Enhet

Datum 2023-12-04

Dnr LTU-2486-2021

Process
11.8 Köpa in varor och tjänster

Beslutsfattare: Rektor Dokumenttyp: Riktlinje Giltighetstid: tillsvidare	Beslutsdatum: 23-12-04 Träder i kraft: 23-12-04
Dokument som upphävs:	

Riktlinjer för informationssäkerhet vid upphandling och inköp

Innehållsförteckning

1. Inledning

Luleå tekniska universitet eftersträvar hög informationssäkerhet i all sin informationsbehandling. Genom ett systematiskt informationssäkerhetsarbete kan risker identifieras tidigt för att undvika att information kommer i orätta händer, förvanskas eller förstörs, vilket kan innebära dyra och tidskrävande åtgärder efter att ett avtal har ingåtts eller produkt anskaffats.

Det är särskilt viktigt att tidigt identifiera konfidentiell information som till exempel personuppgifter, forskningsdata eller annan verksamhetsinformation som kommer att omfattas och påverkas av upphandlingen eller inköpet. Känslig eller sekretessbelagd information och integritetskänsliga personuppgifter får inte behandlas t.ex. i molntjänster[1] utan att en mer ingående risk- och sårbarhetsanalys genomförts och nödvändiga säkerhetsåtgärder vidtagits. Det är viktigt att beslut om hantering av och tillgång till informationen är dokumenterat och fattat av ansvarig chef för verksamheten enligt Rektors besluts- och delegationsordning för LTU.

Informationssäkerhet i upphandlings- och inköpsprocessen är framför allt viktig vid anskaffning av tjänster eller produkter som kommer att hantera, bearbeta, lagra eller överföra verksamhetsinformation eller data på något sätt. Det handlar om att säkerställa att den upphandlade/inköpta tjänsten, produkten eller IT-stödet uppfyller de krav som identifierats som nödvändiga för att skydda informationen både inom vår organisation och hos leverantören under hela avtalsperioden.

2. Dokumentets syfte

Riktlinjen är en del av universitetets ledningssystem för informationssäkerhet och syftar till att säkerställa att universitets medarbetare är väl förtrogna med och kan följa gällande regelverk, lagar och förordningar relaterade till informationssäker upphandling och inköp. Dokumentet bygger i huvudsak på Myndigheten för samhällsskydd och beredskaps (MSB) vägledning om att upphandla informationssäkert[2].

Riktlinjen innehåller en beskrivning av vad informationssäkerhet innebär, en ansvarsöversikt och anvisningar om vad som ska göras inför ett informationssäkert inköp eller en upphandling. Oaktat om det gäller upphandling/inköp av en tjänst, produkt eller ett IT-stöd ska processen för systematisk informationssäkerhet följas för att uppnå en säker informationshantering. En beskrivning mer i detalj om hur processen går till finns i *Arbetsrutiner för informationssäkerhet vid upphandling och inköp*.

[1] Molntjänster är ett samlingsbegrepp för ett stort antal internetbaserade tjänster som tillhandahåller olika typer av IT-lösningar. Det kan röra sig om programvaror, datalagring och andra samarbetsfunktioner.
[2] MSB1177 – november 2018

3. Ansvars- och uppgiftsfördelning

Ansvarig chef för verksamheten, enligt rektors besluts- och delegationsordning för LTU, ska säkerställa att det finns förutsättningar för att följa informationssäkerhetsprocessen enligt den modell som beskrivs under punkt 4.1. nedan. Informationssäkerhetsarbetet ska dokumenteras, beslutas och diarieföras.

Den enskilda medarbetaren eller annan som deltar i upphandlingen ansvarar för att följa gällande riktlinje och hålla sig informerad om hur informationssäkerhet vid upphandlingen eller inköpet av tjänster, varor eller IT-system ska hanteras.

Inom Verksamhetsstödet finns det, förutom stöd för själva inköpet/upphandlingen, stöd för att identifiera informationssäkerhetskrav, IT-säkerhetskrav och legala krav som påverkar de grundläggande förutsättningarna för inköpet eller upphandlingen.

Innan inköp eller upphandling ska kontakt tas med informationssäkerhetssamordnare i god tid för stöd och rådgivning.

4. Informationssäkerhet vid upphandling eller inköp

Att genomföra en upphandling, direktupphandling eller ett inköp på ett informationssäkert sätt handlar om att identifiera och ställa rätt krav för att universitetets information ska hanteras på ett säkert sätt såväl internt som hos extern leverantör. Genom detta initiala arbete kan universitetet förhindra att viktiga informationssäkerhetskrav och andra krav förbises för att eventuellt tillkomma senare i upphandlings- eller inköpsprocessen, eller efter att universitetet ingått avtal vilket kan riskera att bli både kostsamt och tidskrävande men också äventyra informationssäkerheten.

Kraven på informationssäkerhet, och vid behov IT-säkerhet, ska framställas i en kravspecifikation och vara mycket tydliga och gå att utvärdera. Kraven som formuleras för den specifika upphandlingen eller inköpet, ska dessutom definieras tydligt genom att ange vilka krav som är ”ska-krav” respektive ”bör-krav”.[3]

Underlaget för en kravspecifikation ska bygga på informationsklassningen, självvärderingen samt risk- och sårbarhetsanalysen för den informationsbehandling som upphandlingen/ inköpet omfattas av eller ska hantera. Det är framför allt deltagare från verksamheten i den pågående upphandlings- eller inköpsprocessen som måste definiera vilken information som berörs.

4.1 Informationssäkerhetsprocess

En informationsklassning ska göras baserat på informationens känslighet och skyddsvärde med utgångspunkt från aspekterna konfidentialitet, riktighet och tillgänglighet (K,R,T) Informationsklassningen ska klarlägga informationens skyddsbehov.

Det är av yttersta vikt att identifiera säkerhetskrav och lagkrav som kommer att ligga till grund för de informationssäkerhetskrav som ska ställas på tjänsten, produkten eller IT-stödet (s.k. självvärdering).

Därefter ska en risk- och sårbarhetsanalys genomföras för att öka medvetenheten och kunskapen hos beslutsfattare och verksamhetsansvariga om hot, risker och sårbarheter för det egna verksamhetsområdet med anledning av upphandling eller inköp. Denna analys bidrar till att skapa ett underlag för planering, införande samt utbildning för upphandlad vara eller tjänst.

En närmare beskrivning av hur detta arbete genomförs i form av rutiner och arbetsgång finns i dokumentet *Arbetsrutiner för informationssäkerhet vid upphandling och inköp.*

4.2 Hantering av känslig och sekretessbelagd information

Känslig eller sekretessbelagd information och integritetskänsliga personuppgifter[3] får inte behandlas utan att en mer ingående risk- och sårbarhetsanalys genomförts och nödvändiga säkerhetsåtgärder vidtagits. Beslut om behandling och åtgärder ska tas av ansvarig chef och ska vara dokumenterad och diarieförd.

I de fall där molntjänster blir aktuella som ett IT-stöd för informationshanteringen ska legala risker beaktas gällande personuppgifter hos leverantör utanför EU/ESS eller av EU-kommissionens beslutade lista för andra länders tillgång till informationen.[4]

4.3 Säkerhetsskyddad upphandling

När universitetet har för avsikt att genomföra en upphandling som hanterar information som behöver vara säkerhetsskyddad ställs särskilda krav. Det kan handla om:

- Skydd mot brott som kan hota Sveriges säkerhet
- Skydd av hemliga uppgifter som rör Sveriges säkerhet
- Skydd mot terrorism

[3] GDPR
[4] European Commission, Adequacy decisions: How the EU determines if a non-EU country has adequate level of data protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en,
Amerikanska organisationer: Participant Search (dataprivacyframework.gov)

Vid säkerhetsskyddad upphandling med säkerhetsskyddsavtal ska det i vissa fall upprättas en särskild säkerhetsskyddsbedömning. Den upphandlande myndigheten, Luleå tekniska universitet, ska innan upphandlingsprocessen samråda med Säkerhetspolisen som är tillsynsmyndighet. I ett förtydligande ska ansökan om samråd med Säkerhetspolisen ske innan myndigheten annonserar upphandlingen.

Mer information om vad som gäller finns i Arbetsrutinerna för informationssäkerhet vid upphandling och inköp.

5. Uppföljning

Uppföljning och dokumentation om de ställda informationssäkerhetskraven är ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som har avtalats, är viktigt för att kunna bibehålla säkerheten i den upphandlade produkten eller tjänsten under avtalstiden.