Utdrag från *Leveransavtal Webbkarta SOKIGO AB - signed* med upphandlingskrav och informationsklassning för kartproduktion, folkbokföring, webbkarta (extern och intern).

KLASSA - Upphandlingskrav

Informationsklassning 2020 kartproduktion

Säkerhetsnivåer: Konfidentialitet - Nivå 2, Riktighet - Nivå 2, Tillgänglighet - Nivå 1

#	Krav	ISO kapitel	ISO kravområde	Kon.	Rik.	Til.
3501	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.	A.6.1 Intern organisation	A.6.1.1 Informationssäkerhetsroller och ansvar	2	2	
3502	Leverantören ska ha tillsett att ansvar och arbetsuppgifter som står i konflikt med varandra och kan leda till missbruk är åtskilda.	A.6.1 Intern organisation	A.6.1.2 Uppdelning av arbetsuppgifter	2	2	
3503	Leverantören ska ha upprättat kontakter med de myndigheter som berörs av leveransen	A.6.1 Intern organisation	A.6.1.3 Kontakt med myndigheter	2	2	
3504	Leverantören ska ha en policy som beskriver hur de anställda får arbeta på distans avseende drift, förvaltning och support av de levererade tjänsterna.	A.6.2 Mobila enheter och distansarbete	A.6.2.2 Distansarbete	2	2	
3505	Leverantören ska ha processer och rutiner på plats för relevant bakgrundskontroll av personal.	A.7.1 Före anställning	A.7.1.1 Bakgrundskontroll	2	2	
3506	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.	A.7.1 Före anställning	A.7.1.2 Anställningsvillkor	2		
3507	Leverantören ska för sin personal regelbundet 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	2	2	
3508	Leverantören ska ha tydliga och kommunicerade åtgärder för överträdelse av informationssäkerhetsregler.	A.7.2 Under anställning	A.7.2.3 Disciplinär process	2	2	
3509	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	2	2	
3510	Leverantören ska ha dokumenterade regler, rutiner och roller som beskriver tillåten användning av de resurser som ingår i leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.3 Tillåten användning av tillgångar	2		
3511	Leverantören ska ha rutiner och funktioner för att permanent radera information som är relaterade till leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.4 Återlämnande av tillgångar	2		
3512	Leverantören ska under kontraktstiden, dock minst vart tredje år, ha genomfört en riskbedömning för systemet. Identifierade brister ska åtgärdas enligt en dokumenterad plan och kunna redovisas för beställaren.	A.8.2 Informationsklassning	A.8.2.1 Klassning av information	2	2	
3513	Beställarens krav på informationshanteringen ska efterföljas. Om sådana krav inte uttryckligen ställts ska leverantören utan anmodan kunna uppvisa de rutiner som gäller hos leverantören.	A.8.2 Informationsklassning	A.8.2.3 Hantering av tillgångar	2		
3514	digitala identiteterna ska vara personliga och unika över tid. Se vägledningen för tillitsnivå 2 (LoA2) för detaljer.	A.9.2 Hantering av användaråtkomst	A.9.2.1 Registrering och avregistrering av användare	2		

3515	Leverantören ska följa en överenskommen rutin som möjliggör för Beställaren att godkänna hantering (skapande, borttag, ändring) av utpekade behörighetsroller t ex avseende priviligierade (högre) behörigheter. Hanteringen ska vara spårbar.	A.9.2 Hantering av användaråtkomst	A.9.2.2 Tilldelning av användaråtkomst	2		
3516	Leverantören ska använda särskilda personliga användaridentiteter för priviligierade (högre) behörigheter som används för systemadministration. Dessa konton ska vara spårbara och lätta att skilja från vanliga användare.	A.9.2 Hantering av användaråtkomst	A.9.2.3 Hantering av privilegierade åtkomsträttigheter	2	2	
3517	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 systemet används.	A.9.2 Hantering av användaråtkomst	A.9.2.4 Hantering av användares konfidentiella autentiseringsinformation	2	2	
3518	Behörighetssystemet ska logga information om när användare skapades, togs bort eller förändrades samt senaste inloggning.	A.9.2 Hantering av användaråtkomst	A.9.2.5 Granskning av användares åtkomsträttigheter	2		
3519	Leverantören ska ha en rutin för att både avaktivera användarkonton och permanent ta bort konton från systemet.	A.9.2 Hantering av användaråtkomst	A.9.2.6 Borttagning eller justering av åtkomsträttigheter	2		
3520	Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation får hanteras.	A.9.3 Användaransvar	A.9.3.1 Användning av konfidentiell autentiseringsinformation	2	2	
3521	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 privilegierade konton.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.1 Begränsning av åtkomst till information	2	2	
3522	Systemet ska använda lösenord eller bättre för autentisering. Det ska finnas tekniska och administrativa åtgärder för hur lösenord får hanteras i systemet och av användaren. Se vägledning för tillitsnivå 2 (LoA2) för detaljer.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.2 Säkra inloggningsrutiner	2	2	
3523	Systemet ska ha funktioner för att kunna kravställa lösenordslängd, komplexitet och livslängd.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.3 System för lösenordshantering	2		
3524	Leverantören ska skydda och tillse att det finns spårbarhet i de verktyg som avses för underhåll av systemet, dess säkerhetskonfiguration och information.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.4 Användning av privilegierade verktygsprogram	2	2	
3525	Källkod framtagen i egen utveckling ska skyddas för obehöriga förändringar gentemot den godkända och fastställda versionen.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.5 Åtkomstkontroll till källkod för program	2	2	
3526	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	2	2	
3527	Datahallen uppfyller minst skyddsnivå 3 ("datahall" enligt MSB "Vägledning för fysisk informationssäkerhet i it-utrymmen")	A.11.1 Säkra områden	A.11.1.1 Fysiska säkerhetsavgränsningar	2		
3528	Leverantören ska ha rutiner som säkerställer att endast behörig personal har fysisk åtkomst till datahall.	A.11.1 Säkra områden	A.11.1.2 Fysiska tillträdesbegränsningar	2		1
3529	Leverantören ska ha rutiner avseende förändringshantering för de delar som kan påverka leveransens säkerhet och tillgänglighet. Dessa ska följas upp minst en gång under kontraktstiden, dock minst vart tredje år.	A.12.1 Driftsrutiner och ansvar	A.12.1.2 Ändringshantering	2	2	
3530	Leverantören ska ha funktioner, processer och rutiner för att övervaka och göra prognoser avseende prestanda.	A.12.1 Driftsrutiner och ansvar	A.12.1.3 Kapacitetshantering			1
3531	Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i Beställarens tjänst. Testdata ska skyddas och kontrolleras och får inte innehålla information som är känslig eller omfattas av sekretess.	A.12.1 Driftsrutiner och ansvar	A.12.1.4 Separation av utvecklings-, test och driftmiljöer		2	

3532	Leverantören ska ha ett skydd mot skadlig kod som uppdateras kontinuerligt för de delar som ingår i leveransen.	A.12.2 Skydd mot skadlig kod	A.12.2.1 Säkerhetsåtgärder mot skadlig kod	2	2	
3533	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 åtskilt.	A.12.3 Säkerhetskopiering	A.12.3.1 Säkerhetskopiering av information		2	1
3534	Loggningsfunktioner ska finnas för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter. Beställaren ska kunna genomföra granskning av användarrelaterade loggar.	A.12.4 Loggning och övervakning	A.12.4.1 Loggning av händelser	2	2	
3535	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	2	2	
3536	Systemet och relaterad infrastruktur ska använda tidssynkronisering mot samma tidskälla (GPS eller svenska UTC (SP)).	A.12.4 Loggning och övervakning	A.12.4.4 Synkronisering av tid		2	
3537	Leverantören ska verifiera och begränsa den mjukvara som får exekveras inom den levererade tjänsten	A.12.5 Styrning av driftsystem	A.12.5.1 Installation av program på driftsystem		2	
3538	Leverantören ska utan dröjsmål informera beställaren om tekniska sårbarheter i levererade komponenter. Upptäckta sårbarheter ska åtgärdas omgående.	A.12.6 Hantering av tekniska sårbarheter	A.12.6.1 Hantering av tekniska sårbarheter	2	2	1
3539	All kommunikation till och från systemet 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.	A.13.1 Hantering av nätverkssäkerhet	A.13.1.1 Säkerhetsåtgärder för nätverk	2	2	
3540	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	2	2	
3541	Beställaren ska informeras om alla informationsutbyten som sker med andra system utanför Beställarens miljö.	A.13.2 Informationsöverföring	A.13.2.1 Regler och rutiner för informationsöverföring	2	2	
3543	Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra system. Vid webbutveckling ska OWASP:s (www.owasp.org) rekommendationer följas.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.1 Analys och specifikation av informationssäkerhetskrav	2	2	
3544	Leverantören ska ha genomfört säkerhetsåtgärder mot obehörig åtkomst samt obehörig ändring av information som systemet utbyter med andra över öppna nät	A.14.1 Säkerhetskrav på informationssystem	A.14.1.2 Säkerställande av programtjänster på publika nätverk	2	2	
3545	Leverantören ska ha riktlinjer för informationssäkerhet inom sina utvecklingsprocesser. Vid större ändringar ska leverantören identifiera och hantera risker som säkerställer att säkerhetskraven i systemet är uppfyllda.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.2 Rutiner för hantering av systemändringar	2	2	
3546	Leverantören ska ha rutiner för att granska och testa tillgänglighet och säkerhet av ändringar i verksamhetskritiska driftsplattformar.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö	2	2	
3547	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	2	2	
3548	Leverantörens ansvar ska omfatta underleverantörer. Beställaren ska informeras om vilka underleverantörer som nyttjas.	A.15.1 Informationssäkerhet i leverantörsrelationer	A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer	2	2	
3549	Leverantören ska ha rutiner för övervakning, upptäckt, analys, rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.1 Ansvar och rutiner	2	2	

3550	Leverantören ska tillsammans med utpekad roll hos Beställaren samverka i hanteringen av sårbarheter, säkerhetshändelser eller säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.4 Bedömning av och beslut om informationssäkerhetshändelser	2	2	1
3551	Leverantören ska ha rutiner för att hantera säkerhetsincidenter enligt gällande lagar och förordningar.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.5 Hantering av informationssäkerhetsincidenter	2		
3554	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 avtalsmässiga krav	A.18.1.1 Identifiering av tillämplig lagstiftning och avtalsmässiga krav	2	2	1
3555	Om leverantören behandlar personuppgifter i systemet ska Beställaren upprätta biträdesavtal med leverantören avseende personuppgiftsbiträde innan avtalet träder i kraft.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.4 Skydd av personlig integritet och personuppgifter	2	2	
3556	Beställaren ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.	A.18.2 Granskningar av informationssäkerhet	A.18.2.3 Granskning av teknisk efterlevnad	2	2	
3557	Leverantören ska begära tillstånd innan information i systemet (texter, bilder etc) återanvänds i andra sammanhang.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A. 18.1.2 Immateriella rättigheter	2	2	

KLASSA - Upphandlingskrav

Informationsklassning 2020 befolkningsregister

Säkerhetsnivåer: Konfidentialitet - Nivå 2, Riktighet - Nivå 1, Tillgänglighet - Nivå 2

#	Krav	ISO kapitel	ISO kravområde	Kon.	Rik.	Til.
3501	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.	A.6.1 Intern organisation	A.6.1.1 Informationssäkerhetsroller och ansvar	2		2
3502	Leverantören ska ha tillsett att ansvar och arbetsuppgifter som står i konflikt med varandra och kan leda till missbruk är åtskilda.	A.6.1 Intern organisation	A.6.1.2 Uppdelning av arbetsuppgifter	2		2
3503	Leverantören ska ha upprättat kontakter med de myndigheter som berörs av leveransen	A.6.1 Intern organisation	A.6.1.3 Kontakt med myndigheter	2		2
3504	Leverantören ska ha en policy som beskriver hur de anställda får arbeta på distans avseende drift, förvaltning och support av de levererade tjänsterna.	A.6.2 Mobila enheter och distansarbete	A.6.2.2 Distansarbete	2		
3505	Leverantören ska ha processer och rutiner på plats för relevant bakgrundskontroll av personal.	A.7.1 Före anställning	A.7.1.1 Bakgrundskontroll	2		
3506	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.	A.7.1 Före anställning	A.7.1.2 Anställningsvillkor	2		
3507	Leverantören ska för sin personal regelbundet 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	2		2
3508	Leverantören ska ha tydliga och kommunicerade åtgärder för överträdelse av informationssäkerhetsregler.	A.7.2 Under anställning	A.7.2.3 Disciplinär process	2		2
3509	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	2		2
3510	Leverantören ska ha dokumenterade regler, rutiner och roller som beskriver tillåten användning av de resurser som ingår i leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.3 Tillåten användning av tillgångar	2		
3511	Leverantören ska ha rutiner och funktioner för att permanent radera information som är relaterade till leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.4 Återlämnande av tillgångar	2		
3512	Leverantören ska under kontraktstiden, dock minst vart tredje år, ha genomfört en riskbedömning för systemet. Identifierade brister ska åtgärdas enligt en dokumenterad plan och kunna redovisas för beställaren.	A.8.2 Informationsklassning	A.8.2.1 Klassning av information	2		2
3513	Beställarens krav på informationshanteringen ska efterföljas. Om sådana krav inte uttryckligen ställts ska leverantören utan anmodan kunna uppvisa de rutiner som gäller hos leverantören.	A.8.2 Informationsklassning	A.8.2.3 Hantering av tillgångar	2		
3514	Det ska finns en dokumenterad och formell process för hur användaridentiteter hanteras. De digitala identiteterna ska vara personliga och unika över tid.	A.9.2 Hantering av användaråtkomst	A.9.2.1 Registrering och avregistrering av användare	2		
3515	Leverantören ska följa en överenskommen rutin som möjliggör för Beställaren att godkänna hantering (skapande, borttag, ändring) av utpekade behörighetsroller t.ex avseende privilegierade (högre)	A.9.2 Hantering av användaråtkomst	A.9.2.2 Tilldelning av användaråtkomst	2		

3516	Leverantören ska använda särskilda personliga användaridentiteter för priviligierade (högre) behörigheter som används för systemadministration. Dessa konton ska vara spårbara och lätta att skilja	A.9.2 Hantering av användaråtkomst	A.9.2.3 Hantering av privilegierade åtkomsträttigheter	2		
3517	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	A.9.2 Hantering av användaråtkomst	A.9.2.4 Hantering av användares konfidentiella autentiseringsinformation	2		
3518	Behörighetssystemet ska logga information om när användare skapades, togs bort eller förändrades samt senaste inloggning.	A.9.2 Hantering av användaråtkomst	A.9.2.5 Granskning av användares åtkomsträttigheter	2		
3519	Leverantören ska ha en rutin för att både avaktivera användarkonton och permanent ta bort konton från systemet.	A.9.2 Hantering av användaråtkomst	A.9.2.6 Borttagning eller justering av åtkomsträttigheter	2		
3520	Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation får hanteras.	A.9.3 Användaransvar	A.9.3.1 Användning av konfidentiell autentiseringsinformation	2	1	
3521	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	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.1 Begränsning av åtkomst till information	2		
3522	Systemet ska använda lösenord eller bättre för autentisering. Det ska finnas tekniska och administrativa åtgärder för hur lösenord får hanteras i systemet och av användaren	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.2 Säkra inloggningsrutiner	2		
3523	Systemet ska ha funktioner för att kunna kravställa lösenordslängd, komplexitet och livslängd.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.3 System för lösenordshantering	2		
3524	Leverantören ska skydda och tillse att det finns spårbarhet i de verktyg som avses för underhåll av systemet, dess säkerhetskonfiguration och information	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.4 Användning av privilegierade verktygsprogram	2		
3525	Källkod framtagen i egen utveckling ska skyddas för obehöriga förändringar gentemot den godkända och fastställda versionen.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.5 Åtkomstkontroll till källkod för program	2		2
3526	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	2		
3527	Datahallen uppfyller minst skyddsnivå 3 ("datahall" enligt MSB "Vägledning för fysisk informationssäkerhet i it-utrymmen")	A.11.1 Säkra områden	A.11.1.1 Fysiska säkerhetsavgränsningar	2		2
3528	Leverantören ska ha rutiner som säkerställer att endast behörig personal har fysisk åtkomst till datahall.	A.11.1 Säkra områden	A.11.1.2 Fysiska tillträdesbegränsningar	2		2
3529	Leverantören ska ha rutiner avseende förändringshantering för de delar som kan påverka leveransens säkerhet och tillgänglighet. Dessa ska följas upp minst en gång under kontraktstiden, dock	A.12.1 Driftsrutiner och ansvar	A.12.1.2 Ändringshantering	2		2
3530	Leverantören ska ha funktioner, processer och rutiner för att övervaka och göra prognoser avseende kapacitet och prestanda.	A.12.1 Driftsrutiner och ansvar	A.12.1.3 Kapacitetshantering			2
3531	Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i Beställarens tjänst. Testdata ska skyddas och kontrolleras och får inte innehålla information som är känslig eller omfattas av sekretess	A.12.1 Driftsrutiner och ansvar	A.12.1.4 Separation av utvecklings-, test och driftmiljöer			2
3532	Leverantören ska ha ett skydd mot skadlig kod som uppdateras kontinuerligt för de delar som ingår i leveransen.	A.12.2 Skydd mot skadlig kod	A.12.2.1 Säkerhetsåtgärder mot skadlig kod	2		2
3533	Leverantören ska ha rutiner och funktioner för säkerhetskopiering och återställande av information enligt överenskomna tillgänglighetskrav med Beställaren. Säkerhetskopior ska skyddas på	A.12.3 Säkerhetskopiering	A.12.3.1 Säkerhetskopiering av information		1	2

3534	Loggningsfunktioner ska finnas för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter	A.12.4 Loggning och övervakning	A.12.4.1 Loggning av händelser	2		
3535	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	2	1	
3536	Systemet och relaterad infrastruktur ska använda tidssynkronisering mot samma tidskälla (GPS eller svenska UTC (SP)).	A.12.4 Loggning och övervakning	A.12.4.4 Synkronisering av tid		1	
3538	Leverantören ska utan dröjsmål informera beställaren om tekniska sårbarheter i levererade komponenter. Upptäckta sårbarheter ska åtgärdas omgående.	A.12.6 Hantering av tekniska sårbarheter	A.12.6.1 Hantering av tekniska sårbarheter	2	1	2
3539	All kommunikation till och från systemet ska vara skyddad mot obehörig åtkomst eller förvanskning. Det gäller både kommunikation mellan klient och server och mellan olika systemkomponenter. Skyddet ska	A.13.1 Hantering av nätverkssäkerhet	A.13.1.1 Säkerhetsåtgärder för nätverk	2		
3540	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	2		
3541	Beställaren ska informeras om alla informationsutbyten som sker med andra system utanför Beställarens miljö.	A.13.2 Informationsöverföring	A.13.2.1 Regler och rutiner för informationsöverföring	2		
3543	Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra system. Vid webbutveckling ska OWASP:s (www.owasp.org) rekommendationer följas.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.1 Analys och specifikation av informationssäkerhetskrav	2		
3544	obehörig åtkomst samt obehörig ändring av information som systemet utbyter med andra över öppna nät	A.14.1 Säkerhetskrav på informationssystem	A.14.1.2 Säkerställande av programtjänster på publika nätverk	2		
3545	Leverantören ska ha riktlinjer för informationssäkerhet inom sina utvecklingsprocesser. Vid större ändringar ska leverantören identifiera och hantera risker som säkerställer att säkerhetskraven i systemet är	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.2 Rutiner för hantering av systemändringar	2		2
3546	Leverantören ska ha rutiner för att granska och testa tillgänglighet och säkerhet av ändringar i verksamhetskritiska driftsplattformar.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö	2		2
3547	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	2		2
3548	Leverantörens ansvar ska omfatta underleverantörer. Beställaren ska informeras om vilka underleverantörer som nyttjas.	A.15.1 Informationssäkerhet i leverantörsrelationer	A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer	2		2
3549	Leverantören ska ha rutiner för övervakning, upptäckt, analys, rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.1 Ansvar och rutiner	2		2
3550	Leverantören ska tillsammans med utpekad roll hos Beställaren samverka i hanteringen av sårbarheter, säkerhetshändelser eller säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.4 Bedömning av och beslut om informationssäkerhetshändelser	2	1	2
3551	Leverantören ska ha rutiner för att hantera säkerhetsincidenter enligt gällande lagar och förordningar.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.5 Hantering av informationssäkerhetsincidenter	2		2
3552	Leverantören ska ha reservrutiner, reservlösningar och återstartsplaner som uppfyller beställarens krav på tillgänglighet (SLA).	A.17.1 Kontinuitet för informationssäkerhet	A.17.1.2 Införa kontinuitet för informationssäkerhet			2
3554	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 avtalsmässiga krav	A.18.1.1 Identifiering av tillämplig lagstiftning och avtalsmässiga krav	2	1	2

3555	Om leverantören behandlar personuppgifter i systemet ska Beställaren upprätta biträdesavtal med leverantören avseende personuppgiftsbiträde innan avtalet träder i kraft.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.4 Skydd av personlig integritet och personuppgifter	2		
3556	Beställaren ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.	A.18.2 Granskningar av informationssäkerhet	A.18.2.3 Granskning av teknisk efterlevnad	2		2
3557	Leverantören ska begära tillstånd innan information i systemet (texter, bilder etc) återanvänds i andra sammanhang.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A. 18.1.2 Immateriella rättigheter	2	1	

KLASSA - Upphandlingskrav

Informationsklassning 2020 webbkarta extern

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

#	Krav	ISO kapitel	ISO kravområde	Kon.	Rik.	Til.
3501	Leverantören ska ha en dokumenterad organisation där roller, personer och ansvar avseende informationssäkerhet är tydligt definierade.	A.6.1 Intern organisation	A.6.1.1 Informationssäkerhetsroller och ansvar	1	1	1
3507	Leverantören ska för sin personal regelbundet genomföra utbildningar för ökad medvetenhet kring informationssäkerhet.	A.7.2 Under anställning	A.7.2.2 Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet	1	1	1
3511	Leverantören ska ha rutiner och funktioner för att permanent radera information som är relaterade till leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.4 Återlämnande av tillgångar	1		
3512	Leverantören ska ha genomfört en riskbedömning för systemet och genomfört åtgärder för identifierade brister.	A.8.2 Informationsklassning	A.8.2.1 Klassning av information	1	1	1
3513	Beställarens krav på informationshanteringen ska efterföljas. Om sådana krav inte uttryckligen ställts ska leverantören utan anmodan kunna uppvisa de rutiner som gäller hos leverantören.	A.8.2 Informationsklassning	A.8.2.3 Hantering av tillgångar	1		
3514	Användare ska tilldelas personliga och unika användaridentiter. Se vägledningen för tillitsnivå 1 (LoA1) för detaljer.	A.9.2 Hantering av användaråtkomst	A.9.2.1 Registrering och avregistrering av användare	1		
3515	Leverantören ska följa en överenskommen rutin som möjliggör för Beställaren att godkänna utpekade behörigheter.	A.9.2 Hantering av användaråtkomst	A.9.2.2 Tilldelning av användarätkomst	1		
3516	Leverantören ska använda personliga och spårbara användaridentiteter för höga behörigheter som används för systemadministration.	A.9.2 Hantering av användaråtkomst	A.9.2.3 Hantering av privilegierade åtkomsträttigheter	1	1	
3517	Leverantören ska tillhandahålla ett sätt att distribuera och återställa lösenord utan att lösenordet kan röjas till obehöriga. Se vägledning för tillitsnivå 1 (LoA1) för detaljer.	A.9.2 Hantering av användaråtkomst	A.9.2.4 Hantering av användares konfidentiella autentiseringsinformation	1	1	
3518	Behörighetssystemet ska logga information om när användare skapas eller tas bort.	A.9.2 Hantering av användaråtkomst	A.9.2.5 Granskning av användares åtkomsträttigheter	1		
3519	Leverantören ska ha en rutin för att ta bort användaridentiteter från systemet	A.9.2 Hantering av användaråtkomst	A.9.2.6 Borttagning eller justering av åtkomsträttigheter	1		
3520	Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation får hanteras.	A.9.3 Användaransvar	A.9.3.1 Användning av konfidentiell autentiseringsinformation	1	1	
3521	Endast information eller tjänster som ska vara publika ska kunna nås i systemet och relaterad infrastruktur utan godkänd autentisering	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.1 Begränsning av åtkomst till information	1	1	
3522	Systemet ska använda lösenord eller bättre för autentisering. Det ska finnas regler för hur lösenord får hanteras i systemet och av användaren. Se vägledning för tillitsnivå 1 (LoA1) för detaljer.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.2 Säkra inloggningsrutiner	1	1	
3527	Datahallen uppfyller minst skyddsnivå 2 ("datarum", enligt MSB "Vägledning för fysisk informationssäkerhet i it-utrymmen")	A.11.1 Säkra områden	A.11.1.1 Fysiska säkerhetsavgränsningar	1		1

3528	Leverantören ska ha rutiner som säkerställer att endast behörig personal har fysisk åtkomst till datahall.	A.11.1 Säkra områden	A.11.1.2 Fysiska tillträdesbegränsningar	1		1
3530	Leverantören ska ha funktioner, processer och rutiner för att övervaka och göra prognoser avseende prestanda.	A.12.1 Driftsrutiner och ansvar	A.12.1.3 Kapacitetshantering			1
3532	Leverantören ska ha ett skydd mot skadlig kod för de delar som ingår i leveransen.	A.12.2 Skydd mot skadlig kod	A.12.2.1 Säkerhetsåtgärder mot skadlig kod	1	1	1
3533	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 åtskilt.	A.12.3 Säkerhetskopiering	A.12.3.1 Säkerhetskopiering av information		1	1
3534	Loggningsfunktioner ska finnas för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter.	A.12.4 Loggning och övervakning	A.12.4.1 Loggning av händelser	1	1	
3535	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	1	1	
3536	Systemet och relaterad infrastruktur ska använda tidssynkronisering mot samma tidskälla (GPS eller svenska UTC (SP)).	A.12.4 Loggning och övervakning	A.12.4.4 Synkronisering av tid		1	
3538	Leverantören ska utan dröjsmål informera beställaren om tekniska sårbarheter i levererade komponenter. Upptäckta sårbarheter ska åtgärdas omgående.	A.12.6 Hantering av tekniska sårbarheter	A.12.6.1 Hantering av tekniska sårbarheter	1	1	1
3541	Beställaren ska på begäran informeras om alla informationsutbyten som sker med andra system utanför Beställarens miljö.	A.13.2 Informationsöverföring	A.13.2.1 Regler och rutiner för informationsöverföring	1	1	
3543	Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra system samt redovisa dessa för beställaren.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.1 Analys och specifikation av informationssäkerhetskrav	1	1	
3545	Leverantören ska ha riktlinjer för informationssäkerhet inom sina uvecklingsprocesser.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.2 Rutiner för hantering av systemändringar	1	1	1
3548	Leverantörens ansvar ska omfatta underleverantörer. Beställaren ska på begäran informeras om vilka underleverantörer som nyttjas.	A.15.1 Informationssäkerhet i leverantörsrelationer	A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer	1	1	1
3549	Leverantören ska ha rutiner för rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.1 Ansvar och rutiner	1	1	1
3550	Leverantören ska tillsammans med utpekad roll hos Beställaren samverka i hanteringen av sårbarheter, säkerhetshändelser eller säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.4 Bedömning av och beslut om informationssäkerhetshändelser	1	1	1
3554	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 avtalsmässiga krav	A.18.1.1 Identifiering av tillämplig lagstiftning och avtalsmässiga krav	1	1	1
3555	Vid behandling av personuppgifter i systemet ska Beställaren upprätta biträdesavtal med leverantören avseende personuppgiftsbiträde innan avtalet träder i kraft.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.4 Skydd av personlig integritet och personuppgifter	1	1	
3557	Leverantören ska begära tillstånd innan information i systemet (texter, bilder etc) återanvänds i andra sammanhang.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A. 18.1.2 Immateriella rättigheter	1	1	

KLASSA - Upphandlingskrav

Informationsklassning 2020 webbkarta intern

Säkerhetsnivåer: Konfidentialitet - Nivå 2, Riktighet - Nivå 1, Tillgänglighet - Nivå 2

#	Krav	ISO kapitel	ISO kravområde	Kon.	Rik.	Til.
3501	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.	A.6.1 Intern organisation	A.6.1.1 Informationssäkerhetsroller och ansvar	2		2
3502	Leverantören ska ha tillsett att ansvar och arbetsuppgifter som står i konflikt med varandra och kan leda till missbruk är åtskilda.	A.6.1 Intern organisation	A.6.1.2 Uppdelning av arbetsuppgifter	2		2
3503	Leverantören ska ha upprättat kontakter med de myndigheter som berörs av leveransen	A.6.1 Intern organisation	A.6.1.3 Kontakt med myndigheter	2		2
3504	Leverantören ska ha en policy som beskriver hur de anställda får arbeta på distans avseende drift, förvaltning och support av de levererade tjänsterna.	A.6.2 Mobila enheter och distansarbete	A.6.2.2 Distansarbete	2		
3505	Leverantören ska ha processer och rutiner på plats för relevant bakgrundskontroll av personal.	A.7.1 Före anställning	A.7.1.1 Bakgrundskontroll	2		
3506	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.	A.7.1 Före anställning	A.7.1.2 Anställningsvillkor	2		
3507	Leverantören ska för sin personal regelbundet 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	2		2
3508	Leverantören ska ha tydliga och kommunicerade åtgärder för överträdelse av informationssäkerhetsregler.	A.7.2 Under anställning	A.7.2.3 Disciplinär process	2		2
3509	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	2		2

3510	Leverantören ska ha dokumenterade regler, rutiner och roller som beskriver tillåten användning av de resurser som ingår i leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.3 Tillåten användning av tillgångar	2		
3511	Leverantören ska ha rutiner och funktioner för att permanent radera information som är relaterade till leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.4 Återlämnande av tillgångar	2		
3512	Leverantören ska under kontraktstiden, dock minst vart tredje år, ha genomfört en riskbedömning för systemet. Identifierade brister ska åtgärdas enligt en dokumenterad plan och kunna redovisas för beställaren.	A.8.2 Informationsklassning	A.8.2.1 Klassning av information	2		2
3513	Beställarens krav på informationshanteringen ska efterföljas. Om sådana krav inte uttryckligen ställts ska leverantören utan anmodan kunna uppvisa de rutiner som gäller hos leverantören.	A.8.2 Informationsklassning	A.8.2.3 Hantering av tillgångar	2		
3514	Det ska finns en dokumenterad och formell process för hur användaridentiteter hanteras. De digitala identiteterna ska vara personliga och unika över tid.	A.9.2 Hantering av användaråtkomst	A.9.2.1 Registrering och avregistrering av användare	2		
3515	Leverantören ska följa en överenskommen rutin som möjliggör för Beställaren att godkänna hantering (skapande, borttag, ändring) av utpekade behörighetsroller t ex avseende priviligierade (högre) behörigheter. Hanteringen ska vara spårbar.	A.9.2 Hantering av användaråtkomst	A.9.2.2 Tilldelning av användaråtkomst	2		
3516	Leverantören ska använda särskilda personliga användaridentiteter för priviligierade (högre) behörigheter som används för systemadministration. Dessa konton ska vara spårbara och lätta att skilja från vanliga användare.	A.9.2 Hantering av användaråtkomst	A.9.2.3 Hantering av privilegierade åtkomsträttigheter	2		
3517	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	A.9.2 Hantering av användaråtkomst	A.9.2.4 Hantering av användares konfidentiella autentiseringsinformation	2		
3518	Behörighetssystemet ska logga information om när användare skapades, togs bort eller förändrades samt senaste inloggning.	A.9.2 Hantering av användaråtkomst	A.9.2.5 Granskning av användares åtkomsträttigheter	2		
3519	Leverantören ska ha en rutin för att både avaktivera användarkonton och permanent ta bort konton från systemet.	A.9.2 Hantering av användaråtkomst	A.9.2.6 Borttagning eller justering av åtkomsträttigheter	2		
3520	Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation får hanteras.	A.9.3 Användaransvar	A.9.3.1 Användning av konfidentiell autentiseringsinformation	2	1	

3521	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.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.1 Begränsning av åtkomst till information	2		
3522	Systemet ska använda lösenord eller bättre för autentisering. Det ska finnas tekniska och administrativa åtgärder för hur lösenord får hanteras i systemet och av användaren.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.2 Säkra inloggningsrutiner	2		
3523	Systemet ska ha funktioner för att kunna kravställa lösenordslängd, komplexitet och livslängd.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.3 System för lösenordshantering	2		
3524	Leverantören ska skydda och tillse att det finns spårbarhet i de verktyg som avses för underhåll av systemet, dess säkerhetskonfiguration och information.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.4 Användning av privilegierade verktygsprogram	2		
3525	Källkod framtagen i egen utveckling ska skyddas för obehöriga förändringar gentemot den godkända och fastställda versionen.	A.9.4 Styrning av åtkomst till system och tillämpningar	A.9.4.5 Åtkomstkontroll till källkod för program	2		2
3526	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	2		
3527	Datahallen uppfyller minst skyddsnivå 3 ("datahall" enligt MSB "Vägledning för fysisk informationssäkerhet i it-utrymmen")	A.11.1 Säkra områden	A.11.1.1 Fysiska säkerhetsavgränsningar	2		2
3528	Leverantören ska ha rutiner som säkerställer att endast behörig personal har fysisk åtkomst till datahall.	A.11.1 Säkra områden	A.11.1.2 Fysiska tillträdesbegränsningar	2		2
3529	Leverantören ska ha rutiner avseende förändringshantering för de delar som kan påverka leveransens säkerhet och tillgänglighet. Dessa ska följas upp minst en gång under kontraktstiden, dock minst vart tredje år.	A.12.1 Driftsrutiner och ansvar	A.12.1.2 Ändringshantering	2		2
3530	Leverantören ska ha funktioner, processer och rutiner för att övervaka och göra prognoser avseende kapacitet och prestanda.	A.12.1 Driftsrutiner och ansvar	A.12.1.3 Kapacitetshantering			2
3531	Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i Beställarens tjänst. Testdata ska skyddas och kontrolleras och får inte innehålla information som är känslig eller omfattas av sekretess.	A.12.1 Driftsrutiner och ansvar	A.12.1.4 Separation av utvecklings-, test och driftmiljöer			2

3532	Leverantören ska ha ett skydd mot skadlig kod som uppdateras kontinuerligt för de delar som ingår i leveransen.	A.12.2 Skydd mot skadlig kod	A.12.2.1 Säkerhetsåtgärder mot skadlig kod	2		2
3533	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 åtskilt.	A.12.3 Säkerhetskopiering	A.12.3.1 Säkerhetskopiering av information		1	2
3534	Loggningsfunktioner ska finnas för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter. Beställaren ska kunna genomföra granskning av användarrelaterade loggar.	A.12.4 Loggning och övervakning	A.12.4.1 Loggning av händelser	2		
3535	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	2	1	
3536	Systemet och relaterad infrastruktur ska använda tidssynkronisering mot samma tidskälla (GPS eller svenska UTC (SP)).	A.12.4 Loggning och övervakning	A.12.4.4 Synkronisering av tid		1	
3538	Leverantören ska utan dröjsmål informera beställaren om tekniska sårbarheter i levererade komponenter. Upptäckta sårbarheter ska åtgärdas omgående.	A.12.6 Hantering av tekniska sårbarheter	A.12.6.1 Hantering av tekniska sårbarheter	2	1	2
3539	All kommunikation till och från systemet 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.	A.13.1 Hantering av nätverkssäkerhet	A.13.1.1 Säkerhetsåtgärder för nätverk	2		
3540	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	2		
3541	Beställaren ska informeras om alla informationsutbyten som sker med andra system utanför Beställarens miljö.	A.13.2 Informationsöverföring	A.13.2.1 Regler och rutiner för informationsöverföring	2		
3543	Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra system. Vid webbutveckling ska OWASP:s (www.owasp.org) rekommendationer följas.	A.14.1 Säkerhetskrav på informationssystem	A.14.1.1 Analys och specifikation av informationssäkerhetskrav	2		
3544	Leverantören ska ha genomfört säkerhetsåtgärder mot obehörig åtkomst samt obehörig ändring av information som systemet utbyter med andra över öppna nät	A.14.1 Säkerhetskrav på informationssystem	A.14.1.2 Säkerställande av programtjänster på publika nätverk	2		

3545	Leverantören ska ha riktlinjer för informationssäkerhet inom sina utvecklingsprocesser. Vid större ändringar ska leverantören identifiera och hantera risker som säkerställer att säkerhetskraven i systemet är uppfyllda.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.2 Rutiner för hantering av systemändringar	2		2
3546	Leverantören ska ha rutiner för att granska och testa tillgänglighet och säkerhet av ändringar i verksamhetskritiska driftsplattformar.	A.14.2 Säkerhet i utvecklings- och supportprocesser	A.14.2.3 Teknisk granskning av tillämpningar efter ändringar i driftsmiljö	2		2
3547	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	2		2
3548	Leverantörens ansvar ska omfatta underleverantörer. Beställaren ska informeras om vilka underleverantörer som nyttjas.	A.15.1 Informationssäkerhet i leverantörsrelationer	A.15.1.1 Informationssäkerhetsregler för leverantörsrelationer	2		2
3549	Leverantören ska ha rutiner för övervakning, upptäckt, analys, rapportering, eskalering och hantering av säkerhetshändelser och säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.1 Ansvar och rutiner	2		2
3550	Leverantören ska tillsammans med utpekad roll hos Beställaren samverka i hanteringen av sårbarheter, säkerhetshändelser eller säkerhetsincidenter.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.4 Bedömning av och beslut om informationssäkerhetshändelser	2	1	2
3551	Leverantören ska ha rutiner för att hantera säkerhetsincidenter enligt gällande lagar och förordningar.	A.16.1 Hantering av informationssäkerhetsincidenter och förbättringar	A.16.1.5 Hantering av informationssäkerhetsincidenter	2		2
3552	Leverantören ska ha reservrutiner, reservlösningar och återstartsplaner som uppfyller beställarens krav på tillgänglighet (SLA).	A.17.1 Kontinuitet för informationssäkerhet	A.17.1.2 Införa kontinuitet för informationssäkerhet			2
3554	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 avtalsmässiga krav	A.18.1.1 Identifiering av tillämplig lagstiftning och avtalsmässiga krav	2	1	2
3555	Om leverantören behandlar personuppgifter i systemet ska Beställaren upprätta biträdesavtal med leverantören avseende personuppgiftsbiträde innan avtalet träder i kraft.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A.18.1.4 Skydd av personlig integritet och personuppgifter	2		
3556	Beställaren ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.	A.18.2 Granskningar av informationssäkerhet	A.18.2.3 Granskning av teknisk efterlevnad	2		2

3557	Leverantören ska begära tillstånd innan information i systemet (texter, bilder etc) återanvänds i andra sammanhang.	A.18.1 Efterlevnad av juridiska och avtalsmässiga krav	A. 18.1.2 Immateriella rättigheter	2	1	