Informationssäkerhet vid upphandling - riktlinje



Antagen av kommunstyrelsen 2024-03-06

Dokumentinformation

Fastställt av:	Kommunstyrelsen
Fastställt, datum:	2024-03-06
Dokumentsansvarig:	Chef säkerhetsenheten
Ansvarig för revidering:	Informationssäkerhetsamordnare
Gäller för:	Ansvariga för upphandlingar
Gäller till, datum:	Gäller tills vidare. Uppdateras vid behov.

Innehållsförteckning

Dokumentinformation 2
Informationssäkerhet vid upphandling 4
1 Inledning 4
2 Informationssäkerhet vid upphandling 4
2.1 Upphandlingens flöde 4
2.2 Att tänka på när organisationer delar tjänster 4
2.3 Att tänka på vid ramavtal 5
2.4 Att tänka på vid säkerhetsskyddad upphandling 5
3 Förbered upphandling 5
3.1 Styrande dokument 5
3.2 Identifiera information och gör en initial informationssäkerhetsklassning 5
3.3 Genomför en riskbedömning 6
4 Genomför upphandlingen 6
4.1 Definiera informationssäkerhetskrav 6
5 Att upphandla IT-system 6
5.1 Var kommer informationen att finnas 6
5.2 Särskilda informationssäkerhetskrav vid upphandling av IT-system 7
6 Mer information 7

Informationssäkerhet vid upphandling

1 Inledning

Information är en av kommunens viktigaste tillgångar och en väsentlig förutsättning för att kunna bedriva verksamheten. Kommunens informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt.

Detta dokument vänder sig till informationsägare som ska upphandla nya produkter (varor eller tjänster) i syfte att tillse rätt krav utifrån informationssäkerheten.

2 Informationssäkerhet vid upphandling

Informationssäkerhet vid upphandling innebär att:

1. Den information som hanteras under upphandlingsarbetet behandlas på ett säkert sätt både inom egna organisationen och hos intresserade leverantörer (informationssäker process)
2. Varan eller tjänsten uppfyller de krav på informationssäkerhet som identifierats som nödvändiga under hela avtalsperioden (informationssäker leverans).

2.1 Upphandlingens flöde

För att förtydliga när olika aktiviteter för en säker informationshantering ska genomföras finns ett arbetsflöde med tre steg.

- Steg 1: Förbereda. Förstudie genomförs i syfte att identifiera vilka behov som finns av informationssäkerhet. Informationen ska informations-säkerhetsklassificeras.
- Steg 2: Upphandla. Dokumentera informationssäkerhetskraven och lägg till dem bland de övriga krav som ställs i upphandlingen. Utvärdera inkomna anbud mot ställda krav.
- Steg 3: Realisera. Säkerställ att leveransen uppfyller kraven på informationssäkerhetsåtgärder. Genomför regelbundna uppföljningar under den tid avtalet gäller. Vid avtalets slut säkerställ att information inte finns kvar hos leverantören.

2.2 Att tänka på när organisationer delar tjänster

Kommunen kan gå samman och dela tjänster i stället för att själv upphandla, utveckla eller använda till exempel IT-system. Då kommunen delar tjänster med en annan kommun/organisation är det viktigt att klarlägga ansvar och roller, fastställa arbetssätt för hur informationssäkerhetskraven ska hanteras samt hur

kraven ska följas upp. Grundprincipen är att den eller de organisationer vars information ska hanteras formulerar sina informationssäkerhetskrav.

2.3 Att tänka på vid ramavtal

Vid tecknande av ramavtal behöver man identifiera de högsta informationssäkerhetskrav som kan bli aktuella.

Innehållet i ett ramavtal kan inte påverkas vid avrop varken gällande kravens utformning eller innehåll.

2.4 Att tänka på vid säkerhetsskyddad upphandling

Om den information som leverantören kommer att få åtkomst till faller in under Säkerhetsskyddslagen, kontakta säkerhetssamordnare. Upphandlingen ska genomföras med så kallade säkerhetsskyddsavtal (SUA). Säkerställ då att:

- erforderligt säkerhetsskyddsavtal finns med motparten
- en säkerhetsskyddsanalys av uppdraget genomförs och resultatet dokumenteras
- säkerhetskrav dokumenteras för respektive upphandling och förmedlas leverantören och säkerhetsskyddschefen.

3 Förbered upphandling

3.1 Styrande dokument

De styrdokument, utöver detta, som beskriver de interna kraven på informationssäkerhet är:

- Informationssäkerhet – policy
- Informationssäkerhet, fysisk och teknisk säkerhet – riktlinje
- Informationssäkerhet klassning och riskanalys – riktlinje

3.2 Identifiera information och gör en initial informationssäkerhetsklassning

Identifiera vilken information som kommer att hanteras under själva upphandlingen och vilken information som den externa aktören kommer att få tillgång till under avtalstiden. Utifrån den information som identifierats genomförs en initial informationssäkerhetsklassning.

Använd den enkla metoden som beskrivs i styrdokumentet: ”Informationssäkerhet klassning och riskanalys – riktlinje”.

Om den upphandlande verksamheten bedriver samhällsviktig verksamhet eller om det gäller Sveriges säkerhet så bör informationssäkerhetsklassningen göras enligt den kompletta metoden. Denna informationssäkerhetsklassning kan antingen

göras samlat utifrån all information som finns i systemet eller utifrån den enskilda informationstillgången.

3.3 Genomför en riskbedömning

Gör en riskbedömning för att värdera de risker som är förknippade med hanteringen av informationen.

- Vilka hot finns mot informationen? Vad kan hända?
- Vad blir konsekvenserna om det inträffar?
- Hur stor sannolikhet är det att de inträffar?
- Red ut om en konsekvensbedömning enligt Dataskyddsförordningen ska göras samt om förhandssamråd med Integritetsskyddsmyndigheten ska begäras vad gäller personuppgiftsbehandling.

4 Genomför upphandlingen

4.1 Definiera informationssäkerhetskrav

Ställ de informationssäkerhetskrav som behövs för att uppnå det skydd som man bedömt att informationstillgången behöver ha efter informationssäkerhetsklassningen. Standarden ISO 27000-serien kan vara ett stöd vid formuleringen av kraven. Realisera, förvalta och avsluta upphandlingen.

På denna punkt skiljer sig inte informationssäkerhet från andra krav som ska realiseras, förvaltas och följas upp.

5 Att upphandla IT-system

Informationssäkerhetskraven vid upphandling av IT-system utgår från informationssäkerhetsklassning och riskanalys. Utöver detta finns några speciella områden att ta hänsyn till, se nedan rubriker.

5.1 Var kommer informationen att finnas

Var kommer informationen finns vid olika driftsituationer? Informationen kan finnas hos kommunen, utkontrakterad hos en leverantör eller i en molntjänst.

De säkerhetsåtgärder som används för informationen ska motsvara det skyddsbehov som informationssäkerhetsklassningen ledde fram till. Vid både utkontraktering och molntjänst finns informationen tillgängligt fysiskt hos leverantören. Då gäller det att säkerställa via avtal att leverantören skyddar informationen i sin IT-miljö med de säkerhetsåtgärder som informationssäkerhetsklassningen lett fram till.

5.2 Särskilda informationssäkerhetskrav vid upphandling av IT-system

För mer information om respektive punkt nedan hänvisas till den rådgivning som lämnas från Myndigheten för samhällsskydd och beredskap (MSB).

- Definiera informationssäkerhetskrav enligt samma modell som under avsnitt 3.2 med särskilt fokus på kraven på IT-miljön.
- Reglera i avtal ansvarsförhållande mellan leverantör och organisation till exempel för säkerhetsåtgärder, backup-rutiner, skydd mot attacker av olika slag.
- Säkerställ behovet av kontinuitet och driftssäkerhet vid kriser och vad som gäller för krisberedskap och force majeure.
- Säkerställ kontrollen över användningen av underleverantörer, speciellt underleverantörer som är molntjänster.
- Säkerställ kännedom om leverantörens andra kunder så att förhållanden hos dessa inte kan påverka tillgången till informationen.
- Säkerställ säkerheten i överföringen och behörigheten till självbetjäningsgränssnitt.
- Säkerställ säkerheten vid leverantörens personals åtkomst till informationen, mjukvaran och hårdvaran.
- Säkerställ att informationen inte drabbas av inlåsningseffekter hos leverantören.
- Säkerställ eventuella rättsliga risker till exempel vilket lands regelverk som gäller för leverantören.

6 Mer information

För mer information hänvisas till den rådgivning som lämnas från Myndigheten för samhällsskydd och beredskap (MSB).

”Upphandla informationssäkert – en vägledning”

”Upphandling till samhällsviktig verksamhet – en vägledning”