2019-02-12

Informationssäkerhet vid upphandling och inköp av IT-system och tjänster

Karolinska institutet

Dokumenthantering

Detta dokument är aktuellt vid aktuellt datum då dokumentet producerades eller senast uppdaterades. Dokument med historik finns sparad under informationssäkerhetsfunktionen arbetsmapp i SharePoint: KI Informationssäkerhet → Informationssäkerhet i upphandling

Revisionshistorik

Dokumentet har ändrats enligt följande:

Datum	Version nr	Kommentar	Reviderad av
2018-12-03	0.1	Dokument upprättat	Lukas Grönquist
2018-12-06	0.2	Kompletteringar	Lukas Grönquist
2018-12-20	0.3	Revision efter möte med Lennart Martinsson	Lukas Grönquist
2019-01-07	0.4	Språkliga förändringar	Lukas Grönquist
2019-02-12	0.5	Kompletteringar	Lukas Grönquist
2019-03-07	0.6	Avgränsat vägledningen till IT-system och tjänster efter möte med Nils Emlund	Lukas Grönquist

Godkännande historik

Detta dokument godkänns enligt följande:

Datum	Version nr	Godkänd av	Titel

Innehållsförteckning

Dokumentansvarig Lukas Grönquist		Senast sparat 2019-05-29 13:13
Version 0.6	Senast uppdaterat av Lukas Grönquist	DNR

1 Inledning

En del av KI:s informationssäkerhetsarbete är att säkerställa att de IT-system och IT-tjänster som upphandlas och köps in kravställs med avseende på tjänstens skyddsåtgärder. Denna vägledning har tagits fram för att informationssäkerhetskrav ska vara en del av upphandlings- och inköpsprocessen för IT-system och tjänster vid KI.

Att ta med informationssäkerhetskrav redan innan upphandlingen medför generellt sätt en högre nivå av säkerhet och är ett mer kostnadseffektivt tillvägagångsätt än att lägga på säkerheten efter. Denna vägledning bygger på MSB:s vägledning för informationssäkerhet vid upphandling[1].

1.1 Syfte

Syftet med dokumentet är att:

- Fungera som stöd vid upphandlingen av varor och tjänster som innebär en informationshantering.

1.2 Begrepp och definitioner i dokumentet

Begrepp/förkortning	Beskrivning
KI	Karolinska Institutet
Konfidentialitet	Säkerställa att känslig information endast är åtkomlig för behöriga personer
Riktighet	Säkerställa att information är tillförlitlig, korrekt och komplett
Tillgänglighet	Säkerställa att information är tillgänglig utifrån verksamhetens behov
Informationsklassning	Att genom konsekvensanalys identifiera skyddsbehovet för en viss informationsmängd.
Upphandling	Inom ramen för begreppet ’upphandling’ ingår även inköp

[1] https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Vagledning-for-informationssakerhet-vid-upphandling/

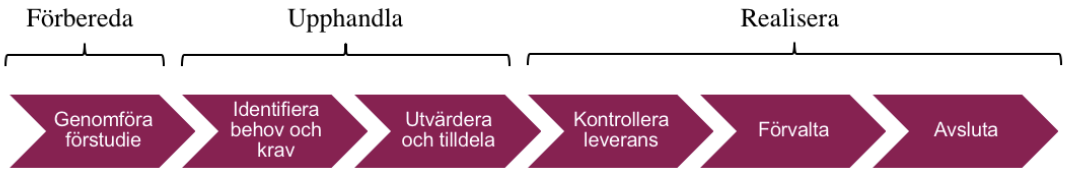
Dokumentansvarig Lukas Grönquist		Senast sparat 2019-05-29 13:13
Version 0.6	Senast uppdaterat av Lukas Grönquist	DNR

2 Process för upphandling och inköp

Informationssäkerhet vid upphandling och inköp innebär både att:

- den information som hanteras under upphandlingsarbetet behandlas på ett säkert sätt både inom KI och hos eventuella leverantörer (informationssäker upphandlingsprocess).
- varan eller tjänsten uppfyller de krav på informationssäkerhet som har identifierats som nödvändiga under hela avtalsperioden (informationssäker leverans)

Denna vägledning fokuserar primärt på den sistnämnda punkten – hur KI säkerställer att varan eller tjänsten uppfyller KI:s krav på informationssäkerhet. För att säkerställa detta ska processen nedan och tillhörande aktiviteter genomföras. För mer detaljerad information om varje steg i processen, se kapitel *3 Instruktioner för en säker upphandling.*



2.1 Förbereda

I den förberedande fasen ska en förstudie genomföras för att identifiera vilka grundförutsättningar som finns för att kunna ta beslut om det är aktuellt med en upphandling eller om behovet ska lösas på ett annat sätt.

Aktiviteter:

- Identifiera behovet av varan eller tjänsten
- Identifiera informationen som ska hanteras i varan eller tjänsten
- Genomföra en initial informationsklassning
- Identifiera interna och externa krav som påverkar informationen
- Genomföra en initial riskbedömning
- Besluta om hur behovet ska realiseras

2.2 Upphandla

Under upphandlingen ska informationssäkerhetskraven tas fram och dokumenteras vilka senare ska bli en del av de krav som ställs i upphandlingen. Inkomna anbud ska sedan utvärderas mot ställda informationssäkerhetskrav.

Aktiviteter:

- Besluta att behovet ska realiseras med upphandling
- Identifiera roller och ansvar som behöver delta vid kravställningen
- Genomföra en fördjupad informationsklassning
- Genomföra en fördjupad riskbedömning
- Identifiera säkerhetskrav baserat på genomförd informationsklassning och riskbedömning

- Definiera utvärderingsmodell för säkerhetskrav
- Färdigställa upphandlingsunderlag
- Godkänna upphandlingsmaterial
- Utvärdera leverantörer
- Utvärdera leverantörerrnas kravuppfyllnad
- Fatta tilldelningsbeslut
- Skriva avtal

2.3 Realisera

När upphandlingen är klar behöver det säkerställas att leveransen uppfyller ställda krav. I vissa fall kan det även vara önskvärt att göra regelbundna uppföljningar av leveransen för att säkerställa efterlevnad under tid.

Det sista steget vid en upphandling är när relationen med leverantören ska avslutas, det behöver då säkerställas att KI:s information inte längre finns kvar hos leverantören.

Aktiviteter:

- Säkerställa att leveransen uppfyller ställda krav
- Godkänna leverans
- Följa upp att säkerhetskraven uppfylls under tid
- Identifiera behov av förändringar
- Förbereda avslut av leverantörsrelationen
- Ta hem information
- Säkerställa att ingen information finns kvar hos leverantören

Dokumentansvarig Lukas Grönquist		Senast sparat 2019-05-29 13:13
Version 0.6	Senast uppdaterat av Lukas Grönquist	DNR

3 Instruktioner för en säker upphandling

3.1 Förbereda

Syftet med förberedelserna är att identifiera sådant som eventuellt skulle kunna förhindra en upphandling. Exempel på såna situationer skulle kunna vara om det visar sig att leverantören ska hantera känsliga personuppgifter enligt GDPR utanför EU/EES eller om en molntjänsteleverantör inte kan garantera tjänstens tillgänglighet.

3.1.1 Identifiera information och genomför initial klassning

Under förstudien behöver information som kommer att hanteras av leverantören under avtalstiden identifieras. Om det redan finns en genomförd informationsklassning för den information som ska hanteras av leverantören kan den med fördel användas. Om det inte finns ska en initial informationsklassning göras, KI:s informationssäkerhetssamordnade kan agera stöd vid den initiala klassningen. Denna behöver minst innehålla följande:

1. Vilka krav på konfidentialitet gäller för den identifierade informationen?
    a. Kommer själva upphandlingsunderlaget innehålla sekretessbelagda uppgifter eller uppgifter som är känsliga för KI?
    b. Kommer leverantören hantera sekretessbelagda uppgifter eller uppgifter som är känsliga för KI vid utförandet av tjänsten?
    c. Kommer leverantören hantera känsliga personuppgifter eller andra personuppgifter vid utförandet av tjänsten?
2. Vilka krav på riktighet gäller för den identifierade informationen?
    a. Vilka konsekvenser får det om informationen förvanskas/förändras?
3. Vilka krav på tillgänglighet gäller för den identifierade informationen?
    a. Hur lång tid kan KI vara/klara sig utan tillgång till informationen?
    b. Finns situationer eller tidpunkter när informationen måste vara tillgänglig? Exempelvis kan det finnas särskilda krav på att lönesystem måste vara tillgängliga vid löneutbetalningar.

3.1.2 Identifiera interna och externa krav

En viktig del i informationsklassningen är att identifiera interna och externa krav, flera krav kan påverka informationens klassning. Även om de interna eller externa kraven inte direkt påverkar skyddsbehovet för informationen kan det finnas specifika hanteringsregler i kraven.

Exempel på interna krav:

- KI:s regler och riktlinjer för informationssäkerhet[2]

[2] KI:s informationssäkerhetssida på Medarbetarportalen, https://ki.se/medarbetare/informationssakerhet?_ga=2.49810272.778891151.1545131827-2009057241.1543310822

- KI:s integritetsskyddspolicy[3]
- KI:s lösenordspolicy[4]

Exempel på externa krav, för detta arbete kan den juridiska enheten stödja:

- GDPR[5]
- MSBFS 2016:1[6]
- OSL[7]
- Avtal med samarbetspartners eller andra leverantörer

3.1.3 Genomföra initial riskbedömning

För den initiala riskbedömningen bör KI:s modell för riskbedömningar användas, även för detta arbete kan KI:s informationssäkerhetssamordnare agera stöd. Följande frågor bör besvaras i den initiala riskbedömningen.

1. Vad kan hända?
    - Specificera vad det är som ska upphandlas – är det ett system som ska driftas i KI:s miljö, någon form av utkontraktering (inklusive molntjänst) eller en kombination där tjänsten är uppdelad så att vissa delar hanteras internt och vissa externt. Utifrån detta bör ni sedan analysera vilka risker som leveransmodellen kan medföra.
    - Fundera ut händelser (hot) som kan påverka informationen, KI och andra parter.
2. Vad är sannolikheten och konsekvenserna om det inträffar?
    - Tänk på hur KI, andra parter, allmänheten och andra kan drabbas om hoten skulle realiseras.
    - Bedöm hur sannolikt det är att händelsen (hotet) realiseras och vad de potentiella konsekvenserna av händelsen skulle kunna bli.

3.1.4 Besluta om hur behovet ska hanteras

Baserat på den genomförda förstudien kan det nu beslutas om varan eller tjänsten ska upphandlas eller inte. Om det har identifierats allvarliga risker eller verksamhetskritisk information som leder till en osäkerhet kring upphandling ska KI:s informationssäkerhetsfunktion kontaktas och rådfrågas. I många fall går dessa risker att hantera genom att tillföra ytterligare säkerhetsåtgärder.

---

[3] https://ki.se/medarbetare/integritetsskyddspolicy

[4] https://ki.se/medarbetare/regler-for-losenord-pa-karolinska-institutet

[5] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

[6] Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1)

[7] Offentlighets- och sekretesslag (2009:400)

3.2 Upphandla

När det är beslutat att en upphandling ska genomföras behöver informationssäkerhetskraven för tjänsten eller varan identifieras.

För att uppnå ett bra resultat av upphandlingen kan personer med olika kompetenser behöva delta. Exempel på kompetens som kan behövas:

- **Förvaltning** - för att ställa krav på hur samarbetet med leverantör ska fungera – både under och efter avtalets tid.
- **Informationshantering** - för att ställa krav på hur informationen ska delas, bearbetas, lagras.
- **Dataskydd (juridiska enheten)** – för att ställa krav på en eventuell hantering av personuppgifter samt för att upprätta ett personuppgiftsbiträdesavtal
- **Informationssäkerhet** - för att formulera informationssäkerhetskrav samt för att bevaka informationssäkerhetsfrågor som uppkommer under upphandlingen
- **IT-säkerhet** - för att formulera IT-säkerhetskrav samt för att bevaka IT-säkerhetsfrågor som uppkommer under upphandlingen
- **IT** - för att bedöma hur tjänsten kan kunna integreras i befintlig infrastruktur
- **Upphandling** - för att välja rätt förfarande, kvalitetssäkra upphandlingsdokumenten och säkerställa att upphandlingen resulterar i ett affärsmässigt och verksamhetsmässigt fungerande avtal.

Om ovanstående resurser används bör de även ha ett ansvar för att verifiera att kraven inom deras kompetensområden uppfylls av leverantören.

3.2.1 Säkerhetskrav vid upphandlingen

För att kunna identifiera informationssäkerhetskraven behöver en fördjupning göras i vilken information som ska hanteras och tillhörande risker. Detta görs genom en fördjupad informationsklassning och riskbedömning.

Fördjupad informationsklassning:

Om informationen inte redan har genomgått en fördjupad informationsklassning behöver detta göras. Denna informationsklassning ska genomföras med KI:s metodik för informationsklassning vilken resulterar i ett antal utvalda säkerhetsåtgärderna som finns i Compliance Portalen[8]. För att få tillgång till säkerhetsåtgärderna behöver KI:s informationssäkerhetsavdelning kontaktas. De säkerhetsåtgärder som finns i Compliance Portalen bygger på den internationella säkerhetstandarden ISO/IEC 270001.

Observera att detta är en djupare analys än vad som ska göras i förstudien.

Fördjupad riskanalys:

Riskanalysen ska identifiera om de säkerhetsåtgärder som har tagits fram efter informationsklassning är tillräckliga eller om ytterligare säkerhetsåtgärder behöver ställas på:

- Leverantören

[8] https://ki.se/medarbetare/informationssakerhet

- Varan eller tjänsten
- KI:s organisation

Under riskanalysen ska de identifierade riskerna dokumenteras, potentiella konsekvenser ska beskrivas. De åtgärder som planeras för att minska dessa risker ska också identifieras och dokumenteras.

I avtalet bör det även finnas information om vilka säkerhetsåtgärder som ska följas upp, hur detta ska ske och av vem och med vilken frekvens.

3.2.2 Informationsägarens roll

Riskbedömningen och föreslagna säkerhetsåtgärder ska överlämnas till informationsägaren som fattar beslut om hur riskerna ska hanteras. Eftersom att skadan/konsekvenserna av eventuellt bristande säkerhet drabbar informationsägaren så är det denna som måste bedöma resultatet av både informationsklassningen och riskbedömningen.

3.2.3 Specifika frågeställningar för upphandling av IT-system:

Inför en upphandling av IT-system bör följande frågeställningar lyftas upp och diskuteras av berörda parter inom KI.

- Hur styrs åtkomsten till KI:s information? Vad kan vi styra gällande åtkomst till exempel KI:s driftmiljö (tid när leverantören kan komma åt, beställning av öppning och stängning av åtkomst till KI:s miljö)? Hur bör behörighetshanteringen se ut? Vilka olika åtkomstgrupper behövs inklusive behörigheter för att genomföra support samt teknisk administration av IT-miljön?
- Vilken typ av spårbarhet (loggning) ska finnas för användaraktiviteter och teknisk administration? Hur ska granskning av dessa loggar göras?
- Hur ska informationsutbytet göras mellan leverantören och KI? Genom åtkomst eller en överföring och hur?
- Hur ska KI skydda informationen under lagring och överföring? Vilka krypteringslösningar ska användas?
- Vilken tillgänglighet i tjänsten (inklusive återställningstider) måste leverantören uppfylla?
- Ska leverantören ansvara för att det finns strukturerad ändringshantering och testmiljöer för att prova uppdateringar?
- Vilka krav ställer KI på leverantörens rutiner för hantering av sårbarheter i IT-miljön?
- Hur är leverantörens IT-arkitektur uppsatt och konfigurerad, och vilka säkerhetsåtgärder är införda? Ger detta sammantaget informationen tillräckligt skydd? Skiljer leverantören driftmiljö och testmiljö från varandra? Har de några rutiner för vilken information som de får hantera i olika IT-miljöer? Hur sker godkännandet av att flytta information från test till drift?
- Vem ansvarar för licenser och för att uppfylla immateriella rättigheter? Vilket skydd mot skadlig kod har leverantören? Finns skydd för att upptäcka försök till och förhindra obehörig åtkomst?

- Vilka krav har KI på säkerhetskopiering av informationen? Hur ska leverantören testa säkerhetskopior? I vilket format ska leverantören lagra informationen? Vad är maximal tid för att återläsa informationen?
- Hur vill KI att leverantören ska rapportera de eventuella incidenter (hos leverantören) som kan orsaka konsekvenser för KI? Har leverantören något arbetssätt för hur de ska upptäcka, hantera och utreda incidenter?
- Vilken support vill KI att leverantören ska tillhandahålla?
- Behöver KI reglera åtkomst till källkoden på något sätt?
- Hur ser flexibiliteten ut, det vill säga KI:s möjlighet att skala upp användningen av tjänsten på ett ekonomiskt fördelaktigt sätt?
- Om leveransen är att utveckla programvara, har leverantören:
    - Rutiner och miljöer för att hantera kod på säkert sätt?
    - Rutiner för säker programmering?
    - Testmiljöer och testdata som säkerställer slutproduktens kvalitet och uppfyller rättsliga krav till exempel avseende behandling av personuppgifter?

3.3 Realisera

När varan eller tjänsten är levererad måst KI följa upp att leverantören uppfyller det som står i avtalet.

3.3.1 Leveransgodkännande

Det första steget i uppföljningen är att kontrollera att alla leveranser uppfyller de krav som har ställts. Detta innebär att dokumentera resultatet av de verifieringar (tester av att kraven uppfylls) som har genomförts. Hur själva leveransgodkännandet ska gå till ska framgå av avtalet.

Om driften är extern behöver KI tillsammans med leverantören säkerställa att alla viktiga säkerhetsåtgärder fungerar. Den externa leverantören kanske behöver åtgärder eventuella brister innan leveransen kan accepteras.

3.3.2 Uppföljning, kravuppfyllnad av leveransen

Under avtalets tid bör det regelbundet genomföras uppföljningar av hur leverantören uppfyller de säkerhetsåtgärder som avtalet innehåller. Detta görs för att kunna bibehålla säkerheten i den upphandlade produkten eller tjänsten under avtalstiden.

Om det uppstår några problem vid uppföljningen kan det krävas extra uppföljning.

3.3.3 Förbereda slutet på en avtalsrelation

När en avtalsperiod går ut är det av stor vikt att KI får tillbaka all information tillhörande KI från leverantören (om det krävs). Dessutom behöver informationen vara i ett format som såväl KI som andra leverantörer kan använda.