Mittuniversitetet
MID SWEDEN UNIVERSITY

Kravkatalog upphandling av IT

Publicerad: 2020-11-13

Beslutsfattare: Helena Wallskog

Handläggare: Eva Rodin Svantesson

Beslutsdatum: 2020-11-13

Giltighetstid: Från beslutsdatum och framåt till dess att dokumentet uppdateras.

Ansvarig för förvaltning: Riktlinjerna förvaltas av infrastrukturavdelningen.

Målgrupp: Upphandlare, Infrastrukturavdelningen och upphandlande verksamheter.

Sammanfattning: Dokumentet är en katalog över IT-relaterade krav som ska användas vid upphandling av system där IT-produkter eller IT-tjänster ingår. Katalogen är inte fullständig när det gäller kravställning kring IT, men katalogen kan användas som en utgångspunkt. Kraven är anpassade till Myndigheten för samhällsskydd och beredskaps föreskrifter 2020:6-8. Mindre justering genomförd 20210203 gällande tillgänglighet.

Innehållsförteckning

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.

Samtliga krav är ställda som **ska** och **bör-krav**. Vilka krav som ska ställas beror på upphandlingen, systemets målgrupp och storlek. Vissa krav styrs dock av informationsklassning på den information systemet ska hanteras, 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 Infrastrukturavdelningen. Notera att dokumentet inte kan användas i sin helhet i en upphandling, aktuella krav hämtas från kravkatalogen till upphandlingsunderlaget.

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

Ytterligare stöd i arbetet är ”Upphandla informationssäkert – en vägledning” från MSB. https://www.msb.se/RibData/Filer/pdf/28742.pdf

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 modell för informationsklassning som ingår i ledningssystemet för informationssäkerhet. Klassningen ligger till grund för att avgöra vilka krav i denna katalog som kan uteslutas. Som bilaga till kravkatalogen finns också kraven på säkerhetsåtgärder som utgår från den genomförda informationsklassningen Det är en kombination av organisatoriska, administrativa, fysiska och tekniska åtgärder som är kopplade till informationsklassningens konsekvensnivåer.

1.2 Särskilda anvisningar avseende molntjänster – utkontraktering

Om upphandlingen innefattar en molntjänst och den kommer att hantera information klassad med **hög konfidentialitet, riktighet och tillgänglighet eller personuppgifter**

så ska avstämning göras med universitetets jurist och dataskyddsombud innan upphandlingen inleds.

Enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:6 ska myndigheten innan den låter en extern aktör behandla information, utifrån informationsklassning och riskbedömning, hantera de risker en sådan behandling innebär. Myndigheten ska i avtal ställa krav på vilka säkerhetsåtgärder den externa aktören ska vidta och hur myndigheten följer upp dessa krav.

Avtalet mellan myndigheten och den externa aktören bör reglera;

1. att den externa aktören ska ha tillräcklig kompetens avseende informationssäkerhet,
2. hur den externa aktören ska överlämna information till myndigheten om misstänkta eller inträffade incidenter, avvikelser och sårbarheter
3. hur den externa aktören ska följa upp sitt egna och eventuella underleverantörers systematiska och riskbaserade informationssäkerhetsarbete, och
4. hur myndighetens information ska återlämnas när avtalet upphör.

1.2.1 Krav enligt vägledningen

Ansvaret för att informationen hanteras säkert av en leverantör kan inte utkontrakteras, det är endast uppdraget som kan utkontrakteras.

Vid utkontraktering av it-tjänster bör det som minimum ställas krav på följande:

- Att leverantören har ett etablerat systematiskt och riskbaserat informationssäkerhetsarbete.
- Att organisationen får insyn i säkerhetsarkitekturen som används för att leverera tjänsten.
- Att organisationen, eller tredje part, får möjlighet att granska den del av it-miljön som utkontrakteringen omfattar och att it-säkerhetstester får genomföras mot den miljön.
- Att säkerheten hos leverantören utvecklas i linje med utvecklingen inom teknologi och hotbilden över tid.
- Att organisationen får en översikt över vem hos leverantören som får insyn i och tillgång till organisationens information, var och hur denna ska behandlas och lagras samt beskrivning av mekanismer för åtskillnad från andra kunder.
- Att leverantören har åtkomst- och behörighetsstyrning (även för sina egna medarbetare), liksom andra säkerhetsåtgärder såsom kryptering, loggning och fysisk och logisk säkerhet.
- Att leverantören har övervakning som syftar till att upptäcka incidenter samt hur leverantören hanterar sina egna och kundernas hotbilder och relevanta hotaktörer.

- Att leverantören har rutiner för avvikelse- och incidenthantering samt hur rapportering sker mellan leverantören och organisationen.
- Att leverantören har kris- och beredskapsplaner (kontinuitetshantering) som är tillräckliga utifrån organisationens behov.
- Att användande av underleverantörer och deras användande av underleverantörer ska godkännas av organisationen innan de får åtkomst till information eller annan kännedom om informationshanteringen.
- Att det är klarlagt och finns avtal om vilka aktiviteter som ska utföras vid avslutande av kontrakten, bland annat återföra/flytta/radera organisationens information.

1.3 Typografiska konventioner

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

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 upphandlingsdokumentet

1.4 Giltighetstid

Kravkatalogen ses över löpande (minst en gång per år). Ansvarig för uppdatering är Infrastrukturavdelningen. Den senaste versionen av katalogen finns tillgänglig på informationssäkerhetssidan på webben.

2. Klienters IT-miljö

2.1 Krav avseende webbaserade system

Systemet ska stödja klientdatorer och mobila enheter.

2.1.1 Stöd av webbläsare

Webbaserade system ska under hela avtalsperioden fungera med samtliga på marknaden kända webbläsare och plattformar.

Beskriv vilka plattformar som stöds och vad som rekommenderas.

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.

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.

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

2.2.1 Säker leverans av klient

Om en så kallad klient används inom lösningen, ska leverantören tillhandahålla en säker och tillförlitlig leverans av denna klient.

2.2.2 Plattformar som ska stödjas

Eventuell klientprogramvara ska fungera med samtliga på marknaden kända operativsystem.

Beskriv vilka operativsystem som stöds och vad som rekommenderas.

2.2.3 Mobila plattformar som ska stödjas

Eventuell programvara för mobila plattformar (appar) ska fungera med samtliga på marknaden kända system.

Beskriv vilka system som stöds och vad som rekommenderas.

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.

Beskriv vilka system som används för paketering av programvara.

2.2.5 Krav på underliggande operativsystem

Löpande patchning av operativsystem och andra programvaror 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 Administratörsbehörigheter

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

2.2.8 Installationsplats

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

2.2.9 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.

2.2.10 Distanssupport

Om leverantören erbjuder distanssupport ska supporten ske på ett säkert sätt.

Beskriv hur distanssupport genomförs och med vilket/vilka programvaror.

3. Användarhantering och inloggning

3.1 Personliga användarkonton

Användarkonton ska vara personliga.

3.2 Federerad inloggning (SSO)

Användare bör logga in i systemet genom multifaktorautentisering (MFA). Autentisering ska kunna ske med AD vid Miun.

3.3 Tillämpningsspecifika lösenord

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

3.3.1 Lösenordslängd

Systemet ska inte tillåta lösenord kortare än 8 tecken.

3.3.2 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.

3.3.3 Lagring av lösenord

Lösenord för lokal användardatabas ska inte lagras i klartext

Beskriv hur lösenord lagras.

3.3.4 Lösenordsåterställning

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

Beskriv hur lösenordsåterställning sker.

3.3.5 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.

3.3.6 Periodiska lösenordsbyten

Periodiska lösenordsbyten ska inte krävas.

3.3.7 Lösenordskomplexitet

Miun bör 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).

Beskriv vilka möjligheter som finns.

3.4 Begränsning av åtkomst till valda IP-adresser

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

4. Allmänna säkerhetskrav

4.1 Backuper

4.1.1 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.

Att beakta: Om det avser ett enkelt system som inte hanterar data där kravet på tillgänglighet är högt, kan lägre krav ställas. Kravet är kostnadsdrivande.

Beskriv rutiner.

4.1.2 Tid för återläsning

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

Tillämpning tid för återläsning
Anpassa tidsgränserna till behoven för det aktuella systemet.

4.1.3 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 Lagring av data

4.2.1 Krypterad lagring

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

4.2.2 Destruktion av lagringsmedia

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

Beskriv rutiner.

4.3 Kommunikationssäkerhet

Information (som är särskilt skyddsvärd) som sänds över nätverk ska vara krypterad med vedertagen säker metod.

Beskriv metod och rutiner.

4.4 Säkerhet i webbaserade system

4.4.1 Åtkomst med https

Webbtjänsten ska vara åtkomlig endast vid krypterad användning av https.

4.4.2 Domänadress för webbaserade system

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

4.5 Certifikathantering

4.5.1 Giltighet av certifikat (TLS)

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

4.5.2 Utfärdande av certifikat under domänen miun.se

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

4.5.3 Utfärdande av övriga certifikat

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

4.5.4 TLS Version

Lägsta godkända version för TLS är 1.2. TLS 1.3 ska stödjas och är att föredra.

4.5.5 Kryptering

För kryptering ska AES stödjas.

4.5.6 RSA

Vid användning av RSA ska den privata nyckeln vara minst 2048 bitar lång.

4.5.7 Hashning

För hashning ska SHA256 stödjas. SHA384 bör stödjas.

4.6 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.

4.7 Hantering av IT- och informationssäkerhetsincidenter

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

4.8 Rapportering av IT- och informationssäkerhetsincidenter

Informationssäkerhetsincidenter som berör eller involverar Miun ska rapporteras till e-postadress - helpdesk@miun.se eller till kontakt@miun.se

4.9 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.

Sårbarheter som ligger på en säkerhetsnivå motsvarande critical, ex. 0-day eller att en leverantör av operativsystem eller programvara uppmanar till skyndsam uppdatering ska det göras senast inom en arbetsvecka.

4.10 Formella säkerhetskrav

4.10.1 Säkerhetsrevision på Miun:s begäran

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

4.10.2 Certifiering enligt ISO 27001

Leverantören ska vara ISO 27001-certifierad.

5. Loggning och behandlingshistorik

5.1 Händelser och information som kan loggas

Utifrån nedanstående lista väljs händelser och information som ni i upphandlingen vill kravställa på;

- inloggningar och inloggningsförsök
- utloggningar
- tillägg av användare
- borttag av användare
- förändringar av behörigheter
- skapande av uppgifter
- visning av uppgifter
- förändring av uppgifter
- borttag av uppgifter
- typ av händelse
- tidpunkt för händelsen
- subjekt (användare eller system) som initierade händelsen
- uppgift som påverkades av händelsen

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 Miun:s möjlighet att ta del av loggar

Möjlighet ska ges för Miun att maskinellt och med automatik ta del av loggdata.

Beskriv hur kravet uppfylls.

5.4 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.

5.5 Gallring av loggdata

Loggar ska gallras enligt krav i Miuns dokumenthanteringsplan. Planen finns att hämta på följande sida;

https://www.miun.se/medarbetare/gemensamt/handbok-for-arkiv-och-diarium/

Om det inte är möjligt att automatisera gallringen ska den göras av leverantören kostnadsfritt.

6. E-post

6.1 Avsändaradresser

6.1.1 Avsändare under miun.se

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

6.1.2 Servrar för e-post

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

6.2 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 Miuns e-postfilter. Särskiljning kan till exempel göras på avsändande server, avsändaradress, eller fast innehåll i meddelandet.

Beskriv hur denna e-post kan särskiljas.

6.3 Skyddsvärd information

Information som Miun bedömer är av konfidentiell art, känsliga personuppgifter, eller uppgifter med särskilda integritetskrav ska inte skickas via e-post.

7. Användbarhet och tillgänglighet

7.1 Tillgänglighet (drift)

Systemet ska vara tillgängligt minst 99,7% av tiden, mätt över perioden 07:00-18:00 under årets samtliga vardagar. Servicefönster ska normalt läggas 18:00-07:00 vardagar, eller på helger. På förhand avtalade servicefönster ingår inte i beräkningen av tillgänglighet (om systemet ställer högre krav på tillgänglighet ska kravet justeras utifrån det).

Beskriv rutiner och servicefönster.

7.2 Tillgänglighet (användbarhet)

Krav på tillgänglighet styrs av bland annat lagen om offentlig upphandling (SFS 2016:1145, 9 kap 2 §), arbetsmiljölagen (SFS 1977:1160, 2 kap 1 §), diskrimineringslagen (SFS 2008:567, 1 kap 1§), lag om tillgänglighet till digital offentlig service (SFS 2018:1937), och förordning om de statliga myndigheternas ansvar för genomförande av handikappolitiken (SFS 2001:526)

7.2.1 Allmänna krav på tillgänglighet

Systemet ska tillgodose samtliga behov som beskrivs i EN 301 549, senaste versionen avsnitt 4.2. Som bevis för att kraven är tillgodosedda kan anbudsgivare använda någon av de deklarationer som anges i ETSI TR 101 551 avsnitt 5.2.5. Beträffande innehåll och form för deklarationen, se EN 301 549 bilaga C.

7.2.2 Tillgänglighet i webbaserade system

Webbaserade system ska uppfylla kraven i WCAG 2.1, 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

7.2.3 Tillgänglighet i mobila gränssnitt

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

https://www.funka.com/contentassets/9131835638b640cf96baf2ef62a2fba4/riktlinjer_for_tillgangliga_mobilgranssnitt_2012.pdf

https://www.funka.com/contentassets/d005946001ef460eb4df58a4fc967b83/riktlinjer-for-navigation-i-mobilgranssnitt-svenska-funka.pdf

7.3 Språk

Systemet ska vara på svenska.

7.4 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.

I de fall hela eller delar av lösningen ska integreras i Miun:s IT-miljö ska leverantören ta hänsyn till eventuella begränsningar som finns i denna.

8. Integrationer

Tillämpning av integrationer

System som ska hämta data från, skicka data till, eller på annat sätt integreras med Miun:s andra system, måste kravställas utifrån ett integrationsperspektiv. Denna kravställning kan vara komplex och ska därför göras i samråd med Infrastrukturavdelningen.

Nedan följer några exempel på hur sådana krav kan vara utformade

8.1 Integration med annan programvara

8.1.1 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

Lösningen ska under avtalsperioden löpande underhållas så att den fungerar med ovanstående versioner eller dess efterföljare.

8.1.2 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).
- Office 365

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

8.2 Integration med andra system

8.2.1 Allmänna krav

Leverantören ska kunna tillhandahålla ett tekniskt gränssnitt för integration. 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.

Beskriv tekniken och rutinerna.

8.2.2 Händelsestyrda integrationer

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

8.2.3 Batchintegration

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

8.2.4 Utläsning av data

Miun ska ha möjlighet att få en utläsning av all Miun-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 Miun:s begäran eller tillgängliggöra det via ett tekniskt gränssnitt.

9. Systemets livscykel

9.1 Införande

9.1.1 Migrering från befintliga system

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

Beskriv hur migreringen går till.

9.2 Förvaltning och samverkan

Leverantören ska ansvara för att genomföra kalenderkvartalsvisa samverkansmöten med Miun på operativ- och taktisk nivå samt minst halvårsvis på strategisk nivå. Leverantören ska ansvara för att dokumentera mötena och översända protokoll till deltagarna.

9.2.1 Strategisk nivå

Vid samverkansmöten på strategisk nivå ska affärsrelationen mellan Parterna och de övergripande förutsättningarna för samarbetet behandlas. I strategiskt forum utbyts visioner, strategier och målsättningar i syfte att kontinuerligt se över och anpassa affärsrelationen efter parternas förutsättningar och behov.

9.2.2 Taktisk nivå

Vid samverkansmöten på taktisk nivå ska kommersiella och löpande behov med målet att kontinuerligt utveckla och tillhandahålla ändamålsenliga Tjänster behandlas. I taktiskt forum behandlas målsättning från båda Parter, sammanfattning av Tjänster och eskalerade punkter från operativt forum samt att leverantören informerar om utveckling inom Kontraktet. Leverantören ska vidare avrapportera en allmän bedömning av säkerhetsnivån, eventuella förändringar i hotbilden eller risker som kan ha bäring på Tjänster, samt en sammanställning av under perioden inträffade störningar.

9.2.3 Operativ nivå

Vid Samverkansmöten på operativ nivå ska frågor för att säkerställa kvaliteten och tillgängligheten i Tjänster behandlas. Leverantören ska bland annat redovisa aktuell dokumentation, föregående periods driftstatistik med uppgifter om Åtgärdstid, Avbrottstid samt antal Fel per kategori. Hantering och reglering av viten ska göras i samband med dessa möten och eskaleras vid behov. Även åtgärder som förbättrar och utvecklar samarbetet och Tjänster ska diskuteras.

9.3 Avveckling

Se även krav 4.2.2 Destruktion av lagringsmedia.

9.3.1 Export till framtida system

Leverantören ska kostnadsfritt 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.

10. Rättsliga krav

10.1 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.

10.2 Incidentrapportering

Mittuniversitetet universitet omfattas av obligatorisk IT-incidentrapportering enligt MSBFS 2020:8. Leverantören ska rapportera IT-incidenter till Miun på ett sådant sätt att myndigheten kan uppfylla kraven i MSBFS 2020:8, alternativt själv rapportera IT-incidenter till MSB om aktören omfattas av rapporteringsskyldigheten.

10.3 Dataskydd enligt dataskyddsförordningen

Om systemet upphandlas som en tjänst och innehåller personuppgifter ska ett personuppgiftsbiträdesavtal tecknas. Mall för personuppgiftsbiträdesavtal tillhandahålls av upphandlaren. Avtalet måste granskas och anpassas till den aktuella upphandlingen. Inför upphandlingen bör följande checklista granskas: https://www.miun.se/globalassets/forvaltning/infra/informationssakerhet/checklista---offentlig-upphandling-och-gdpr.pdf

10.3.1 Informationsförvaltning

Om systemet innehåller allmänna handlingar som ska gallras/bevaras ska det ställas krav på den funktionaliteten. Kravställning diskuteras med upphandlare och arkivarie. Se även: Att ställa arkivkrav på IT-system

- vid universitet och högskolor

11. Övriga krav

11.1 Servicenivåer

- Tjänst ska vara i Drift dygnet runt, årets alla dagar.
- Servicetiden ska vara Arbetsdagar mellan 07:00-18:00.
- Åtgärdstid mäts under Servicetid.

- Åtgärdande av Kritiska Fel (kategori 1) som ej avslutats under avtalad Servicetid ska, om Miun begär det, fortsätta till dess att Felet är åtgärdat.
- Åtgärdstid ska maximalt vara fyra timmar per Kritiskt fel (kategori 1) samt 12 timmar per Allvarligt fel (kategori 2). För Ringa fel (kategori 3) ska åtgärdstiden maximalt vara 80 timmar.
- Under Servicetid är maximalt två Kritiska Fel (kategori 1) och åtta Allvarliga fel (kategori 2) tillåtna per kalenderkvartal.

11.1.1 Kritiska fel (kategori 1)

Fel som berör processer som är verksamhetskritiska och/eller som har stor betydelse för Miun. Exempelvis kan detta vara Fel som påverkar en större grupp användare och/eller där Tjänsten inte kan nyttjas alls eller enbart kan nyttjas delvis med stora svårigheter (Avbrottstid).

11.1.2 Allvarliga fel (kategori 2)

Fel som inte bedöms som kritiska men som är allvarliga för Miuns verksamhet. Exempelvis kan detta vara Fel där alternativa användningssätt är möjliga och/eller Fel som enbart berör en mindre grupp användare med lägre verksamhetspåverkan.

11.1.2 Ringa fel (kategori 3)

Fel som är av ringa betydelse för Miuns verksamhet. Exempelvis kan detta vara Fel som påverkar en enskild användare, utan påverkan på Tjänsten som helhet eller rena så kallade skönhetsfel.

Serviceavtal kan tecknas mellan leverantör och Miun

11.2 Anpassning till Miun:s grafiska profil

Systemet ska kunna anpassas till Miun:s grafiska profil.

11.3 Tekniska begränsningar

11.3.1 Inget stöd för QoS

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

11.3.2 Inget tillträde till datorhallar

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

11.3.3 Säkerhetstester

System som är anslutna till Miun: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.

11.4 Dokumentation

Dokumentation (användar- och systemdokumentation) ska levereras i elektroniskt format som är sök- och läsbart.