KLASSA - Upphandlingskrav för system för social dokumentation inom socialtjänstlagen

Namn: Säkerhetskrav | System: Dokumentationssystem | Senast ändrad: 2022-01-31 14:45

Säkerhetsnivåer: Konfidentialitet - Nivå 3, Riktighet - Nivå 1, Tillgänglighet - Nivå 1

#	Krav	ISO kapitel	ISO kravområde
5003	Leverantören ska ha dokumenterade rutiner för distansarbete. Informationsbehandlingen ska vara lika säker på distans som den är vid behandling på leverantörens arbetsplats.	A.6.2 Mobila enheter och distansarbete	A.6.2.2 Distansarbete
5004	Leverantören ska ha processer och rutiner på plats för relevant bakgrundskontroll av personal.	A.7.1 Före anställning	A.7.1.1 Bakgrundskontroll
5005	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. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag.	A.7.1 Före anställning	A.7.1.2 Anställningsvillkor
5006	Leverantören ska för sin personal varje halvår genomföra utbildningar för ökad medvetenhet kring informationssäkerhet samt hålla sig uppdaterad kring beställarens policys, regler och rutiner.	A.7.2 Under anställning	A.7.2.2 Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet
5007	Leverantören ska ha en tydlig och disciplinär process med åtgärder för anställda som har brutit mot informationssäkerhetsregler.	A.7.2 Under anställning	A.7.2.3 Disciplinär process
5008	Leverantören ska till personalen ha kommunicerat de ansvar och skyldigheter som förblir gällande efter ändring eller avslut av anställning. Personalen ska ha skrivit under en ansvarsförbindelse avseende detta.	A.7.3 Avslut eller ändring av anställning	A.7.3.1 Avslut eller ändring av anställds ansvar
5009	Leverantören ska ha dokumenterade regler, rutiner och roller som beskriver tillåten användning av de resurser (t.ex. arbetsdatorer, bärbara datorer eller mobila enheter). som ingår i leveransen. Leverantören ska årligen kontrollera att de efterlevs.	A.8.1 Ansvar för tillgångar	A.8.1.3 Tillåten användning av tillgångar
5010	Leverantören ska ha rutiner och funktioner för att återlämna beställarens fysiska och elektroniska tillgångar då anställning, uppdrag eller avtal upphör. Leverantören ska på begäran kunna uppvisa underlag på att så skett.	A.8.1 Ansvar för tillgångar	A.8.1.4 Återlämnande av tillgångar
5011	Leverantören ska följa beställarens rutiner och processer för informationsklassning samt tillämpa relevanta säkerhetsåtgärder.	A.8.2 Informationsklassning	A.8.2.1 Klassning av information
5012	Beställarens krav på informationshanteringen ska efterföljas i relation till beställarens informationsklassning. Om sådana krav inte ställts ska leverantören utan anmodan kunna uppvisa de rutiner som gäller hos leverantören för hantering av beställarens tillgångar.	A.8.2 Informationsklassning	A.8.2.3 Hantering av tillgångar

5013	Leverantören ska ha en formell och dokumenteras process för hur användaridentiteter hanteras (registrering och avregistrering). Leverantören ska säkerställa att användaridentiteterna hos leverantör och beställare är personliga och unika över tid. Se tillitsramverket (ELN0700) tillitsnivå 3 (LoA3) för detaljer.	A.9.2 Hantering av användaråtkomst	A.9.2.1 Registrering och avregistrering av användare
5014	Leverantören ska följa en överenskommelse för användaråtkomst till beställarens system, tjänster och information. Endast behöriga och enligt överenskommelsen godkända individer ska inneha åtkomst. Hanteringen ska vara spårbar och redovisas för beställaren enligt överenskommelse, minst årligen.	A.9.2 Hantering av användaråtkomst	A.9.2.2 Tilldelning av användaråtkomst
5015	Leverantören ska använda särskilda personliga användaridentiteter för systemadministration. Dessa konton ska vara spårbara och lätta att skilja från vanliga användare. Leverantören ska ha särskilda säkerhetsåtgärder kopplade till systemadministration. (Exempelvis tidsbegränsade behörigheter eller striktare autentisering)	A.9.2 Hantering av användaråtkomst	A.9.2.3 Hantering av privilegierade åtkomsträttigheter
5016	Leverantören ska på ett säkert sätt distribuera, lagra och återställa autentiseringsinformation (exempelvis lösenord) utan att det kan röjas till obehöriga. Autentiseringsinformation får ej lagras i klartext (gäller även systemkonton i källkod). Se vägledning för tillitsnivå 3 (LoA3) för detaljer.	A.9.2 Hantering av användaråtkomst	A.9.2.4 Hantering av användares konfidentiella autentiseringsinformation
5017	Leverantören ska granska sina användares åtkomsträttigheter halvårsvis, Obehöriga eller användare som inte längre behöver åtkomst ska tas bort. Förändringar av åtkomsträttigheter ska dokumenteras av Leverantören och ska vid begäran tilldelas till beställaren.	A.9.2 Hantering av användaråtkomst	A.9.2.5 Granskning av användares åtkomsträttigheter
5018	Leverantören ska ha en rutin för att permanent ta bort användaridentiteter från information, tjänster och system, vid avslutande av anställning, avtal eller uppdrag. Kontroll av efterlevnad ska ske årligen.	A.9.2 Hantering av användaråtkomst	A.9.2.6 Borttagning eller justering av åtkomsträttigheter
5019	Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation ska skyddas och hanteras.	A.9.3 Användaransvar	A.9.3.1 Användning av konfidentiell autentiseringsinformation
5020	Leverantören ska ha systemfunktioner för att begränsa åtkomst till information. Behörigheterna ska tilldelas enligt principen där minsta möjliga behörighet tilldelas utifrån en användares roll och arbetsuppgifter. Detta gäller även konton som används vid kommunikation mellan systemkomponenter samt priviligierade konton. Endast information eller tjänster som ska vara publika ska kunna nås i system utan godkänd autentisering.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.1 Begränsning av åtkomst till information

	Leverantören ska tillse att autentiseringen till beställarens information, tjänster och system ska vara flerfaktorsbaserad i enlighet med kraven som följer av ELN0700.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.2 Säkra inloggningsrutiner
5021	Endast utfärdare godkända av E-legitimationsnämnden (minst nivå 3) eller anslutna inom eIDAS (minst nivå substantiell) rekommenderas. Se vägledning för tillitsnivå 3 (LoA3) för detaljer.		
5022	Leverantören ska tillse att information, tjänster och system har funktioner för att kunna kravställa autentiseringsinformation (pinkod, lösenord etc.) vad gäller komplexitet, längd och livslängd. Se vägledning för tillitsnivå 3 (LoA3) för detaljer.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.3 System för lösenordshantering
5023	Leverantören ska skydda och tillse att det finns spårbarhet i de verktyg som avses för underhåll och säkerhetskonfiguration för information, tjänster och system.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.4 Användning av privilegierade verktygsprogram
5024	Leverantören ska tillse att källkod framtagen i egen utveckling skyddas från obehöriga förändringar. Källkod ska deponeras på ett sådant sätt att beställaren garanteras tillgång om leverantören inte uppfyller sina avtalade förpliktelser.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.5 Åtkomstkontroll till källkod för program
5025	Leverantören ska ha rutiner för kryptering där val av algoritmer, protokoll och nyckellängder samt hantering av krypteringsnycklar framgår.	A.10.1 Kryptografiska säkerhetsåtgärder	A.10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder
5026	Leverantören ska tillse att fysiska avgränsningar är definierade och tillämpade för skydd av områden med känslig eller kritisk information. Om det avser en datahall eller motsvarande ska leverantören tillse att den uppfyller minst skyddsnivå 3 ("datahall" enligt MSB "Vägledning för fysisk informationssäkerhet i it-utrymmen") eller likvärdigt.	A.11.1 Säkra områden	A.11.1.1 Fysiska säkerhetsavgränsningar
5027	Leverantören ska ha rutiner som säkerställer att endast behörig personal har fysisk åtkomst till områden med konfidentiell information, exempelvis en datahall.	A.11.1 Säkra områden	A.11.1.2 Fysiska tillträdesbegränsningar

5028	Leverantören ska dokumentera ansvar för driftsrutiner och göra de tillgängliga för användare som behöver dem.	A.12.1 Driftsrutiner och ansvar	A. 12.1.1 Dokumenterade driftsrutiner
5029	Leverantören ska ha rutiner för att planera, genomföra och dokumentera alla förändringar som påverkar leveransens säkerhet. Större förändringar ska följas upp, kontrolleras och redovisas minst årligen för beställaren.	A.12.1 Driftsrutiner och ansvar	A.12.1.2 Ändringshantering
5030	Leverantören ska ha funktioner, processer och rutiner för att övervaka och göra prognoser avseende framtida krav på systemprestanda.	A.12.1 Driftsrutiner och ansvar	A.12.1.3 Kapacitetshantering
5032	Leverantören ska skydda mot skadlig kod. Det genom att ha säkerhetsåtgärder som inbegriper följande områden: förebygga, upptäcka, hantera och återställa Säkerhetsåtgärderna ska ses över minst årligen.	A.12.2 Skydd mot skadlig kod	A.12.2.1 Säkerhetsåtgärder mot skadlig kod
5033	Leverantören ska ha rutiner och funktioner för säkerhetskopiering och återställande av information enligt överenskomna tillgänglighetskrav med beställaren. Säkerhetskopior ska skyddas på motsvarande sätt som originalinformationen samt förvaras på en separat plats.	A.12.3 Säkerhetskopiering	A.12.3.1 Säkerhetskopiering av information
5034	Leverantören ska tillse att information, tjänster och system har loggningsfunktioner för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter. Loggning ska ske i samråd med beställaren. Leverantören ska aktivt använda loggarna för att upptäcka och hantera incidenter. Beställaren ska kunna genomföra granskning av loggar vid behov.	A.12.4 Loggning och övervakning	A.12.4.1 Loggning av händelser
5035	Leverantören ska skydda loggningsfunktioner och loggningsverktyg mot manipulation och obehörig åtkomst som även omfattar leverantörens personal.	A.12.4 Loggning och övervakning	A.12.4.2 Skydd av logginformation
5036	Leverantören ska tillse att information, tjänster och system, samt relaterad infrastruktur använder tidssynkronisering mot en och samma tidskälla(GPS eller svenska UTC (SP)).	A.12.4 Loggning och övervakning	A.12.4.4 Synkronisering av tid
5038	Leverantören ska bedriva ett kontinuerligt arbete för att identifiera sårbarheter och utan dröjsmål informera en utpekad funktion hos beställaren om de kan innebära ett hot för beställarens information, tjänster och system. Upptäckta sårbarheter ska åtgärdas omgående.	A.12.6 Hantering av tekniska sårbarheter	A.12.6.1 Hantering av tekniska sårbarheter

5039	Leverantören ska säkerställa att all kommunikation till och från system, tjänster eller information ska vara skyddad mot obehörig åtkomst eller förvanskning . Det avser kommunikation mellan klient och server och mellan olika systemkomponenter. Skyddet ska uppdateras löpande utifrån kända sårbarheter.	A.13.1 Hantering av nätverkssäkerhet	A.13.1.1 Säkerhetsåtgärder för nätverk
5040	Leverantören ska tillhandahålla en (logisk eller fysiskt) separerad kundmiljö inklusive behörighetskontrollsystem, loggar och lagring för varje kund.	A.13.1 Hantering av nätverkssäkerhet	A.13.1.3 Separation av nätverk
5041	Leverantören ska följa en överenskommelse med beställaren angående krav för informationsöverföring.	A.13.2 Informationsöverföring	A.13.2.1 Regler och rutiner för informationsöverföring
5042	Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra tjänster och system. Vid utveckling av webbapplikationer eller tillhandahållande av tjänster över publika nätverk ska OWASPs (www.owasp.org) rekommendationer följas.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.1 Analys och specifikation av informationssäkerhetskrav
5043	Leverantören ska ha infört säkerhetsåtgärder som skyddar information i programtjänster på publika nätverk mot obehörig åtkomst och obehörig ändring. Vid utveckling av mobila appar ska OWASP Mobile App Security Checklist följ	A.14.1 Säkerhetskrav på informationssystem	A.14.1.2 Säkerställande av programtjänster på publika nätverk
5044	Leverantören ska ha riktlinjer för systemförändringar som avser informationssäkerhet inom sina utvecklingsprocesser. Vid större ändringar ska leverantören identifiera och hantera risker som säkerställer att säkerhetskraven i system eller tjänster är uppfyllda.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.2 Rutiner för hantering av systemändringar
5045	Leverantören ska ha rutiner för att granska och testa tillgänglighet och säkerhet efter ändringar i verksamhetskritiska driftsplattformar.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö

5046	Leverantören ska ha riktlinjer och instruktioner om beställaren avser att göra egna förändringar i programpaket.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.4 Restriktioner för ändringar av programpaket
5047	Leverantören ska övervaka och styra systemutveckling som är utlagd till en underleverantör.	A.14.2 Säkerhet i utvecklings- och supportsprocesser	A.14.2.7 Outsourcad utveckling
5048	Leverantören ska följa beställarens rutiner och processer för åtkomst till organisationens tillgångar.	A.15.1 Informationssäkerhet i leverantörsrelationer	A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer
5049	Leverantören ska ha dokumenterade rutiner för övervakning, upptäckt, analys, rapportering, eskalering, hantering av säkerhetshändelser och säkerhetsincidenter. Om incidenten i någon mån påverkar beställaren så ska beställaren inkluderas i dessa rutiner.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.1 Ansvar och rutiner
5050	Leverantören ska bedöma och besluta ifall en informationssäkerhetshändelse ska klassas som en informationssäkerhetsinci dent. Om händelsen i någon mån påverkar beställaren så ska beställaren inkluderas i detta beslut.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.4 Bedömning av och beslut om informationssäkerhetshändelser

5051	Leverantören ska ha rutiner för att hantera säkerhetsincidenter enligt gällande lagar och förordningar. Om incidenten i någon mån påverkar beställaren så ska en överenskommen och utpekad funktion hos beställaren inkluderas i dessa rutiner. Rutinerna ska granskas årligen.	A.16.1 Hantering av informations säkerhetsinc identer och förbättringar	A.16.1.5 Hantering av informationssäkerhetsincidenter
5053	Leverantören ska löpande och i samråd med beställaren arbeta för att leveransen i alla lägen följer de aktuella lagar, förordningar, regler och föreskrifter som ställs på beställarens verksamhet.	A.18.1 Efterlevnad av juridiska och avtalsmässig a krav	A.18.1.1 Identifiering av tillämplig lagstiftning och avtalsmässiga krav
5054	Leverantören ska utveckla och införa regler för skydd av personuppgifter med stöd i lagar och förordningar. Dessa regler ska kommuniceras till medarbetare hos leverantören som berörs av leveransen som hanterar personuppgifter.	A.18.1 Efterlevnad av juridiska och avtalsmässig a krav	A.18.1.4 Skydd av personlig integritet och personuppgifter
5055	Beställaren ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.	A.18.2 Granskninga r av informations säkerhet	A.18.2.3 Granskning av teknisk efterlevnad
5056	Leverantören ska begära tillstånd innan information i system (texter, bilder etc.) eller tjänster återanvänds i andra sammanhang.	A.18.1 Efterlevnad av juridiska och avtalsmässig a krav	A. 18.1.2 Immateriella rättigheter