

BILAGA – IT-SÄKERHETSAVTAL

DNR: GAN-2024/16



BILAGA – IT-säkerhetsavtal

Till mellan Beställaren och Leverantören ingånget Avtal om IT-produkter och/eller IT-tjänster bifogas härmed följande Bilaga IT-säkerhetsavtal. Bilagan innehåller de särskilda krav på säkerhet och säkerhetsåtgärder som ska gälla för Leverantörens tillträde till lokaler, anläggningar och andra utrymmen som Beställaren äger eller annars disponerar, samt för tillgång till Beställaren tillhöriga informationssystem och information som Beställaren behandlar.

INNEHÅLL

1. Bakgrund och syfte
2. Särskilda definitioner
3. Tillträde till IT-system
4. Beställarens särskilda säkerhetsföreskrifter
5. Incidenthantering och incidentutredning
6. Loggning och rapportering till Beställare
7. Systemadministration
8. Säkerhetsrevision
9. Internutbildning
10. Särskilda krav på Leverantörens säkerhetsrutiner
11. Övriga Tekniska och organisatoriska säkerhetsåtgärder
12. Återställning och säkerhetskopiering
13. Ersättning för kostnader till följd av säkerhetskrav
14. Säkerhets- och sekretessförbindelse

1. BAKGRUND OCH SYFTE

1.1 Beställarens verksamhet ställer särskilda krav på säkerhet. Särskilda säkerhetsåtgärder måste t.ex. vidtas för att skydda sådan information som behandlas i verksamheten och som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (offentlighets- och sekretesslagen), eller krav på skydd av personuppgifter enligt personuppgiftslagen (1998:204) (personuppgiftslagen) och dataskyddsförordningen (EU 2016/679) eller vid var tid gällande lag.

1.2 För Beställaren är det nödvändigt att tillse att denne tillhörig information ej obehörigen röjs, ändras, görs otillgänglig för behöriga eller förstörs. Syftet med IT-säkerhetsavtalet är att tillse att Avtalet fullgörs på ett sätt som tillgodoser Beställarens behov av informationssäkerhet. De tekniska och organisatoriska säkerhetsåtgärder som Leverantören genom undertecknande av denna bilaga åtar sig att fullgöra ska säkerställa upprätthållande av konfidentialitet, tillgänglighet, riktighet och spårbarhet med avseende på Beställarens information.

1.3 Beställarens information ska skyddas från oavsiktlig eller otillåten förlust, förstörelse, ändring och tillgängliggörande för obehöriga.

2. SÄRSKILDA DEFINITIONER

2.1 Nedanstående begrepp som förekommer i IT-säkerhetsavtalet ska ha nedan angiven innebörd.

Med "Avtalet" avses det kommersiella avtal som ingås mellan Beställaren och Leverantören.

Med "IT-säkerhetsavtalet" avses detta avtal.

Med "Uppdraget" avses det uppdrag eller den tjänst som Leverantören ska utföra enligt Avtalet.

Med "Beställarens information" avses den information som Leverantören erhåller och hanterar under Avtalet samt IT-säkerhetsavtal.

Med "Tekniska och organisatoriska säkerhetsåtgärder" avses åtgärder avsedda att skydda Beställarens information mot oavsiktlig eller olaglig utplåning, oavsiktlig förlust, ändring, otillåten utlämnande eller otillåten åtkomst.

Med "Incident" avses ett oplanerat avbrott i en IT-tjänst eller reduktion av kvaliteten hos en IT-tjänst eller funktionalitet.

Med "Incidenthantering" avses åtgärd för att säkerställa att normal leverans av en IT-tjänst återställs så snabbt som möjligt och påverkan på verksamheten minimeras.

Med "Incidentutredning" avses åtgärder som Parterna vidtar, var för sig eller gemensamt, för att klargöra orsaker till och ansvaret för en inträffad Incident.

3. TILLTRÄDE TILL IT-SYSTEM

3.1

Behörighetskontroll ska utföras avseende användare av Leverantörens IT-system som används för genomförande av Uppdraget. Behöriga användare ska vara individuellt identifierbara. Användaridentitet ska vara personlig och får ej överlåtas på någon annan. Leverantören ska säkerställa att endast personal anställd hos denne som är behörig att utföra Uppdraget ges tillträde till IT-system enligt denna bestämmelse. Följande Tekniska och organisatoriska säkerhetsåtgärder ska användas:

- Tillträde för behöriga användare kontrolleras genom att behöriga användare har ett personligt aktivt ID-kort eller säkerhetsdosa för att logga in.
- Det ska finnas rutiner för tilldelande och upphörande av användarunik ID.
- Kommunikation vid inloggningsförfarandet ska vara krypterad med för ändamålet adekvat säkerhetsnivå.
- Tillträdesbegränsning ska säkerställas genom att lokaler med IT som används för genomförande av Uppdraget låses.
- Förbindelsen ska vara krypterad med VPN-teknik.
- System för intrångsdetektering.
- Antivirusslösningar och annat skydd mot skadlig kod.
- Brandväggar som skyddar IT-systemen från externa angrepp.

4. BESTÄLLARENS SÄRSKILDA SÄKERHETSFÖRESKRIFTER

4.1

Leverantören ska följa vid var tid gällande säkerhetsföreskrifter som Beställaren meddelat angående hantering av Beställarens information, t.ex. informationssäkerhetspolicy, personuppgiftspolicy och liknande.

4.2

Beställaren ska tillse att Leverantören får tillgång till sådana säkerhetsföreskrifter som avses i punkt 4.1 i god tid innan dessa får göras gällande mot Leverantören.

5. INCIDENTHANTERING OCH INCIDENTUTREDNING

5.1

Leverantören ska ha för Avtalet lämpliga, och av Beställaren godkända, rutiner för att genomföra, rapportera och följa upp Incidentutredningar. Incidenter hänförliga till Beställarens information ska inom 48 timmar efter det att Leverantören har upptäckt incidenten rapporteras till Beställaren. Rapporten ska innehålla redogörelse för vad som har hänt och vilka åtgärder Leverantören vidtagit med anledning av Incidenten.

5.2

Behörighet hos Leverantören att utföra Incidentutredningar enligt detta avtal ska vara begränsat till ett fåtal personer. På Beställarens begäran ska Leverantören meddela vilka dessa behöriga personer är.

5.3

Incident- och Patchhantering ska, om Parterna inte överenskommit om annat motsvara ITIL:s rekommendationer. Beställaren ska godkänna Leverantörens Incidenthantering.

6. LOGGNING OCH RAPPORTERING TILL BESTÄLLAREN

6.1

Aktiviteter i Leverantörens IT-system som används för genomförande av uppdraget ska gå att spåra via loggar för Leverantörens behandling av Beställarens information.

6.2

Loggar ska uppfylla krav på spårbarhet avseende tidpunkt för åtgärder jämte användarens identitet. Av loggar ska framgå avvikelser från normal drift och administration, såsom systemfel, ogiltiga inloggningsförsök och försök till obehörig åtkomst, viktiga systemhändelser såsom uppgraderingar, registergallring och funktionsförändringar. Loggar ska finnas för behörighetsförändringar, start och stopp av systemet, resultat av batchar och integrationer, transaktionsloggar samt alla ändringar avseende vad som har tillförts och ändrats i Beställarens information. Av loggarna ska även framgå information om användaridentitet, datum och tidpunkt för inloggning och utloggning samt andra användaraktiviteter som är av betydelse för säkerheten i systemet. Loggarna ska vara skyddade mot obehörig insyn och förändring.

6.3

Leverantören ska på Beställarens begäran tillhandahålla kundunika loggar, varmed förstås loggar som angår en viss fysisk eller juridisk person, eller en viss identifierbar användare avseende användningen av Beställarens system.

6.4

Leverantören ska om Beställaren begär det i skälig omfattning lämna Beställaren rapporter avseende Beställarens information. Dessa ska utvisa återkommande misslyckade inloggningar och intrångsförsök riktade mot specifika applikationer, användarkonton eller särskilt lagringsutrymme. Rapporterna ska om möjligt visa fördelningen på interna respektive externa attacker.

7. SYSTEMADMINISTRATION

7.1

Leverantörens systemadministration IT-system som används för genomförande av uppdraget ska kunna behörighetsstyra vilka systemadministrationsfunktioner som ska gå att använda, samt vilka organisationsenheter och enskilda användare som ska kunna använda funktionerna. En systemadministratör ska inte själv kunna utöka sina egna behörigheter eller rättigheter. Leverantören ska på Beställarens begäran lämna information till Beställaren om vilka anställda eller andra anlitade hos Leverantören som har administratörsbehörighet.

7.2

Systemadministrativa behörigheter hos Leverantören ska inte innefatta rätt ändra Beställarens information utan Beställarens skriftliga medgivande därtill.

8. SÄKERHETSREVISION

8.1

Leverantören medger att revision avseende säkerheten vid Leverantörens behandling av Beställarens information (Säkerhetsrevision) får ske av Beställaren eller av Beställaren utsedd och anvisad extern part. Sådan revision får även omfatta behörighetsadministration, säkerhetsrutiner, loggar och spårbarhet för behandlingen av Beställarens data.

8.2

Leverantören ska inte ha rätt till någon ersättning för eventuella kostnader som uppstår för denne i anledning av Säkerhetsrevision såvida inte annat överenskommits skriftligen.

9. INTERNUTBILDNING

9.1

Innan Uppdraget påbörjas kan Beställaren komma att utbilda de personer hos Leverantören som är behöriga att utföra Uppdraget. Anställda eller andra som anlitats av Leverantören för att utföra Uppdraget ska fortlöpande utbildas i för ändamålet adekvat och skälig omfattning.

10. SÄRSKILDA KRAV PÅ LEVERANTÖRENS INFORMATIONSSÄKERHETSROUTINER

10.1

Om inte annat anges i Avtalet eller särskilt överenskommits skriftligen mellan Parterna gäller följande särskilda krav på Leverantörens säkerhetsrutiner.

10.2

Leverantören ska ha säkerhetsrutiner som motsvaras av de krav som ställs i ISO/IEC, serierna 27000 och 31000. Ändringar av Leverantörens säkerhetsföreskrifter ska skriftligen meddelas Beställaren.

11. ÖVRIGA TEKNISKA OCH ORGANISATORISKA SÄKERHETSÅTGÄRDER

11.1

Leverantören ska säkerställa att erforderligt skydd mot skadlig kod upprätthålls. Det ska ske genom att ny information kontrolleras innan den tillförs IT-system som används för Uppdragets genomförande i syfte att säkerställa att information innehållande skadlig kod ej tillförs. Programvara som skyddar mot skadlig kod ska uppdateras kontinuerligt enligt Leverantörens riktlinjer för skydd mot skadlig kod.

11.2

IT-system som används för genomförande av Uppdraget ska ha skydd mot intrång och möjliggöra intrångsdetektering. Leverantörens riktlinjer för intrångsdetektering och skydd mot intrång ska dokumenteras av Leverantören.

11.3

Leverantören ska säkerställa att IT-system som används för genomförande av Uppdraget ej ligger nere och är ur funktion i sådan omfattning att det stör genomförandet av Uppdraget. I syfte att hindra att IT-störningar påverkar genomförandet av Uppdraget ska Leverantören bedöma den tid som IT-systemet kan ligga nere eller annars vara ur funktion utan att det stör genomförandet av Uppdraget. Leverantören utser en reservrutin som kan användas om dess IT-system är ur funktion och det stör Uppdragets genomförande i väsentlig omfattning. Leverantören ska dokumentera vilken reservrutin som ska användas för det fall IT-systemet ligger nere i sådan omfattning att det stör genomförandet av Uppdraget.

12. ÅTERSTÄLLNING OCH SÄKERHETSKOPIERING

12.1

Om inte annat anges i Avtalet eller särskilt överenskommits mellan Parterna gäller följande krav avseende återställning och säkerhetskopiering.

12.2

Leverantören ska ha rutiner för säkerhetskopiering. Rutinerna för säkerhetskopiering ska säkerställa att Beställarens information kan återskapas i händelse av en störning. Säkerhetskopior ska bevaras i godkänt säkerhetsskåp. Säkerhetskopior ska testas regelbundet och de bör krypteras. Förebyggande åtgärder ska genomföras samband med åtgärder i IT-system som används för genomförande av uppdraget.

13. ERSÄTTNING FÖR KOSTNADER TILL FÖLJD AV SÄKERHETSKRAV

13.1

Om inte annat anges i Avtalet, detta avtal eller särskilt överenskommits skriftligen mellan Parterna har Leverantören ingen rätt till ersättning för de kostnader som uppstår till följd av åtgärder som genomförs enligt denna bilaga.

14. SEKRETESSFÖRBINDELSE

14.1

På Beställarens begäran ska Leverantören, av denne anställd eller anlitad personal underteckna av Beställaren anvisad sekretessförbindelse.

14.2

Sekretessförbindelsen syftar till att säkerställa att Leverantören, av denne anställd eller anlitad personal, eller av denne anlitad underleverantör informerats om och tagit del av de sekretessbestämmelser som ska gälla med anledning av Uppdraget. Undertecknande av sådan handling ska inte uppfattas som att Leverantörens ansvar i något avseende övergår till fysisk person som Leverantören anlitar.

14.3

Information som omfattas av sekretess och som Leverantören har hanterat eller bevarat vid genomförande av Uppdraget omfattas av tystnadsplikt. Tystnadsplikten gäller även efter att Avtalet har upphört. Leverantören ska säkerställa att av denne anställd eller anlitad personal eller av denne anlitad Underleverantör informeras om innebörden av sekretessen och tillse att sekretessförbindelser undertecknas av alla berörda personer. Sekretessförbindelserna ska vid avtalets upphörande överlämnas till Beställaren.