SKL Kommentus Inköpscentral

Bilaga 05 – Villkor för informationssäkerhet Trygghetslarm och larmmottagning 2019

	Villkor
1	Leverantören ska för de delar av verksamheten som berörs i leveransen ha ett ledningssystem för informationssäkerhet (LIS) som baseras på SS-EN ISO/IEC27001:2017 eller motsvarande. Ledningssystemet ska omfatta bland annat att samtliga säkerhetskritiska administrativa och tekniska processer är dokumenterade och vilar på en formell grund där roller, ansvar och befogenheter finns tydligt definierade.
2	Leverantören ska ha tillsett att ansvar och arbetsuppgifter som står i konflikt med varandra och kan leda till missbruk är tekniskt eller organisatoriskt åtskilda.
3	Leverantören ska ha en policy som beskriver hur de anställda får arbeta på distans avseende drift, förvaltning och support av de levererade tjänsterna. Leverantören ska regelbundet kontrollera att den efterlevs.
4	Leverantören ska ha avtal om tystnadsplikt med sina anställda. Tystnadsplikten ska omfatta information om leverantörens kunder. Via avtal ska leverantören även säkerställa tystnadsplikt för underleverantörer.
5	Leverantören ska för sin personal regelbundet genomföra utbildningar för ökad medvetenhet kring informationssäkerhet samt hålla sig uppdaterad kring den upphandlande myndighetens policys, regler och rutiner.
6	Leverantören ska ha rutiner och funktioner för att permanent radera information som är relaterade till leveransen. Leverantören ska på begäran kunna uppvisa underlag på att så skett.
7	Leverantören ska genomföra regelbundna riskbedömningar för system som används för utförandet av uppdraget, dock minst årligen. Identifierade brister ska åtgärdas omgående och redovisas för den upphandlande myndigheten.
8	Det ska finns en dokumenterad och formell process för hur användaridentiteter hanteras. De digitala identiteterna ska vara personliga och unika över tid.
9	Leverantören ska följa en överenskommen rutin som möjliggör för den upphandlande myndigheten att godkänna hantering (skapande, borttag, ändring) av utpekade behörighetsroller t ex avseende priviligierade (högre) behörigheter. Hanteringen ska vara spårbar och redovisas för den upphandlande myndigheten enligt överenskommelse, dock minst årligen.
10	Leverantören ska använda särskilda personliga användaridentiteter för systemadministration. Dessa konton ska vara spårbara och lätta att skilja från vanliga användare. Den upphandlande myndigheten ska informeras om vilka som innehar dessa behörigheter och när behörigheter ändras.
11	Leverantören ska tillhandahålla ett sätt att distribuera och återställa lösenord utan att lösenordet kan röjas till obehöriga. Behörighetsinformation som t.ex. lösenord får ej lagras i klartext (gäller även systemkonton i källkod). Motsvarande krav gäller även för temporära filer som skapas i användarens arbetsstation när system som används för utförandet av uppdraget brukas.
12	Behörighetssystem ska logga information om när användare skapades, togs bort eller förändrades samt senaste inloggning.
13	Leverantören ska ha en rutin för att både avaktivera användarkonton och permanent ta bort konton från system som används för utförandet av uppdraget.
14	Leverantörens behörigheter ska tilldelas enligt principen där minsta möjliga behörighet tilldelas utifrån användares roll och arbetsuppgifter. Detta gäller även konton som används vid kommunikation mellan systemkomponenter, exempelvis mellan applikation och databas samt priviligierade konton. Leverantören ska på begäran av upphandlande myndighet tillhandahålla rutinerna.
15	Inloggningen ska vara flerfaktorsbaserad i enlighet med kraven som följer av ELN0700. Endast utfärdare godkända av E-legitimationsnämnden (minst nivå 3) eller anslutna inom eIDAS (minst nivå substantial) rekommenderas.
16	System som används för utförandet av uppdraget ska ha funktioner för att kunna kravställa aktiveringsdatat (pinkod, lösenord etc) vad gäller komplexitet, längd och livslängd.
17	Leverantören ska skydda och tillse att det finns spårbarhet i de program som används för underhåll av system som används för utförandet av uppdraget, dess säkerhetskonfiguration och information.

18	Leverantören ska ha rutiner för kryptering där val av algoritmer, protokoll och nyckellängder samt hantering av krypteringsnycklar framgår.
19	Datahallen ska ha ett fysiskt skydd. Skyddet ska uppfylla kraven i tillämpliga nationella eller internationella standarder.
20	Leverantören ska ha rutiner avseende förändringshantering för de delar som kan påverka leveransens säkerhet och tillgänglighet. Dessa ska följas upp minst årligen och redovisas för den upphandlande myndigheten.
21	Leverantören ska ha funktioner, processer och rutiner för att övervaka kapacitet och prestanda i it-system som krävs för att utföra uppdraget.
22	Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i den upphandlande myndighetens tjänst. Testdata ska skyddas och kontrolleras och får inte innehålla information som är känslig eller omfattas av sekretess.
23	Leverantören ska ha ett skydd mot skadlig kod som uppdateras kontinuerligt för de delar som ingår i leveransen.
24	Leverantören ska ha rutiner och funktioner för säkerhetskopiering och återställande av information enligt överenskomna tillgänglighetskrav med den upphandlande myndigheten. Säkerhetskopior ska skyddas på motsvarande sätt som originalinformationen samt förvaras åtskilt.
25	Loggningsfunktioner ska finnas för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter. Tiden som logginformation sparas ska kunna bestämmas av den upphandlande myndigheten som också ska kunna genomföra granskning av användarrelaterade loggar.
26	Leverantören ska skydda loggningsfunktioner och loggningsverktyg mot manipulation och obehörig åtkomst som även omfattar leverantörens personal.
27	System som används för utförandet av uppdraget och relaterad infrastruktur ska använda tidssynkronisering mot samma tidskälla (GPS eller svenska UTC (SP)).
28	Leverantören ska verifiera och begränsa den mjukvara som får exekveras (göra en körning av ett dataprogram) inom de levererade tjänsterna som används för utförandet av uppdraget
29	Leverantören ska utan dröjsmål informera den upphandlande myndigheten om tekniska sårbarheter i levererade komponenter. Upptäckta sårbarheter ska åtgärdas omgående.
30	All kommunikation till och från system som används för utförande av uppdraget ska vara skyddad mot obehörig åtkomst eller förvanskning. Det gäller både kommunikation mellan klient och server och mellan olika systemkomponenter. Skyddet ska uppdateras löpande utifrån kända sårbarheter.
31	Leverantören ska tillhandahålla en (logisk eller fysiskt) separerad kundmiljö inklusive behörighetskontrollsystem, loggar och lagring för varje upphandlande myndighet.
32	Leverantören ska ha genomfört säkerhetsåtgärder mot obehörig åtkomst samt obehörig ändring av information som utbyts mellan system och som används för utförandet av uppdraget.
33	Leverantören ska ha riktlinjer för informationssäkerhet inom sina utvecklingsprocesser. Vid större ändringar ska leverantören identifiera och hantera risker som säkerställer att säkerhetskraven i system som används för utförandet av uppdraget är uppfyllda.
34	Leverantören ska ha dokumenterade rutiner för övervakning, upptäckt, analys, rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter.
35	Leverantören ska tillsammans med den upphandlande myndigheten samverka i hanteringen av sårbarheter, säkerhetshändelser eller säkerhetsincidenter. Den upphandlande myndigheten ska informera leverantören om vem som är kontaktperson för samverkan.
36	Leverantören ska på begäran vara delaktig i den upphandlande myndighetens övningar i krishantering minst en halv dag/år.
37	Den upphandlande myndigheten ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.