna innefattar både leverantörens och LiU:s egen hantering. Det krävs även att ärenden ska vara spårbara genom till exempel ett ärendenummer.

Om LiU ska ansvara för support till slutanvändare krävs utbildning av LiU:s tekniker.

11.3 Avveckling

Se även krav 4.3.2 Destruktion av lagringsmedia.

11.3.1 Export till framtida system

Leverantören ska tillhandahålla information och stöd som krävs för export av data till framtida system. Sådant stöd ska omfatta minst export till datafil/databas samt detaljerad teknisk beskrivning av dataformatet/datamodellen eller liknande.

11.3.2 Övriga krav

Kraven på avveckling av systemet varierar från system till system. För system som innehåller hårdvara (till exempel batterier, elektronik eller liknande) kan krav på skrotning vara aktuella.

12 Övriga krav

12.1 Anpassning till LiU:s grafiska profil

Undantag kan godkännas av universitetets informationssäkerhetssamordnare.

Systemet ska kunna anpassas till LiU:s grafiska profil.

12.2 Tekniska begränsningar

Tillämpning av tekniska begränsningar

LiU har inte vilka möjligheter som helst att göra tekniska anpassningar av sin infrastruktur, så vissa tekniska begränsningar måste ingå i kraven.

Redogör alltid med IT-avdelningen kring tekniska begränsningar. Kraven nedan är inte uttömmande.

12.2.1 Inget stöd för QoS

Stöd för QoS ska inte krävas i LiU:s nätverk, alternativt ska kostnad för implementation av QoS i LiU:s nätverk ingå i anbudet.

12.2.2 Ingen fast telefoni

Om fast telefoni (telefoni via kabel; digital eller analog) krävs ska den inte kopplas via LiU:s växel och kostnad för installation av nödvändiga anslutningar ska ingå i anbudet.

12.2.3 Inget tillträde till datorhallar

Ska utrustning placeras i LiU:s datorhallar får leverantören inte kräva eget fysiskt tillträde till dessa utrymmen.

12.2.4 Fysiska servrar

Fysiska servrar som placeras i LiU:s datorhallar ska vara avsedda för rackmontering (inga tower-lådor) och ska levereras med justerbara rackmonteringsskenor som möjliggör service utan att systemet lyfts ut ur stativen.

12.2.5 Placering av teknisk utrustning

Teknisk utrustning som inte hanteras av LiU:s egen personal får inte placeras i samma utrymmen som LiU:s egen utrustning (korskopplingsrum och liknande). Om hyra av lokaler för att placera utrustning krävs, räknar LiU upp kostnaden för anbudet med denna hyra.

12.2.6 Inga brandväggar

LiU driver ett öppet nätverk. Lösningen ska inte kräva brandvägg hos LiU. Om lösningen kräver en brandvägg ska denna ingå i anbudet.

12.2.7 Säkerhetstester

System som är anslutna till LiU:s interna nätverk kan komma att utsättas för automatiska och enklare manuella penetrationstest utan föregående varning. De ska vara robusta nog att hantera detta utan störning i tjänsten som levereras.

12.2.8 Dynamiska adresser

Servertjänster som ingår i anbudet ska inte kräva att anslutningar görs från utpekade IP-adresser eller från nätverk av mindre storlek än de som omfattar hela LiU (främst 130.236.0.0/16, 2001:6b0:17::/48).

12.3 Dokumentation

Dokumentation ska levereras i elektroniskt format som är sökbart och läsbart på Windows, OS X, Linux, Android och iOS, och som kan skrivas ut. Exempel på format som är acceptabla är PDF, Microsoft Word, man-sidor, och webbaserad dokumentation.