Ärendenummer
[Ärendenummer]
Motpartens ärendenummer
[Motpartens ärendenummer]

Dokumentdatum
2025-10-06

Konfidentialitetsnivå
[Konfidentialitetsnivå]

Avtalsbilaga avseende informationssäkerhet

De gula texterna nedan avser exempel på vilka stycken som ska finnas med och används av den upphandlande verksamheten för att ”filtrera ut” relevanta krav utifrån identifierade skyddsvärden. Vilka krav som är aktuella för en specifik upphandling kommer alltså att framgå av förfrågningsunderlaget för respektive upphandling.

Kontaktpersoner

Leverantörens kontaktperson: [Namn]

Beställarens kontaktperson: [Namn]

Bakgrund

Denna bilaga reglerar vilka informationssäkerhetskrav Beställaren har för den information som behandlas i Uppdraget.

Syfte med informationssäkerhetskrav är att säkerställa Trafikverkets verksamhet och dess kontinuitet samt minimera konsekvenserna av informationssäkerhetsincidenter.

Mål med informationssäkerhetskrav är att skydda informationstillgångar avseende konfidentialitet, riktighet och tillgänglighet. Med informationstillgång avses både information och de system och utrustning som information behandlas i.

Skydd av informationstillgångar från obehörigt röjande, manipulation, förstörelse och åtkomst sker med organisatoriska, fysiska, tekniska och personalrelaterade säkerhetsåtgärder. I vissa fall behöver även äktheten i informationen kunna verifieras. Säkerhetsåtgärder ska förebygga, upptäcka och korrigera informationssäkerhetsincidenter.

Kraven har sin bakgrund dels i författningskrav, dels i krav i standarden SS-EN ISO/IEC 27001 och 27002 samt verksamhetskrav.

Omfattning

Kraven omfattar all information oavsett om informationen behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö som informationen förekommer.

Informationssäkerhetskraven omfattar information som Leverantören erhåller från Beställaren, den information som Leverantören upprättar inom Uppdraget eller får kännedom om på annat sätt och som rör Beställarens verksamhet.

Om säkerhetsskyddsklassificerade uppgifter hanteras i avtalet
//För uppgifter som säkerhetsskyddsklassificerats gäller istället för denna bilaga de regler som framgår av säkerhetsskyddsavtal.//

Allmänna krav

Informationssäkerhetskraven omfattar information som Leverantören erhåller från Beställaren samt information som Leverantören upprättar inom Uppdraget eller får kännedom om på annat sätt och som rör Beställarens verksamhet. Kraven gäller oavsett om informationen behandlas automatiskt eller manuellt, och oberoende av i vilken form eller IT-miljö informationen förekommer.

Information får endast hanteras i informationssystem som uppfyller Beställarens krav i enlighet med avtalet.

Nedan text ska finnas med om uppgifterna hade omfattats av sekretess enligt offentlighets- och sekretesslagen (2009:400) om uppgifterna i handlingen förvarats hos Trafikverket. Med handling avses i detta fall exempelvis ett dokument som Leverantören erhållit eller skapat som en del av Uppdraget.
//Leverantören får inte sprida eller på annat sätt nyttja utredningsmaterial eller arbetsresultat som tas fram inom ramen för Uppdraget utan Beställarens skriftliga medgivande.//

Ledningssystem för informationssäkerhet

Kravet på ett systematiskt informationssäkerhetsarbete är två-delat och utgår från det bedömda skyddsvärdet för den information som ska hanteras inom ramen för avtalet. Det finns ett högre krav som gäller för information med högre skyddsvärde och typiskt sett sekretessreglerade uppgifter samt ett lägre krav för information med lägre skyddsbehov. Om kravet på ett

ledningssystem för informationssäkerhet är aktuellt kommer något av följande kravnivåer att framgå av förfrågningsunderlaget. I samband med upphandlingsprocessen kommer beställande verksamhet att be leverantören kort beskriva sitt informationssäkerhetsarbete enligt en särskild mall som är anpassad efter de två nivåerna nedan.

//Leverantören ska för de delar av verksamheten som berörs av Uppdraget ha ett ledningssystem för informationssäkerhet (LIS) som baseras *på SS-EN ISO/IEC 27001* och *SS-EN ISO/IEC 27002* eller likvärdigt.//

Alternativt…

//Leverantören ska för de delar av verksamheten som berörs av Uppdraget arbeta i former som följer ledningssystem för informationssäkerhet baserat på *SS-EN ISO/IEC 27001* och *SS-EN ISO/IEC 27002* eller likvärdigt.//

Genomgång av krav och samråd

Detta krav gäller vid behandling av information med högre skyddsbehov.
//Beställaren ska tillsammans med Leverantören i samband med kontraktstecknandet eller startmöte gå igenom informationssäkerhetskraven för att skapa så goda förutsättningar som möjligt för en god säkerhetskultur och ett gott informationssäkerhetsarbete. Detta ska ske innan Uppdraget inleds. Återkommande samråd ska ske minst två gånger varje 12-månadersperiod och när det är påkallat. Beställaren ansvarar för att kalla till de halvårsvisa mötena. Leverantören ansvarar för att kalla till samråd när det är påkallat.//

Alternativt…
//Beställaren ska tillsammans med Leverantören i samband med kontraktstecknandet eller startmöte gå genom informationssäkerhetskraven för att skapa så goda förutsättningar som möjligt för en god säkerhetskultur och ett gott informationssäkerhetsarbete. Detta ska ske innan Uppdraget inleds. Samråd ska ske vid behov i syfte att lösa frågor som uppkommer efterhand avseende informationssäkerhet. Beställaren och Leverantören ansvarar var och en för sig att kalla till samråd när behov uppstår.//

Kontaktperson

Leverantören ska ha en utpekad kontaktperson i informationssäkerhetsfrågor inom Uppdraget. Kontaktpersonen ska vara insatt i de informationssäkerhetskrav som gäller för Uppdraget. Kontaktpersonen ska i Uppdragets informationssäkerhetsfrågor ha mandat

att fatta beslut i förhållande till Beställaren.
Om Leverantören byter kontaktperson ska ny kontaktperson meddelas till Beställaren.

För att säkerställa att Leverantören kan rapportera incidenter även utanför kontorstid, enligt avsnittet Incidentrapportering nedan, ska Beställaren förse Leverantören med en uppdaterad kontaktlista.

Krav på underleverantörer

Detta krav gäller vid behandling av information med skyddsbehov samt om uppgifter omfattas av sekretess
//Leverantören får vid hantering av Beställarens information inte anlita underleverantörer för fullgörande av Uppdraget utan Beställarens godkännande. Leverantören ska till Beställaren redovisa samtliga underleverantörer som ska användas inom ramen för Uppdraget och som ska behandla Beställarens information.

I det fall parterna avtalar om att Leverantören får använda angiven underleverantör ansvarar Leverantören för att underleverantören uppfyller samma krav som Leverantören förbinder sig till enligt denna bilaga.

Vid byte eller förändring av underleverantör ska Beställaren underrättas och godkänna underleverantören innan denne ges tillgång till Beställarens information.//

Användning av tjänsteleverantörer

Detta krav gäller vid behandling av information med skyddsbehov samt om det förekommer uppgifter som omfattas av sekretess eller personuppgiftsbehandling.
//Med tjänsteleverantör avses leverantörer som tillhandahåller funktioner eller tjänster för informationshantering som Beställaren inte har en avtalsrelation till genom Uppdraget. Det kan exempelvis vara olika typer av tjänster och funktioner för lagring, samarbete, dokumenthantering eller mjukvara vilka är baserade på en tjänsteleverantörs plattform och som tillhandahålls över internet.

Tjänsteleverantörer ska betraktas som underleverantörer vilket innebär att användning av tjänsteleverantörer för behandling av information inom ramen för Uppdraget inte är tillåtet utan godkännande från Beställaren. Det inkluderar anlitande av tjänsteleverantörer avseende service eller support

som innebär att tjänsteleverantören i sin service och support har åtkomst till Beställarens information.//

Behörighet för åtkomst till information

Behörighet till Beställarens information får endast ges till personer som deltar i Uppdraget.

Detta krav gäller vid behandling av information med skyddsbehov.
//Behörighet för åtkomst till Beställarens information får endast ges till personer hos Leverantören som behöver uppgifterna i sitt uppdrag och som har tillräckliga kunskaper i informationssäkerhet, se krav i kapitlet Kompetenskrav.

Med behörighet avses behörigheter som tilldelas i informationssystem och tjänster samt behörighet som ges för tillträde till områden och utrymmen där Beställarens information behandlas.
Utgångspunkten ska vara att man endast har tillgång till den information som man behöver för att kunna utföra sina arbetsuppgifter.//

Detta krav gäller om Leverantören ges tillgång till Trafikverkets informationssystem.
//Behörig för åtkomst till Beställarens informationssystem
Leverantören ska snarast, senast inom två dagar underrätta Beställaren om behörigheter behöver ändras eller ska upphöra rörande Leverantörens personal i Uppdraget. Detta ska ske exempelvis vid byte av arbetsuppgifter eller om deltagandet i Uppdraget upphör.
I de fall Leverantören själv förfogar över behörighetstilldelning till Beställarens informationssystem ska ändring göras snarast, senast inom två dagar.//

Detta krav (som förekommer i två nivåreglerade versioner) gäller om leverantören behandlar information i egna system eller hos tjänsteleverantör.
//Leverantören ska kvartalsvis följa upp att endast behöriga personer har åtkomst till Beställarens information.
Beställaren äger rätt att följa upp att angivna krav efterlevs genom att begära behörighetslistor som visar vilka som har åtkomst till Beställarens informationstillgångar och i vilket syfte åtkomsten har givits.
Leverantören ska kunna redovisa vilka personer som vid en given tidpunkt haft behörighet för åtkomst till Beställarens information. Redovisning ska kunna ske minst 3 månader bakåt i tid.

Leverantören ska kunna redovisa vilken information som Leverantörens medarbetare behandlat 1 månad bakåt i tid.//

Alternativt…
//Leverantören ska månadsvis följa upp att endast behöriga personer har åtkomst till Beställarens information.
Beställaren äger rätt att följa upp att angivna krav efterlevs genom att begära behörighetslistor som visar vilka som har åtkomst till Beställarens informationstillgångar och i vilket syfte åtkomsten har givits.
Leverantören ska kunna redovisa vilka personer som vid en given tidpunkt haft behörighet för åtkomst till Beställarens information. Redovisning ska kunna ske minst 6 månader bakåt i tid.
Leverantören ska kunna redovisa vilken information som Leverantörens medarbetare behandlat 3 månader bakåt i tid.//

Säker överföring av information

Säker överföring av information

Detta krav gäller vid behandling av information med skyddsbehov.
//Leverantören ska säkerställa att överföring av information ska ske på sådant sätt att inte obehöriga kan ta del av informationen eller att informationen obehörigen ändras eller förstörs. Det gäller överföring som Leverantören gör under genomförandet av Uppdraget såväl som vid överföring av information till Beställaren.

Beställaren och Leverantören ska senast vid startmötet komma överens om hur överföring av information ska genomföras mellan Leverantören och Beställaren som uppfyller kraven på informationssäkerhet.//

Digital signering

Detta krav gäller vid behandling av information med högre skyddsbehov.
//Beställaren har höga krav på riktighet. Leverantören ska därför ha möjlighet, om Beställaren så kräver, att kunna signera framtagna digitala handlingar med en typ av digital signering som Beställaren godkänner. Signering ska ske av behörig person hos Leverantören. Leverantören intygar i och med det handlingens äkthet. Signering ska ske när den digitala handlingen nått färdig status och godkänts. Syftet med signeringen är att säkerställa riktighet och autenticitet.

Beställaren och Leverantören ska senast vid startmötet komma överens om vilka metoder för signering som ska användas.//

Hantering av lagringsmedia

Detta krav gäller vid behandling av information med skyddsbehov.
//Information som överförs till olika lagringsmedia så som CD/DVD-skiva, minneskort, hårddisk eller USB-minne ska skyddas mot obehörig åtkomst och obehörig förändring. Om lagringsmediet innehåller information ska det skyddas mot obehörig åtkomst och hållas under uppsikt. Informationen ska krypteras och det ska krävas lösenord för åtkomst.

Innan avsändande till Beställaren ska Leverantören genomsöka innehållet på lagringsmediet efter skadlig kod. Genomsökningen får inte innebära att informationen i samband med skanningen röjs för obehörig.

Om lagringsmedia skickas via postförsändelse ska val av tjänst säkerställa att försändelsen är spårbar och att försändelsen tas emot av rätt mottagare, det vill säga skickas med rekommenderad post (REK).//

Kompetenskrav

Detta krav gäller vid behandling av information med skyddsbehov samt information som omfattas av sekretess.
//Leverantörens personal som deltar i Uppdraget ska ha kompetens inom informationssäkerhet och sekretess. Leverantörens personal ska delta i de utbildningar som Beställaren bestämmer, vilket inkluderar eventuella repetitionsutbildningar.

Om Leverantören har egna utbildningar ska Beställaren göra en bedömning om dessa kan ersätta de av Beställaren erbjudna utbildningar. Leverantören ska, om egen godkänd utbildning genomförs, föra logg på vilka personer som gått utbildningarna och när detta skett och kunna redovisa detta för Beställaren vid begäran.

Om särskilda krav på kompetens ställs i upphandlingen så som certifiering, intyg, viss utbildning, viss erfarenhet eller annat motsvarande som har betydelse för informationssäkerheten ska verifikat kunna uppvisas för Beställaren att dessa särskilda krav uppfylls.

Beställaren ska innan Uppdraget påbörjas säkerställa att de personer hos Leverantören som kan komma att få tillträde till Beställarens information har tillräcklig kompetens i informationssäkerhetsfrågor.//

Incidentrapportering

Med incident avses händelse som undergräver tillgängligheten, riktigheten, konfidentialiteten eller autenticiteten för information inom Uppdraget eller i övrigt funktionalitet hos Uppdragets resultat.

Leverantören ska vid inträffad incident eller misstänkt inträffad informationssäkerhetsincident där Beställarens information omfattas utan onödigt dröjsmål informera Beställaren om det inträffade med information om

- vad som hänt,
- vilken information som omfattas,
- status samt vidtagna och
- pågående åtgärder.

Leverantören ska rapportera status under arbetets gång samt medverka vid Beställarens rapporteringsskyldighet till externa myndigheter.

Informationen ska lämnas till den av Beställaren utpekade kontakten och Leverantören ska informera om vem Beställaren har som kontaktperson hos Leverantören i ärendet. Beställaren ska rådfrågas vid val av åtgärder som påverkar Beställarens information.

Incidentrapportering i enlighet med NIS-direktivet[1]

Detta krav gäller om tjänsten omfattas av NIS-direktivet.

//Med incidenter avses störningar vilka får betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten.

Leverantören ska vid inträffad incident eller misstänkt inträffad incident där Beställarens information omfattas, utan onödigt dröjsmål informera Beställaren om det inträffade.

Leverantören ska hålla Beställaren informerad om status på arbetet och förse Beställaren med den information som Beställaren behöver för att uppfylla rapporteringskraven enligt vid var tid gällande författning.

Initial rapport (första skedet)

Initial rapport ska lämnas utan dröjsmål till Beställarens kontaktperson. Rapporten ska innehålla en beskrivning av inträffad incident, utifrån

a. tidpunkt för när incidenten inträffade och när den upptäcktes,

[1] *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*

b. om incidenten eller störningen är pågående, avslutad eller om det är okänt,
c. vilka tjänster som är påverkade och som berör Trafikverket
d. bedömning om hur länge störningen/incidenten kommer pågå
e. beskrivning av incidenten och dess hantering
f. kontaktperson hos Leverantören i aktuell störning/incident.

Rapport i andra skedet

Andra skedets rapport ska ha inkommit till Beställarens kontaktperson inom 24 timmar efter att första skedets rapport lämnats. Rapporten ska innehålla

a. i vad störningen/incidenten inträffat
b. händelseförlopp om mer information framkommit från rapportering i första skedet,
c. beskriva vidtagna och planerade åtgärder

Leverantören ska rapportera status under arbetets gång samt medverka vid Beställarens slutliga rapporteringsskyldighet (rapport i tredje skedet).

Beställaren ska konsulteras vid val av åtgärder som påverkar Beställarens informationstillgångar.

Rapporter skickas till Beställarens utsedda kontaktperson. Vid kommunikation av information som omfattas av sekretess ska kommunikationssätt som hindrar obehörig åtkomst användas eller på annat sätt som överenskoms med Beställaren.//

Misstänkta eller konstaterade sårbarheter

Leverantören ska utan dröjsmål informera Beställaren om misstänkta eller konstaterade sårbarheter i det tekniska och administrativa skyddsåtgärderna som innebär eller kan innebära att Beställarens information riskeras genom att kraven på konfidentialitet, riktighet eller tillgänglighet påverkas negativt.

Information om misstänkta eller konstaterade sårbarheter ska ske till Beställarens utsedda kontaktperson.

Kontroll av efterlevnad

Detta krav gäller vid behandling av information med skyddsbehov.
//Beställaren har rätt att kontrollera att de i Beställarens krav redovisade och avtalade informationssäkerhetskraven följs under den tid Leverantören

behandlar Beställarens informationstillgångar. Det gäller också efter avslutat uppdrag.

Kontroll kan ske genom egenkontroller där Leverantören ombeds svara på frågor avseende efterlevnad av krav. Revision kan också ske genom att Beställaren besöker Leverantören vid Leverantörens verksamhetsställen. Leverantören ska medverka vid Beställarens kontroll.

Beställaren har rätt att genomföra kontrollen via tredje part som då utför kontrollen på Beställarens uppdrag.

Alla kontroller och revisioner som kan göras av leverantörer ska också gälla underleverantörer oavsett led. Leverantören garanterar att underleverantörerna tillåter detta.//

Åtgärder avseende informationstillgångar vid avtalets upphörande eller byte till annan Leverantör

Detta krav gäller vid behandling av information med skyddsbehov.
//Vid upphörande av hela eller delar av avtalet, oavsett orsak, ska Leverantören vara behjälplig i samband med avvecklingen av informationstillgångar och vid byte till annan leverantör. Detta innefattar exempelvis besvarande av förfrågningar, teknisk assistans och överlämning av all information som producerats inom ramen för Uppdraget. Leverantörens åtaganden enligt detta avsnitt gäller under en tid om högst sex månader från avtalets upphörande oavsett orsak.

Leverantör ska tillse att aktiviteter i samband med avveckling utförs inom av Beställaren angivna skäliga tidsramar. En detaljerad plan upprättas inför avvecklingen om Beställaren begär det. Under avveckling ska Leverantör på Beställarens begäran samarbeta med ny leverantör till Beställaren. Avvecklingen ska ske på ett sätt som underlättar överlämnande av pågående eller avslutad leverans till Beställaren eller tredje part utan oskälig kostnad eller störning för Beställaren.

Leverantör ska under överlämnandefasen bidra med sin kompetens till Beställaren och/eller tredje part. Leverantör ska under överlämnandefasen säkerställa att nyckelpersoner är tillgängliga för medverkan i överlämnandet i den omfattning som efterfrågas, dock med efter omständigheterna skälig framförhållning. Med nyckelpersoner avses personer som är viktiga för överlämnandet på grund av att personen har speciell kompetens eller har haft

en speciell roll. Nyckelpersoner ska vara tillgängliga under hela den tid som anges i första stycket.//