Informationssäkerhet

Stödanvisning
anskaffning och utveckling

Östhammars kommun

Målgrupp	Upphandlingsfunktion, chefer och nyckelpersoner alla kontor och verksamheter
Avsändare	Kommunledningskontoret, Digitalisering och projektledning
Dokumentansvarig	Informationssäkerhetssamordnare
Framtagen	2024-10-09
Reviderad	-

ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Innehåll

Innehåll

Innehållet utgår från kommunens program och vägledning för informationssäkerhet och ger en fördjupad beskrivning över anskaffning (upphandling) och utveckling av IT-tjänster. Här ges stödanvisningar för kravställning så att avtalet omfattas av sådana krav att informationen hanteras, skyddas och följs upp i enlighet med kommunens styrdokument och verksamheternas krav på säkerhet och skydd utifrån klassning.

Mål och syfte

Målet är en ensad process för upphandling och utveckling som svarar mot externa krav, interna behov och som bidrar till att skydda informationen i kommunens verksamheter. Syftet är att kunna kravställa en tillfredställande säkerhet vid upphandling.

Att upphandla it-system

Med it-system menas alla informationsbehandlande tekniska system, från fristående produkter till hela IT-miljöer som antingen driftas internt (IT-centrum) eller externt (t.ex. molntjänst). Även tjänster som utveckling och anpassning av system och olika drifttjänster ingår.

Steg 1 – Förberedelse

1.1 Kartlägga information

Kartlägg vilken slags information som kommer att hanteras och som leverantören kommer att få tillgång till under avtalstiden. Använd *mallen för kartläggning av information* som stöd.

1.2 Genomför en första klassning av informationen – Typ A

När informationen är kartlagd behöver en första informationsklassning göras på den tänkta informationen. Resultatet används vid kravspecificeringen. Om det redan finns en genomförd informationsklassning kan den användas som underlag. Som stöd kan annars *mallen för klassning av information* användas.

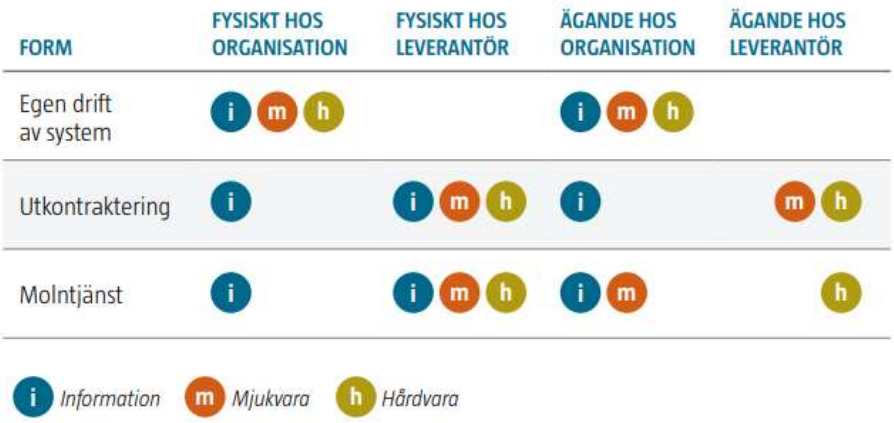
1. Vilka krav på ***konfidentialitet*** gäller för informationen?
    - Kommer upphandlingsunderlaget innehålla sekretessbelagda uppgifter eller uppgifter som är känsliga för organisationen?
    - Kommer leverantören hantera sekretessbelagda uppgifter eller uppgifter som är känsliga för organisationen vid själva utförandet av tjänsten?
    - Kommer leverantören hantera känsliga personuppgifter eller andra personuppgifter?
2. Vilka krav på ***riktighet*** gäller för informationen?
    - Vilka konsekvenser får det om informationen är felaktig eller blir förstörd?
3. Hur ser ***tillgänglighetsbehoven*** för informationen ut?
    - Hur lång tid kan organisationen vara utan informationen?
    - Finns det situationer eller tidpunkter när informationen måste vara tillgänglig?

1.3 Identifiera samhällsviktig verksamhet

En viktig del i förberedelsen är att fastställa om särskilda krav behöver ställas på leverantören för att denne kommer att leverera något till en samhällsviktig verksamhet.
Se ”MSB:s Upphandling till samhällsviktig verksamhet – en vägledning”

1.4 Klargör var informationen finns

Vid upphandling av it-system behöver man utgå från informationsklassningen och klargöra var informationen, mjukvaran respektive hårdvaran befinner sig fysiskt. Det påverkar vilka och mot vem kraven ska ställas. Oavsett driftform är det viktigt att ta hänsyn till var informationen befinner sig när den delas, bearbetas och lagras och hur den slutligen arkiveras eller förstörs. Bilden nedan visar vem som har åtkomst till information, mjukvara och hårdvara genom att visa var dessa finns fysiskt och hur ägandeförhållandena ser ut.



Källa: MSB

Om organisationen t.ex. ska köpa it-system för egen drift, översta raden i bilden, finns information, mjukvara och hårdvara fysiskt hos oss (IT-centrum). Vi hanterar uppdateringar av systemet utan att leverantören behöver ha åtkomst till det. Vid ut kontraktering (låta extern leverantör sköta driften), mellersta raden, kommer både hårdvara, mjukvara finnas fysiskt hos leverantören, medan informationen är åtkomlig både för oss och leverantören.

1.5 Identifiera interna och externa krav

Interna krav – Finns det några regler eller övriga interna behov som berör upphandlingen? Det kan t.ex. vara policyer, detaljerade styrningar kring hur organisationen kan, bör/ska agera eller rekommendationer av olika slag.
Externa krav – Finns det några rättsliga krav eller övriga externa behov och krav för det som ska upphandlas? T.ex. EU-förordningar, NIS2, GDPR, svenska lagar och förordningar, myndighetsföreskrifter. Beroende på vilken typ av information som kommer att omfattas kan externa krav utesluta upphandling. T.ex. om man vill upphandla en molntjänst och där kommer känsliga personuppgifter att hanteras. Enligt GDPR måste personuppgifter skyddas enligt specifika säkerhetskrav.

1.6 Genomför en första riskbedömning

En riskbedömning behöver göras för att förstå de risker som är förknippade med att hantera informationen. Bedömningen görs på den information som förväntas hanteras, inte på systemet/tjänsten. Om det redan finns en genomförd riskbedömning (riskanalys) kan den användas som underlag. Som stöd kan annars *mallen för riskhantering* användas.

1. ***Vad*** kan hända?
    - Specificera vad det är som ska upphandlas – är det ett system som ska driftas i egen miljö, extern drift/molntjänst eller en kombination där vissa delar hanteras externt och vissa internt?
    - Fundera ut händelser (hot) som kan påverka informationen, organisationen, kunder och andra.
2. Vad blir ***konsekvenserna*** om det inträffar?
    - Hur kan organisationen, allmänheten, kunder och andra drabbas?
3. Hur ***sannolikt*** är det att det inträffar?
    - Bedöm hur sannolikt det är att det händer
4. Behöver en ***konsekvensbedömning*** göras?

Dokumentera riskbedömningen och ge den chef som äger risken möjlighet att komplettera om denne inte varit med vid bedömningen.

Steg 2 – Upphandla

Det här avsnittet tar upp de delar av upphandlingen som handlar om fastställande av krav på informationssäkerhet och vad man behöver tänka på när avtal skrivs för att säkerställa en säker leverans.

2.1 Roller i upphandlingen

Under upphandlingsarbetet behövs någon som ansvarar för att bevaka informationssäkerhetsfrågor. Detta görs genom:

- att kravställa
- att utvärdera olika leverantörers anbud avseende säkerhetsåtgärder och
- att kontrollera att införda säkerhetsåtgärder omhändertagit informationsägarens intressen samt
- att kontrollera att leverantören och de avtalade säkerhetsåtgärderna svarar mot ställda krav

I kravställningen ska det framgå vilka roller och ansvar som leverantören måste ha för att möta ställda krav.
Vid behov kontakta informationssäkerhetsteamet, infosakerhet@osthammar.se

2.2 Säkerhetskrav

Vid Steg 1 - Förberedelse utförs en första informationsklassning och riskbedömning på ett övergripande plan. Genom en fördjupad informationsklassning och riskbedömning får man fram de underlag som krävs för att få fram rätt informationssäkerhetskrav. Informations-säkerhetskraven baseras sedan på vilken nivå informationen är klassad (nivå 1, 2 eller 3). Som stöd till upphandlingen finns *bilaga Bruttokravlista enligt informationssäkerhet ISO-*

standard 27002 att använda där informationssäkerhetskrav väljs utifrån, klassning, behov och tillämplighet.

Beroende på informationens känslighet, behov av riktighet och tillgänglighet kan kraven behöva utökas. I anbuden ska det tydligt framgå hur leverantören garanterar säkerheten utifrån kravställningen som ställts. Utöver de informationssäkerhetskrav som tas fram rekommenderas även krav på att anbudsgivarna ska fylla i *bilaga Säkerhetsdeklaration*.

2.3 Genomför en fördjupad informationsklassning – Typ B

Fördjupad informationsklassning motsvarar den informationsklassning som normalt genomförs för att identifiera vilken konsekvens otillräckligt skydd kan få för organisationen avseende konfidentialitet, riktighet och tillgänglighet (se *stödanvisningarna för kartläggning, klassning och riskhantering*). Den utförs för att verifiera om informationssäkerhetskraven fortfarande är samma som vid typ A- klassningen (den första klassningen) eller om det har förändrats. Det gäller både

- information som ingår i själva upphandlingen och som anbudsgivaren måste få kännedom om för att kunna lämna anbud och
- information som överlåts till leverantören att hantera, i t.ex. ett verksamhetssystem

Använd klassningens resultat för att fastställa vilka säkerhetsåtgärder leveransen ska uppfylla.

2.4 Genomför en fördjupad riskbedömning

Syftet med fördjupad riskbedömning är att identifiera om de säkerhetsåtgärder som identifierats är tillräckliga eller om ytterligare säkerhetsåtgärder behöver ställas på

- leverantören,
- varan eller tjänsten,
- den egna organisationen/verksamheten.

Om nya förutsättningar om hur skyddet för informationen kommer att se ut framkommer under upphandlingen behöver riskbedömningen kompletteras utifrån de nya förutsättningarna. T.ex. om den tänkta tekniska lösningen som framkommer av anbuden är en annan än den som riskbedömts från början. Som stöd finns *mallen utökad riskanalys.*

Både informationsklassningen och riskbedömningen med föreslagna säkerhetsåtgärder lämnas sedan till informationsägaren och chefen som äger risken för beslut om hur riskerna ska hanteras.

2.5 Kompetenser i upphandlingen

Beroende på vad som ska upphandlas kan, förutom upphandlingsfunktionen och informationssäkerhetssamordnare, följande kompetenser behövas.

- **Förvaltning** för att säkerställa krav på hur samarbetet med leverantören ska fungera under avtalstiden och när avtalet upphör.
- **Informationshantering** för att vägleda i att ställa krav på hur information delas, bearbetas och lagras.
- **Informationsägarskap** och **verksamhetsansvar** för att identifiera krav och behov

- **IT** för att bedöma hur tjänsten ska kunna integreras på lämpligt sätt i befintlig infrastruktur
- **IT-säkerhet** för att formulera it-säkerhetskrav
- **Dataskydd** för att bevaka alla dataskyddsfrågor
- **Arkivering** för att bevaka gallring och arkiveringsfrågor

Steg 3 - Avtal

3.1 Krisberedskap, force majeure

Om upphandlingen avser att säkerställa behovet av kontinuitet och driftsäkerhet vid kriser behöver man tydliggöra leverantörens ansvar genom att ta in en klausul avseende hur force majeure i avtalet inte gäller under vissa förutsättningar. På detta sätt får man kontroll över vilka händelser som enligt avtalet ska ingå i force majeure.

3.2 Leverantörens säkerhetskrav på oss

I vissa fall kan även leverantören ställa säkerhetskrav på oss, eftersom en kunds bristande säkerhet kan riskera säkerheten för både leverantören och deras övriga kunder. De krav som leverantören ställer på vår organisation kan till exempel omfatta krav på visst skydd mot skadlig kod, viss brandväggskonfiguration eller viss behörighetshantering. Om leverantören har denna typ av krav ska det framgå i avtalet.

3.3 Arkivering och gallring

Utifrån rättsliga krav och verksamhetens egna behov (se kommunens dokumenthanterings-planer) ska viss information gallras medan annan måste bevaras under kortare eller längre tid. Därför kan man behöva ställa särskilda krav i avtalet på hur gallring och arkivering ska ske.

3.4 Vite

Avtalet behöver reglera möjligheten att kräva vite om säkerhetsåtgärder inte uppfylls. Vitesbeloppen bör sättas på en nivå så att risken minimeras för att leverantören hellre tar ett vitesföreläggande än den ekonomiska kostnad som ett fullföljande av avtalet kan innebära.

3.5 Tilldelning av kontrakt

Innan man fattar ett tilldelningsbeslut och undertecknar avtalet bör man genomföra en fördjupning av befintlig riskanalys. Denna ska inbegripa den leverantör som ni nu valt samt eventuella underleverantörer. Utgå från den lösning ni valt, de säkerhetsåtgärder som leveransen innehåller och avtalets löptid vid riskbedömningen. Stöd finns i *mallen utökad riskanalys.*

Steg 4 - Realisera, förvalta och avsluta upphandlingen

Här börjar man med att säkerställa att leveransen har de säkerhetsåtgärder som avtalats. Därefter förvaltas relationen med leverantören och genomför regelbundna uppföljningar av att leveransen över tid uppfyller avtalet. När avtalet avslutas ska informationen inte längre finnas kvar hos leverantören.

4.1 Uppföljning, kontroll och kvalitetssäkring

Uppföljning och kontroll är viktigt för att kunna bibehålla säkerheten i den upphandlade produkten eller tjänsten under avtalstiden, de säkerhetsåtgärder som man kommit överens om i avtalet bör regelbundet följas upp med leverantören.
Dokumentera fortlöpande överenskommelser och sådant som kommuniceras muntligt.

Stöddokument, bilagor och mallar

Stödmaterial nås via INES Anskaffa och utveckla och Vägledning och stöd

- Bruttokravlista enligt informationssäkerhet ISO-standard 27002
- Utökad riskanalys
- Säkerhetsdeklaration (leverantör)
- Sekretessförbindelse informationssäkerhet (NDA, leverantör)