Försäkran om tillämplighet ISO27001:2013

Version av den 23/02/2023 **Ändrad av: Säkerhetsteamet**

Klassificering: Offentlig

ISO27001:2013

		Implementerad lösning	Bevis och resultat
4	**Organisationens bakgrund**		
4.1	Förståelse för organisationen och dess sammanhang	Omfattning av SaaS säkerhetsstyrningssystem (SEPO12)	SELI030 - SOA
4.2	Förståelse för de berörda parternas behov och förväntningar		
4.3	Fastställande av omfattningen av ledningssystemet för informationssäkerhet		
4.4	Ledningssystem för informationssäkerhet		
5	**Ledarskap**		
5.1	Ledarskap och engagemang	Hantering av styrning, roller och ansvar för ISMS (SEPS4)	Åtagandeförklaring från ledningen
5.2	Policy		Protokoll från möten i strukturer för informationssäkerhet
5.3	Organisatoriska roller, ansvarsområden och befogenheter		
6	**Planering**		
6.1	Åtgärder för att hantera risker och möjligheter	Riskbedömning och behandlingsprocess (SEPS5)	Resultat av riskanalys och RTP
6.2	Mål för informationssäkerhet och planering för att uppnå dem		
7	**Stöd**		
7.1	Resurser	Säkerhet för mänskliga resurser	HR-processer och dokument
7.2	Kompetens		
7.3	Medvetenhet		
7.4	Kommunikation	(SEPO9) Kommunikationsprocess för	Protokoll från möten i säkerhetskommittén
7.5	Dokumenterad information		Process för elektronisk dokumenthantering
8	**Drift**		
8.1	Operativ planering och kontroll	Process för hantering av dokumentation (SEPS2)	Protokoll från möte i säkerhetskommittén
8.2	Riskbedömning av informationssäkerhet	Policy för kontroll, övervakning och förbättring (SEPO17) Riskhanteringsprocess (SEPS5)	Resultat av riskanalys och riskhanteringsplan
8.3	Informationssäkerhet riskhantering		
9	**Prestationsbedömning**		
9.1	Övervakning, mätning, analys och utvärdering	Kontroll, övervakning och förbättringspolicy (SEPO17) Efterlevnad	Säkerhetskommitténs
9.2	Internrevision	och revisionshantering (SEPO10)	mötesprotokoll Revisionsplanering
9.3	Ledningens genomgång	Hantering av styrning, roller och ansvar för ISMS (SEPS4)	Ledningens genomgång
10	**Förbättring**		
10.1	Avvikelser och korrigerande åtgärder	Hantering av efterlevnad och revision (SEPO10)	Planering av revision
10.2	Kontinuerlig förbättring	Policy för kontroll, övervakning och förbättring (SEPO17)	Protokoll från säkerhetskommitténs möten Protokoll från ledningens genomgång

LO = Rättsliga förpliktelser
CO = Contractual Obligations
BC = Business Commitment
BP = Best Practices
RA = Riskanalys

Genomförandet av de säkerhetskontroller som definieras i förklaringen om tillämplighet är avsett att minska de säkerhetsrisker som kan finnas i ISMS.

ISO27001:2013 Bilaga A

Krav			Ingår	LO	CO	BC	BP	RA	Lösning implementerad	Bevis och resultat
5	**Riktlinjer för informationssäkerhet**									**SEPO16 - Cegid Cloud Factory policy för informationssäkerhet**
5.1	**Ledningens riktlinjer för informationssäkerhet**	**Ge ledningen riktlinjer och stöd för information säkerhet i enlighet med verksamhetens krav och relevanta lagar och förordningar**	**Inklusive**							
5.1.1	Policyer för informationssäkerhet	En uppsättning riktlinjer för informationssäkerhet skall definieras, godkännas av ledningen, offentliggöras och meddelas anställda och relevanta externa parter.	JA					X	En policy för informationssäkerhet har utarbetats Den granskas årligen och godkänns av avdelningen för molntjänster	Åtagandeförklaring från ledningen
5.1.2	Översyn av riktlinjerna för informationssäkerhet	Riktlinjerna för informationssäkerhet skall ses över vid planerade intervall eller om betydande förändringar inträffar för att säkerställa deras fortsatta lämplighet, tillräcklighet och effektivitet.	JA					X		
6	**Organisation av informationssäkerhet**									**SEPS4 - Hantering av styrning, roller och ansvar för ISMS**
6.1	**Intern organisation**	**Upprätta ett ledningsramverk för att initiera och kontrollera införande och drift av informationssäkerhet inom organisationen**	**Inklusive**							
6.1.1	Roller och ansvar för informationssäkerhet	Alla ansvarsområden för informationssäkerhet ska definieras och fördelas.	JA					X	Koncernens säkerhetsteam är tvärfunktionellt organiserat. Den är hierarkiskt och operativt oberoende av ISMS-verksamheten.	Presentation av uppdragen och organisationen av de team som arbetar med informationssäkerhet
6.1.2	Uppdelning av arbetsuppgifter	Motstridiga arbetsuppgifter och ansvarsområden skall åtskiljas för att minska möjligheterna till obehörig eller oavsiktlig Ändring eller missbruk av någon av organisationens tillgångar.	JA					X	DevOps-liknande organisation av uppdrag och team	Organisation av AzurDevOps-team
6.1.3	Kontakt med myndigheter	Lämpliga kontakter med relevanta myndigheter måste upprätthållas.	JA		X			X	Cegids säkerhetsteam har regelbundet utbyte med CNIL och ANSSI	E-post/Meddelandeutbyte
6.1.4	Kontakt med särskilda intressegrupper	Lämpliga kontakter med särskilda intressegrupper eller andra specialister säkerhetsforum och yrkessammanslutningar skall upprätthållas.	JA					X	Medarbetarna i Cegid Security Team är medlemmar i följande organisationer: CLUSIR / CLUSIF /Club ISO 27001	Motivering för att prenumerera på Clusir/Clusif/
6.1.5	Informationssäkerhet i projektledning	Informationssäkerhet ska behandlas i projektledningen, oavsett vilken typ av projekt det rör sig om.	JA					X	Organisation av team och processer i agilt läge (Azure DevOps) för beaktande av säkerhet i infrastruktur och utveckling i alla projekt som rör ISMS	Organisation av AzurDevOps-team Säker utvecklingsstadga Avtal om interna tjänster Cloud/Dev Säkerhet för infrastrukturprojekt
6.2	**Mobila enheter och distansarbete**	**Säkerställa säkerheten vid distansarbete och användning av mobila enheter**								**SEOP7- Mobila enheter och distansarbete**
6.2.1	Policy för mobila enheter	En policy och stödjande säkerhetsåtgärder ska antas för att hantera Riskerna med att använda mobila enheter	JA					X	Kryptering av anställdas bärbara datorer Sekretessfilter	
6.2.2	Telearbete	En policy och stödjande säkerhetsåtgärder skall införas för att skydda information som nås, bearbetas eller lagras på distansarbetsplatser.	JA				X	X	MFA och VPN i mobilitetssituationer	
7	**Säkerhet för mänskliga resurser**									**SEPO9-Säkerhet för mänskliga resurser**

7.1	**Före anställning**	**Se till att anställda och entreprenörer förstår sina ansvarsområden och är lämpliga för de roller som de beaktas.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
7.1.1	Screening	Bakgrundskontroller av alla kandidater för anställning ska utföras i enlighet med relevanta lagar, förordningar och etiska regler och ska stå i proportion till verksamhetskraven, klassificeringen av den information som ska nås och de upplevda riskerna	JA			X		X	En kontroll av referenser (examensbevis, brottsregister etc.) utförs av koncernens rekryteringsteam	Rekryteringsförfaranden inom koncernen HR Avtal om SaaS/HR-tjänster	
7.1.2	Anställningsvillkor	Avtal med anställda och entreprenörer skall ange sitt och organisationens ansvar för information säkerhet	JA			X		X	Anställningsavtalet som undertecknas av de nya anställda innehåller en sekretess- och en konkurrensklausul		
7.2	**Under anställningstiden**	**Se till att anställda och entreprenörer är medvetna om och fullgöra sitt ansvar för informationssäkerheten**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
7.2.1	Ledningens ansvarsområden	Ledningen skall kräva att alla anställda och entreprenörer tillämpar informationssäkerhet i enlighet med organisationens fastställda riktlinjer och förfaranden.	JA				X		Formellt engagemang från avdelningen för molntjänster genom olika kommittéer, möten och kommunikation kring säkerhet och ISMS	Åtagandeförklaring från ledningen	
7.2.2	Medvetenhet om informationssäkerhet, utbildning och fortbildning	Alla anställda i organisationen och, i förekommande fall, entreprenörer ska få lämplig utbildning och medvetenhetsträning och regelbundna uppdateringar av organisationens policyer och förfaranden, som är relevanta för deras arbetsfunktion.	JA			X	X	X	Säkerhetsutbildning för nyanställda tillhandahålls systematiskt En årlig plan för medvetenhet tas fram	Utbildningsplaner och innehåll Innehåll och resultat av medvetandehöjande åtgärder	
7.2.3	Disciplinärt förfarande	Det ska finnas en formell och kommunicerad disciplinär process för att vidta åtgärder mot anställda som har begått en brott mot informationssäkerheten.	JA			X	X	X	Ett disciplinärt förfarande kan inledas vid överträdelse av ISSP eller stadgan för användning av IT-verktyg och utrustning	Interna bestämmelser Anställningsavtal Förstärkt sekretessklausul	
7.3	**Uppsägning och byte av anställning**	**Skydda organisationens intressen som en del av processen att byte eller uppsägning av anställning.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
7.3.1	Uppsägning eller byte av arbetsuppgifter	Ansvar och skyldigheter avseende informationssäkerhet som kvarstår efter uppsägning eller byte av anställning ska definieras, kommuniceras till den anställde eller uppdragstagaren och upprätthållas.	JA	X	X			X	Anställda informeras om sitt ansvar i händelse av en förändring, uppsägning eller avslutande av kontrakt av sin HR-korrespondent	Anställningsavtal	
8	**Förvaltning av tillgångar**									**SEPO5-Asset management**	
8.1	**Ansvar för tillgångar**	**Identifiera organisatoriska tillgångar och definiera lämpliga ansvar för skydd**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
8.1.1	Inventering av tillgångar	Tillgångar som hör till anläggningar för information och informationsbehandling skall identifieras och en inventering av dessa tillgångar skall göras. upprättas och underhålls.	JA				X	X	Förteckningen över tillgångar granskas och uppdateras i riskanalysverktyget	Förteckning över tillgångar	
8.1.2	Ägande av tillgångar	Tillgångarna i inventeringen ska vara ägda.	JA				X	X	Tillgångarna ägs av avdelningen för molntjänster	Definiera ägaren av fysiska tillgångar och ägarens roll	
8.1.3	Godtagbar användning av tillgångar	Regler för godtagbar användning av information och av tillgångar som är knutna till anläggningar för informations- och databehandling skall vara identifieras, dokumenteras och genomföras.	JA		X		X	X	En policy för acceptabel användning har utarbetats och kommunicerats till de anställda	Policy för godtagbar användning	
8.1.4	Avkastning på tillgångar	Alla anställda och externa användare ska återlämna alla organisatoriska tillgångar som de innehar när de avslutar sin anställning. anställning, kontrakt eller överenskommelse.	JA		X		X		Återlämnande av tillgångar enligt inventeringen av den anställdes uppsägningsformulär under chefens ansvar	Cegid Groups personalavdelning	
8.2	**Klassificering av information**	**Säkerställa att informationen får en lämplig nivå av skydd i enlighet med dess betydelse för organisation.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**		**SEPS2-Dokumentationshantering**	
8.2.1	Klassificering av information	Informationen skall klassificeras med avseende på rättsliga krav, värde, kritisk betydelse och känslighet för obehörigt röjande eller obehörig ändring.	JA				X		Informationen klassificeras enligt 5 kriterier		
8.2.2	Märkning av information	En lämplig uppsättning förfaranden för informationsmärkning skall utarbetas och genomföras i enlighet med det system för informationsklassificering som organisationen har antagit.	JA				X		Alla tillgångar (dokument, kundtillgångar) omfattas av policyn för förvaltning av tillgångar. Denna policy tar hänsyn till nivån av klassificering av tillgångar som är förknippad med dess nivå av spridning och kryptering som är nödvändig för dess spridning	RCNT7- Klientdiskens livscykel	
8.2.3	Hantering av tillgångar	Förfaranden för hantering av tillgångar skall utvecklas och genomföras i enlighet med det system för informationsklassificering som antagits av organisationen.	JA				X				
8.3	**Hantering av media**	**Förhindra obehörigt röjande, ändring, borttagning eller förstöring av information som lagrats på media.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
8.3.1	Hantering av flyttbara media	Förfaranden skall införas för hantering av flyttbara medier i enlighet med det klassificeringssystem som antagits av organisation.	JA			X			Begränsning av användningen av flyttbara media (USB) för anställda DC-leverantör Rutin för flyttbara media för lagring av kunddata	Stadga för användning av IS-verktyg	
8.3.2	Kassering av media	Media ska kasseras på ett säkert sätt när de inte längre behövs, med hjälp av formella förfaranden.	JA	X	X	X		X	Formatering på låg nivå av lagringsmedia på de anställdas arbetsstationer Fysisk förstöring av lagringsmedia för kunddata av DC-leverantörerna	Bevis på att data förstörts genom SaaS produktion/tillgång till dokumentförstörare	
8.3.3	Fysisk överföring av media	Medier som innehåller information ska skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport.	JA		X	X		X	Kryptering av flyttbara lagringsmedier vid överföring av kunddata Spårning av kvitton och försändelser med Chronopost	RCNT7- Klientdiskens livscykel	
9	**Kontroll av åtkomst**									**SEPO1-Zugångskontroll**	
9.1	**Affärsmässiga krav på åtkomstkontroll**	**Begränsa tillgången till information och informationsbehandling anläggningar**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			

9.1.1	Policy för åtkomstkontroll	En policy för åtkomstkontroll skall upprättas, dokumenteras och granskas på grundval av verksamhets- och informationssäkerhetskrav.	JA		X		X	X	X	Policy för åtkomstkontroll granskas årligen	
9.1.2	Tillgång till nätverk och nätverkstjänster	Användare ska endast ges tillgång till det nät och de nättjänster som de har särskilt tillstånd att använda.	JA				X	X		En rättighetsmatris säkerställer hanteringen av användarrättigheter och tillgång till resurser. Denna matris revideras minst en gång per år.	Matris för rättigheter
9.2	**Hantering av användaråtkomst**	**Säkerställa behörig användaråtkomst och förhindra obehörig tillgång till system och tjänster**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
9.2.1	Registrering och avregistrering av användare	En formell process för registrering och avregistrering av användare ska implementeras för att möjliggöra tilldelning av åtkomsträttigheter.	JA		X	X	X	X	X	Hantering av användarregistreringar/avregistreringar i vårt orkestreringsverktyg för Cloud Factory-plattformen	Serviceförfrågan och arbetsflöde stratus
9.2.2	Tillhandahållande av användaråtkomst	En formell process för tillhandahållande av användaråtkomst ska införas för att Tilldela eller återkalla åtkomsträttigheter för alla användartyper till alla system och tjänster.	JA		X	X	X	X	X		
9.2.3	Hantering av privilegierade åtkomsträttigheter	Tilldelning och användning av privilegierade åtkomsträttigheter ska begränsas och kontrollerad.	JA				X	X	X	Tilldelningsrättigheter per användargrupp för de applikationer som ska användas	Cegid Cloud Factory rättighetsmatris
9.2.4	Hantering av hemlig autentiseringsinformation för användare	Tilldelningen av hemliga autentiseringsuppgifter skall kontrolleras genom en formell ledningsprocess.	JA				X	X	X	Autentiseringsinformation kommuniceras i enlighet med en formaliserad HR-process Det kommuniceras endast när den anställdes personnummer tilldelas	
9.2.5	Granskning av användarnas åtkomsträttigheter	Tillgångsägare ska regelbundet se över användarnas åtkomsträttigheter	JA				X	X	X	En förnyad validering av teamrättigheter av chefer genomförs varje kvartal	Kvartalsvis lista över revalidering av rättigheter validerad av chefer
9.2.6	Avlägsnande eller justering av tillträdesrättigheter	Alla anställdas och externa parters åtkomsträttigheter till information och anläggningar för informationsbehandling ska upphävas när deras anställning, kontrakt eller avtal upphör, eller justeras vid förändring.	JA				X	X	X	När våra HR-verktyg bekräftar att anställningsperioden har upphört behandlas begäran i vårt orkestreringsverktyg.	Serviceförfrågan och Stratus Workflow
9.3	**Användarnas ansvar**	**Gör användarna ansvariga för att skydda sina autentiseringsinformation.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
9.3.1	Användning av hemlig autentiseringsinformation	Användare skall vara skyldiga att följa organisationens praxis vid användning av av hemlig autentiseringsinformation	JA				X	X	X	Regler för användning av hemlig information är tydligt definierade i stadgan för användning av IT-verktyg	SENT14- Policy för hantering av lösenord Policy för godtagbar användning
9.4	**Åtkomstkontroll för system och applikationer**	**förhindra obehörig åtkomst till system och applikationer**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
9.4.1	Begränsning av tillgång till information	Tillgång till information och funktioner i tillämpningssystem ska vara begränsas i enlighet med policyn för åtkomstkontroll.	JA				X	X		Matrisen för rättigheter och åtkomst definierar åtkomst per affärsgrupp och per applikation	Matris för rättigheter
9.4.2	Säkra procedurer för inloggning	Om det krävs enligt policyn för åtkomstkontroll skall åtkomsten till system och tillämpningar kontrolleras genom ett säkert inloggningsförfarande.	JA					X	X	Cegid Cloud Factory-medarbetarnas anslutning till produktionsmiljöerna sker via en P.A.M. (Bastion) och via ett säkert fjärråtkomstsystem (RDM)	Användarhandbok för PAM
9.4.3	System för hantering av lösenord	Systemen för hantering av lösenord ska vara interaktiva och säkerställa lösenord av hög kvalitet.	JA					X	X	En policy för lösenordshantering definieras för Cegid Cloud Factorys anställda samt för kunder använda Cegids SaaS-applikationer	SENT14- Policy för hantering av lösenord
9.4.4	Användning av privilegierade verktygsprogram	Användningen av verktygsprogram som kan åsidosätta system- och applikationskontroller skall begränsas och kontrolleras noggrant.	JA							Ett verktyg för hantering och begränsning av skugg-IT används för att kontrollera användningen av obehöriga program och applikationer	Matris för rättigheter
9.4.5	Åtkomstkontroll till programkällkod	Tillgång till programmets källkod skall begränsas	JA					X	X	Manus förvaras i säkra utrymmen som endast är tillgängliga för produktionsteamen	Lista över behöriga användare
10	**Kryptografi**										**SEPO12-Informationsöverföring och kryptering**
10.1	**Kryptografiska kontroller**	**Säkerställa korrekt och effektiv användning av kryptografi för att skydda konfidentialiteten, autenticiteten och/eller integriteten hos information.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
10.1.1	Policy för användning av kryptografiska kontroller	En policy för användning av kryptografiska kontroller för skydd av information skall utarbetas och genomföras.	JA		X	X	X	X		Policy för kryptering av flöden och data Denna policy ses över regelbundet för att tillhandahålla den bästa säkerhetsnivån i enlighet med god praxis	Årlig översyn av denna policy
10.1.2	Nyckelhantering	En policy för användning, skydd och livslängd för kryptografiska nycklar ska utvecklas och genomföras under hela deras livscykel.	JA				X	X		Administration av certifikat för HTTPS-åtkomst i enlighet med god praxis Erkänd certifikatutfärdare, förvaring av nycklar i ett nyckelvalv Hantering av krypteringsnycklar för data som lagras i datacentren	Certifikat som administreras av Cegid och utfärdas av en erkänd CA Nyckelhantering av Cegid (privat moln) eller av leverantören (offentligt moln)
11	**Fysisk och miljömässig säkerhet**										**SEPO1 Tillträdeskontroll / SEPO6 Fysisk och miljömässig säkerhet**
11.1	**Säkra områden**	**Förhindra obehörig fysisk åtkomst, skada och störning av organisationens information och anläggningar för informationsbehandling.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
11.1.1	Fysisk säkerhetsperimeter	Säkerhetsperimetrar skall definieras och användas för att skydda områden som innehåller antingen känslig eller kritisk information och information bearbetningsanläggningar	JA					X		Drifts- och produktionsteam befinner sig i fysiskt isolerade lokaler	Serviceavtal med stödjande verktyg
11.1.2	Fysiska inpasseringskontroller	Säkra områden ska skyddas genom lämpliga inpasseringskontroller för att se till att endast behörig personal har tillträde	JA					X	X	Säker tillgång till produktionslokalerna med badge endast för behöriga medarbetare	Månatlig åtkomstkontrollista
11.1.3	Säkring av kontor, rum och anläggningar	Fysisk säkerhet för kontor, rum och anläggningar skall utformas och tillämpad	JA					X	X	Låsta dörrar med larm vid långvarig öppning	
11.1.4	Skydd mot externa hot och miljöhot	Fysiska skyddsåtgärder mot naturkatastrofer, illvilliga angrepp eller olyckor bör utformas och genomföras	JA			X	X	X	X	Skydd av byggnaden där produktionsteamen finns Strömförsörjning, luftkonditionering, nätverkskablar etc.	
11.1.5	Arbete inom säkra områden	Rutiner för arbete inom säkra områden skall utformas och tillämpas.	JA						X	Skydd av byggnaden där produktionsteamen finns Strömförsörjning, luftkonditionering, nätverkskablar etc. För Talentsofts långvariga lokaler finns det inget arbete i säkra områden. Detta krav är därför inte	Avtal om interna leverantörstjänster med General Services
11.1.6	Leverans- och lastutrymmen	Tillträdespunkter såsom leverans- och lastningsområden och andra punkter där obehöriga personer kan komma in i lokalerna skall kontrolleras och om möjligt isoleras från informationsbehandling. anordningar för att förhindra obehörigt tillträde	JA					X	X	Leveranser sker till byggnadens säkerhetsdator Kontrollen utförs av ett privat säkerhetsföretag under ledning av Cegids SG	
11.2	**Utrustning**	**Förhindra förlust, skada, stöld eller äventyrande av tillgångar och avbrott i organisationens verksamhet.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			

11.2.1	Placering och skydd av utrustning	Utrustningen ska placeras och skyddas så att riskerna från miljöhot och miljöfaror minskas, liksom möjligheterna för obehörig åtkomst.	JA				X	X	Känslig utrustning förvaras i säkra lokaler	Avtal om interna leverantörstjänster med General Services
11.2.2	Stödjande verktyg	Utrustningen ska skyddas mot strömavbrott och andra Störningar orsakade av fel i stödjande verktyg.	JA					X	Oberoende kraftförsörjningssystem är i drift i händelse av fel i det allmänna systemet.	Underhållsavtal med leverantör av växelriktare
11.2.3	Säkerhet vid kabeldragning	Kraft- och telekommunikationskablar som transporterar data eller stödjer Informationstjänster skall skyddas mot avlyssning, störning eller skada.	JA				X	X	SaaS produktions-LAN är ett switchat nätverk som är fysiskt oberoende av resten av företaget	Konfiguration och schema för SaaS nätverksarkitektur
11.2.4	Underhåll av utrustning	Utrustningen ska underhållas korrekt för att säkerställa dess fortsatta tillgänglighet och integritet	JA				X	X	Underhåll av intern utrustning och samarbetspartners läggs ut på entreprenad och formaliseras genom avtal av IT-avdelningen	Internt leverantörsavtal med IT-avdelningen
11.2.5	Avlägsnande av tillgångar	Utrustning, information eller programvara får inte tas med från platsen utan förhandstillstånd	JA					X	Formaliseras i stadgan för användning av IT-verktyg och IT-resurser	
11.2.6	Säkerhet för utrustning och tillgångar utanför lokalerna	Säkerhet skall tillämpas på tillgångar utanför anläggningen med beaktande av följande olika risker med att arbeta utanför organisationens lokaler.	JA				X	X	Diskkryptering, antivirus, säker fjärranslutning via access gateway och/eller VPN	Internt leverantörsavtal med IT-avdelningen
11.2.7	Säkert bortskaffande eller återanvändning av utrustning	All utrustning som innehåller lagringsmedia ska kontrolleras för att säkerställa att alla känsliga uppgifter och licensierad programvara har avlägsnats eller skrivits över på ett säkert sätt innan den kasseras eller återanvänds.	JA	X	X	X	X	X	Förstöring av media som innehåller kunddata eller är relaterade till sådana data (anställdas arbetsstationer)	Bevis på förstörelse av data genom produktion av SaaS enligt molnkontrakt
11.2.8	Obevakad användarutrustning	Användare skall säkerställa att obevakad utrustning har lämpliga skydd	JA				X	X	Stöldskyddskabel på anställdas arbetsstationer	Skärmar låser sig efter 15 minuter (AD-strategi)
11.2.9	Policy för tydliga skrivbord och tydliga skärmar	En policy för tydliga skrivbord för papper och flyttbara lagringsmedier och en policy för tydliga skärmar för informationsbehandlingsanläggningar skall vara antagna	JA				X		Förvaring av dokument i ett särskilt samarbetsutrymme Individuellt förvaringsskåp - Dokumentförstörare för dokument som ska kasseras Automatisk låsning av sessioner vid en längre period av inaktivitet	
12	**Operativ säkerhet**									**SEPO4 Operativ säkerhet**
12.1	**Operativa förfaranden och ansvarsområden**	**Säkerställa korrekt och säker hantering av information bearbetningsanläggningar**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**		
12.1.1	Dokumenterade operativa förfaranden	Driftsrutinerna ska dokumenteras och göras tillgängliga för alla användare som behöver dem	JA				X	X	Alla operativa förfaranden är dokumenterade och tillgängliga för alla SaaS-anställda i EDM	Process för hantering av elektroniska dokument
12.1.2	Hantering av förändringar	Förändringar i organisation, affärsprocesser, information bearbetningsanläggningar och system som påverkar informationssäkerheten skall kontrolleras	JA				X	X	Ett veckomöte om förändringshantering planeras	Protokoll och hantering av ändringar i Inside

12.1.3	Kapacitetsförvaltning	Resursanvändningen skall övervakas, stämmas av och prognoser göras. framtida kapacitetskrav för att säkerställa erforderlig systemprestanda	JA				X	X	X	Löpande övervakning av resurstilldelningen Månatlig kommitté för infrastruktur och resursstorlek	Centreon övervakningskonsol Protokoll från möte om kapacitetsplanering Anpassning av HR till verksamheten
12.1.4	Separering av utvecklings-, test- och driftsmiljöer	Utvecklings-, test- och driftsmiljöer ska separeras för att minska riskerna för obehörigt tillträde till eller obehöriga ändringar av operativ miljö	JA				X	X	X	Segregering genom automatiserat arbetsflöde i Azure DevOps	Nätverksarkitektur
12.2	**Skydd mot skadlig kod**	**Säkerställa att information och anläggningar för informationsbehandling skyddas mot skadlig kod**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**		**RA**		
12.2.1	Kontroller mot skadlig kod	Kontroller för upptäckt, förebyggande och återställning för att skydda mot skadlig kod ska implementeras, i kombination med lämpliga användar medvetenhet	JA					X	X	Centraliserad och hanterad antivirus/antimalware för alla resurser	Antiviral konsol (uppdatering av dokumentet kommer att ske)
12.3	**Säkerhetskopiering**	**Skydda mot förlust av data**	**Inklusive**	**LO**	**BO**	**BC**	**BLO DTR YCK**		**RA**		
12.3.1	Säkerhetskopiering av information	Säkerhetskopior av information, programvara och systemavbilder skall tas och testas regelbundet i enlighet med en överenskommen säkerhetskopieringspolicy.	JA						X	Policyn för säkerhetskopiering tar hänsyn till det specifika i varje kunderbjudande. Den tar hänsyn till tillgänglighet, integritet och lagring.	Rapporter för säkerhetskopiering
12.4	**Loggning och övervakning**	**Registrera händelser och skapa bevis.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**		**RA**		
12.4.1	Loggning av händelser	Händelseloggar som registrerar användaraktiviteter, undantag, fel och informationssäkerhetshändelser ska upprättas, bevaras och regelbundet granskas.	JA	X	X	X	X		X	Informationssäkerhetshändelser centraliseras i ett verktyg för aggregering av loggar. Detta verktyg styrs av en väldefinierad policy	Konsoler för centralisering av loggar (Splunk)
12.4.2	Skydd av logginformation	Loggningsanläggningar och logginformation skall skyddas mot manipulering och obehörig åtkomst	JA	X			X		X	Verktyget för logghantering hostas i en säker arkitektur (redundans, kryptering av flöden och diskar, åtkomsthantering, säkerhetskopiering)	Konsoler för centralisering av loggar (Splunk)
12.4.3	Administratörs- och operatörsloggar	Systemadministratörens och systemoperatörens aktiviteter skall loggas. och loggarna skyddas och granskas regelbundet.	JA		X		X		X	En automatisk rapport över administratörs- och operatörsloggar produceras varje månad	Rapport om administratörskonton (Splunk)
12.4.4	Synkronisering av klockor	Klockorna för alla relevanta system för informationsbehandling inom en organisation eller en säkerhetsdomän skall synkroniseras med en enda referens tid källa	JA		X		X		X	En NTP-synkronisering är konfigurerad på alla tillgångar	Gruppstrategier och NTP-dokument
12.5	**Kontroll av operativ programvara**	**Säkerställa de operativa systemens integritet**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**		**RA**		
12.5.1	Installation av programvara på operativa system	Förfaranden skall införas för att kontrollera installationen av programvara på operativa system.	JA					X	X	Ett verktyg och en centraliserad konsol möjliggör inventering av programvara i drift. Installationsmallar används för konfigurering av virtuella servrar	Konsoler för inventering av programvara
12.6	**Hantering av tekniska sårbarheter**	**Förhindra utnyttjande av tekniska sårbarheter**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**		**RA**		**Operativ säkerhet (OPSEU4)**
12.6.1	Hantering av teknisk sårbarhet	Information om tekniska sårbarheter hos informationssystem som används skall erhållas i god tid, organisationens exponering för sådana sårbarheter skall utvärderas och lämpliga åtgärder skall vidtas. åtgärder för att hantera den associerade risken	JA					X	X	Hantering av sårbarheter sker genom ett skanningsverktyg och genom varningar från CERT Policy för hantering av dessa sårbarheter genom scope i eskaleringsläge	Protokoll från möten för övervakning av IS-säkerheten
12.6.2	Restriktioner för installation av programvara	Regler för användarnas installation av programvara skall vara inrättas och genomförs	JA					X	X	Policy för upptäckt av skugg-IT Verktyg på anställdas arbetsstationer	Stadga för användning av verktyg
12.7	**Överväganden vid revision av informationssystem**	**Minimera revisionsverksamhetens påverkan på den operativa verksamheten system**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**		**RA**		**Operativ säkerhet (OPSEU4)**
12.7.1	Revisionskontroller av informationssystem	Revisionskrav och verksamhet som omfattar verifiering av operativa system ska planeras noggrant och överenskommas så att störningar minimeras. till affärsprocesser	JA					X	X	De olika policyerna (Scan) och avtalen (Pentest) tar hänsyn till affärsområdenas verksamhetsperioder för att minimera effekterna	Mallar för revisions- och testavtal
13	**Kommunikationssäkerhet**										**SEPO14-Hantering av nätverkssäkerhet**
13.1	**Hantering av nätsäkerhet**	**Säkerställa skyddet av information i nätverk och dess Stödjande anläggningar för informationsbehandling.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**		**RA**		
13.1.1	Kontroll av nätverk	Nät skall hanteras och kontrolleras för att skydda information i system och tillämpningar.	JA					X	X	Nätverk och länkar övervakas med hjälp av övervakningsverktyg. Åtkomst spåras och kontrolleras	Förfarande för åtskillnad av rättigheter och team. Åtkomstkontroll och loggar för utrustning. Redundans av team, utrustning och resurser. Intern leverantör - IT-avdelningens serviceavtal Ett serviceavtal som omfattar servicegarantin tillämpas med IT-avdelningen för LAN- och WAN-delen Nätverkspartitionering genom inrättande av DMZ och VLAN. Nätverk och länkar övervakas live av övervakningsverktyg.
13.1.2	Säkerhet för nättjänster	Säkerhetsmekanismer, servicenivåer och förvaltningskrav för alla nättjänster ska identifieras och ingå i avtal om nättjänster, oavsett om dessa tjänster tillhandahålls internt eller outsourcad	JA					X	X	Ett internt serviceavtal formaliseras årligen med IT-avdelningen Det tar hänsyn till nätverkssäkerheten	Nätverk och länkar övervakas live av övervakningsverktyg.
13.1.3	Segregering i nätverk	Grupper av informationstjänster, användare och informationssystem skall vara segregerade på nätverk	JA					X	X	Nätverkspartitionering genom att upprätta DMZ och VLAN.	Dokument om nätarkitektur
13.2	**Överföring av information**	**Upprätthålla säkerheten för information som överförs inom en organisation och med alla externa enheter.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**		**RA**		**SEPO2- Informationsöverföring och kryptering**
13.2.1	Riktlinjer och förfaranden för informationsöverföring	Formella riktlinjer, förfaranden och kontroller för överföring ska finnas på plats för att skydda överföringen av information genom användning av alla typer av Kommunikationsanläggningar	JA					X	X	En policy med regler för kryptering och säkerhet vid kommunikation har upprättats. Den ses över regelbundet.	
13.2.2	Avtal om informationsöverföring	Avtalen ska omfatta säker överföring av företagsinformation. mellan organisationen och externa parter	JA				X	X	X	De säkra utbytesprotokoll som används med tredje part gör det möjligt att garantera integriteten, konfidentialitet och oavvislighet i fråga om information	
13.2.3	Elektroniska meddelanden	Information som ingår i elektroniska meddelanden ska på lämpligt sätt skyddad	JA					X	X	E-post använder endast säkra processer (flöde, autentisering)	Konfiguration av e-postserver

13.2.4	Avtal om sekretess eller tystnadsplikt	Krav på avtal om sekretess eller tystnadsplikt återspegla organisationens behov av skydd av information skall fastställas, regelbundet ses över och dokumenteras	JA			X		X	X	All Cegid-personal som arbetar med konfidentiella uppgifter undertecknar ett sekretessavtal, utan tidsbegränsning, med disciplinära åtgärder eller åtal vid bristande efterlevnad.	HR-processer
14	**Förvärv, utveckling och underhåll**										**SEPO8-Informationssäkerhetspolicy i projektledning**
14.1	**Säkerhetskrav för informationssystem**	**Säkerställa att informationssäkerhet är en integrerad del av informationssystem över hela livscykeln. Detta omfattar även kraven på informationssystem som tillhandahålla tjänster över allmänna nät.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			**SEPO2- Informationsöverföring och kryptering**
14.1.1	Analys och specifikation av krav på informationssäkerhet	De informationssäkerhetsrelaterade kraven skall ingå i kraven för nya informationssystem eller förbättringar av Befintliga informationssystem.	JA				X	X	Formaliserade säkerhetsförfaranden integreras i alla projekt och under hela projektets livscykel.	Frågeformulär om projektets säkerhetskrav	
14.1.2	Säkra applikationstjänster i publika nätverk	Information som ingår i applikationstjänster som passerar över allmänna nät skall skyddas mot bedräglig verksamhet, avtalstvister och obehörigt röjande och obehörig ändring.	JA		X		X	X	Perimeterskydd för åtkomst till offentliga nätverk (brandvägg, IDS/IPS-sond) Kryptering av flöden med certifikat som utfärdats av ett erkänt certifieringsorgan; nycklarna lagras i ett digitalt kassaskåp	Policy för informationsöverföring och kryptering	
14.1.3	Skydda transaktioner för applikationstjänster	Information som ingår i applikationstjänsttransaktioner ska skyddas för att förhindra ofullständig överföring, felaktig dirigering, obehörig ändring av meddelanden och obehörigt röjande, Otillåten kopiering eller uppspelning av meddelanden.	JA				X	X	Användning av säkra protokoll som säkerställer fullständig överföring utan möjlig ändring av informationen och som förbjuder obehörig ändring, obehörigt röjande och obehörig kopiering.		
14.2	**Säkerhet i utvecklings- och supportprocesser**	**Säkerställa att informationssäkerheten är utformad och implementeras inom utvecklingslivscykeln för Informationssystem**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			**SEPO15 - Säker utvecklingspolitik**
14.2.1	Säker utvecklingspolitik	Regler för utveckling av programvara och system skall fastställas och tillämpas på utvecklingen inom organisationen.	JA				X	X	En policy beskriver och fastställer ett ramverk för säkerhet i utvecklingsprocesser	STRATUS	
14.2.2	Förfaranden för kontroll av systemändringar	Ändringar av system inom utvecklingslivscykeln ska kontrolleras genom användning av formella förfaranden för kontroll av ändringar	JA				X		Standardändringar görs via arbetsflödet i plattformens orkestrator. Icke-standardiserade ändringar är hanteras av förändringsprocessen		
14.2.3	Teknisk granskning av ansökningar efter byte av operativ plattform	När driftsplattformar byts ut kan affärskritiska applikationer skall granskas och testas för att säkerställa att det inte finns någon negativ inverkan på organisationens verksamhet eller säkerhet	JA				X	X	Hårdvaru- och/eller systemuppgraderingar testas på pilotgrupper innan de tillämpas i produktionsmiljöer.	Process för uppdatering av systemet	
14.2.4	Restriktioner för ändringar av programvarupaket	Ändringar av programvarupaket skall motverkas och begränsas till nödvändiga ändringar, och alla ändringar skall kontrolleras strikt.	JA				X		Alla ändringar som rör skript och automatiska styrsystem loggas i en GIT	Inga ändringar i koden för de programvarupaket som används	
14.2.5	Principer för konstruktion av säkra system	Principer för konstruktion av säkra system skall fastställas, dokumenteras, underhållas och tillämpas på alla insatser för att införa informationssystem.	JA				X	X	Manus och automatiska styrsystem standardiseras och testas innan de sätts i produktion	Utbildning/medvetenhet	
14.2.6	Säker utvecklingsmiljö	Organisationer ska upprätta och på lämpligt sätt skydda säkra utvecklingsmiljöer för systemutvecklings- och integrationsinsatser som omfattar hela livscykeln för systemutveckling.	JA				X	X	Hantera genom AzureDevOps arbetsflöde och utvecklingsservrar	Nätverksarkitektur	
14.2.7	Outsourcad utveckling	Organisationen skall övervaka och kontrollera verksamheten hos systemutveckling på entreprenad	JA			X		X	Ett internt serviceavtal med utvecklingsenheterna övervakar och kontrollerar aktiviteter och externa tillämpningar av ISMS		
14.2.8	Testning av systemsäkerhet	Testning av säkerhetsfunktioner skall utföras under utveckling	JA				X	X	Testfaserna och efterlevnadstesterna hanteras i Azure DevOps-arbetsflödet		
14.2.9	Testning av systemacceptans	Program för acceptanstestning och tillhörande kriterier skall fastställas för nya informationssystem, uppgraderingar och nya versioner	JA				X	X		Resultat av sårbarhetsskanning	
14.3	**Testdata**	**Säkerställa skyddet av data som används för testning**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
14.3.1	Skydd av testdata	Testdata ska väljas ut noggrant, skyddas och kontrolleras.	JA				X	X	Hantera genom AzureDevOps arbetsflöde och utvecklingsservrar	Kopiera loggning	
15	**Relationer med leverantörer**										**SEP013-Förhållanden med leverantörer**
15.1	**Informationssäkerhet i leverantörsrelationer**	**Säkerställa skydd av organisationens tillgångar som är tillgängliga för leverantörer**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
15.1.1	Informationssäkerhetspolicy för leverantörsrelationer	Krav på informationssäkerhet för att minska riskerna i samband med med leverantörens tillgång till organisationens tillgångar skall överenskommas med leverantören och dokumenteras.	JA		X	X	X	X	X	Säkerhetspolicyn i leverantörsrelationer tar hänsyn till och beskriver säkerhetskraven och åtgärder som är nödvändiga för att uppfylla Cegids rättsliga, regulatoriska och avtalsenliga skyldigheter	
15.1.2	Hantering av säkerhet i leverantörsavtal	Alla relevanta informationssäkerhetskrav ska fastställas och avtalas med varje leverantör som kan få tillgång till, bearbeta, lagra, kommunicera eller tillhandahålla IT-infrastrukturkomponenter för information om organisationen	JA		X	X		X	X	Cegid säkerställer att dess leverantörer är involverade i säkerheten för den levererade tjänsten genom certifiering och avtalsenliga åtaganden	
15.1.3	Leverantörskedjan för informations- och kommunikationsteknik	Avtal med leverantörer ska innehålla krav på att hantera de informationssäkerhetsrisker som är förknippade med informations- och kommunikationstekniktjänster och produktförsörjningskedjan.	JA		X	X		X	X	Cegid säkerställer att dess leverantörer är involverade i säkerheten för den tjänst som levereras genom certifiering och avtalsenliga åtaganden För Talentsofts historiska verksamhet finns det inget utbud i samband med produktion, vilket är Quadrias ansvar. Detta krav har därför inte tagits med.	
15.2	**Ledning av tjänsteleveranser från leverantörer**	**Upprätthålla en överenskommen nivå av informationssäkerhet och service leverans i linje med leverantörsavtal**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**			
15.2.1	Övervakning och granskning av leverantörstjänster	Organisationer ska regelbundet övervaka, granska och kontrollera leverantörers leverans av tjänster	JA		X	X		X	X	Möten i styrkommittén för säkerhet planeras och organiseras med leverantörerna på återkommande basis. Revisioner gör det möjligt att bedöma utveckling och förändringar i avtalsramen	Protokoll från möte i säkerhetskommittén Kyndryl/Microsoft	
15.2.2	Hantera förändringar av leverantörstjänster	Förändringar i leverantörernas tillhandahållande av tjänster, inbegripet upprätthållande och förbättring av befintliga riktlinjer, förfaranden och kontroller för informationssäkerhet, ska hanteras med beaktande av hur kritisk den berörda affärsinformationen, de berörda systemen och de berörda processerna är. och ny bedömning av risker	JA		X	X		X			
16	**Hantering av incidenter inom informationssäkerhet**										**SEPS3-Hantering av säkerhetsincidenter**

16.1	**Hantering av incidenter och förbättringar av informationssäkerheten**	**Säkerställa en konsekvent och effektiv strategi för hantering av informationssäkerhetsincidenter, inklusive kommunikation om säkerhetshändelser och svagheter.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**		
16.1.1	Ansvarsområden och förfaranden	Ledningens ansvarsområden och förfaranden skall fastställas för att säkerställa en snabb, effektiv och ordnad reaktion på informationssäkerhet incidenter	JA	X		X	X	X		
16.1.2	Rapportering av informationssäkerhetshändelser	Informationssäkerhetshändelser skall rapporteras genom lämpliga	JA	X		X	X	X	Process för hantering av säkerhetsincidenter i enlighet med ISO 27035, inklusive rapportering av säkerhetsincidenten	
16.1.3	Rapportering av svagheter i informationssäkerheten	Anställda och entreprenörer som använder organisationens informationssystem och informationstjänster skall vara skyldiga att notera och rapportera alla observerade eller misstänkta brister i informationssäkerheten i system eller	JA	X		X	X	X	Förkvalificering av evenemanget Kvalificeringsfas Undersökning	
16.1.4	Bedömning av och beslut om informationssäkerhetshändelser	Informationssäkerhetshändelser ska bedömas och det ska beslutas om de ska klassificeras som informationssäkerhetsincidenter.	JA	X		X	X	X	Kommunikation/rapporterin g Bearbetning Återkoppling	Stratus
16.1.5	Åtgärder vid incidenter som rör informationssäkerhet	Informationssäkerhetsincidenter skall hanteras i enlighet med	JA	X		X	X	X	Avslutande av incidenten En RACI-matris fastställer roller och ansvar för varje fas En veckovis	
16.1.6	Lärdomar av incidenter som rör informationssäkerhet	Kunskaper från analys och lösning av informationssäkerhetsincidenter skall användas för att minska sannolikheten för eller effekterna av framtida incidenter.	JA	X		X	X	X	genomgång av incidenter genomförs	
16.1.7	Insamling av bevismaterial	Organisationen skall definiera och tillämpa förfaranden för identifiering, insamling, anskaffning och bevarande av information, som kan tjäna som bevis	JA	X		X	X	X		
17	**Informationssäkerhetsaspekter av kontinuitetshantering**									**SEIT25-SaaS krishantering**
17.1	**Kontinuitet i informationssäkerheten**	**Kontinuiteten i informationssäkerheten ska vara inbyggd i organisationens system för hantering av kontinuitet i verksamheten**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**		
17.1.1	Planering av kontinuitet för informationssäkerhet	Organisationen skall fastställa sina krav på informationssäkerhet och kontinuiteten i hanteringen av informationssäkerhet i o g y n n s a m m a situationer, t.ex. under en kris eller katastrof.	JA			X	X	X	En policy för kontinuitet i verksamheten utgör ett ramverk för organisationen och processerna för kontinuitet i informationssäkerheten. En "kod röd"-process reglerar krishanteringen	

17.1.2	Genomförande av kontinuitet i informationssäkerheten	Organisationen skall upprätta, dokumentera, införa och underhålla processer, förfaranden och kontroller för att säkerställa den erforderliga nivån av kontinuitet för informationssäkerhet under en ogynnsam situation	JA			X	X	X	Olika processer gör det möjligt att upprätthålla informationssäkerheten (säkerhetskopiering av data, motståndskraft hos infrastruktur och personalresurser, administration av säkra verktyg för distansproduktion)	Hantering av incidenter/kod röd
17.1.3	Verifiera, granska och utvärdera kontinuiteten i informationssäkerheten.	Organisationen skall regelbundet verifiera de etablerade och implementerade kontinuitetskontrollerna för informationssäkerhet för att säkerställa att de är giltiga och effektiva under ogynnsamma situationer.	JA			X	X	X	Kontinuiteten i informationssäkerheten bedöms på återkommande basis	
17.2	**Uppsägningar**	**Säkerställa tillgången till utrustning för informationsbehandling**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**		
17.2.1	Tillgång till utrustning för informationsbehandling	Anläggningar för informationsbehandling skall vara försedda med redundans som är tillräcklig för att uppfylla tillgänglighetskraven.	JA		X	X	X	X	Mekanismer för redundans och motståndskraft för arkitekturer och team är aktiva från början till slut. Det finns en ständig övervakning av dessa mekanismer.	SaaS-arkitekturdokument
18	**Överensstämmelse**									**SEPO10-Efterlevnad och revisionshantering**
18.1	**Överensstämmelse med rättsliga och avtalsmässiga krav**	**Undvika överträdelser av lagar, förordningar, föreskrifter eller avtal skyldigheter som rör informationssäkerhet och av eventuella säkerhetskrav.**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**		
18.1.1	Identifiering av tillämplig lagstiftning och avtalskrav	Alla relevanta krav i lagar, förordningar och avtal samt organisationens tillvägagångssätt för att uppfylla dessa krav skall uttryckligen identifieras, dokumenteras och hållas uppdaterade för varje informationssystem och för organisationen.	JA	X	X		X	X	Cegid Groups juridiska process definierar, dokumenterar och uppdaterar alla lagar, förordningar och avtal Krav som är tillämpliga på ISMS.	Rättslig process
18.1.2	Immateriella rättigheter	Lämpliga förfaranden skall införas för att säkerställa efterlevnad a v lagar, andra författningar och avtalskrav som rör immateriella rättigheter och användning av egenutvecklade programvaruprodukter.	JA	X	X		X	X	Cegid Cloud Factory har åtagit sig att säkerställa efterlevnad av lagar, förordningar och avtalskrav som rör immateriella rättigheter och användning av egenutvecklade programvaruprodukter. Programvaran köps in från kända och välrenommerade källor för att säkerställa att upphovsrätten respekteras.	Licensregister
18.1.3	Skydd av register	Registren ska skyddas mot förlust, förstörelse, förfalskning, obehörig åtkomst och obehörigt utlämnande, i enlighet med lagar och andra författningar, avtal och verksamhetskrav.	JA	X	X		X		Uppgifterna ska skyddas mot förlust, förstörelse, förfalskning, obehörig åtkomst och obehörigt offentliggörande.	
18.1.4	Sekretess och skydd av personligt identifierbar information	Sekretess och skydd av personligt identifierbar information ska säkerställs enligt kraven i relevant lagstiftning och relevanta föreskrifter i tillämpliga fall	JA	X	X		X	X	Den allmänna dataskyddsförordningen har varit tillämplig på tillämpningsområdet sedan den 25 maj 2018. I detta sammanhang har Cegid utsett ett dataskyddsombud som ansvarar för att övervaka ämnet i hela koncernen	
18.1.5	Reglering av kryptografiska kontroller	Kryptografiska kontroller ska användas i enlighet med alla relevanta avtal, lagar och andra författningar	JA					X	Cegid Cloud Factory följer tillämpliga avtal, lagar och förordningar som rör Kryptografi. Cegid varken importerar eller exporterar några kryptografiska lösningar.	
18.2	**Granskning av informationssäkerhet**	**Säkerställa att informationssäkerhet implementeras och drivs i enlighet med organisationens riktlinjer och förfaranden**	**Inklusive**	**LO**	**CO**	**BC**	**BLO DTR YCK**	**RA**		
18.2.1	Oberoende granskning av informationssäkerheten	Organisationens strategi för hantering av informationssäkerhet och dess genomförande (dvs. kontrollmål, kontroller, policyer, processer och förfaranden för informationssäkerhet) ska granskas oberoende med planerade intervall eller när betydande förändringar inträffar.	JA				X	X	Cegid Cloud Factory genomför en internrevision av informationssystemet minst en gång per år. En genomgång av ledningen planeras i slutet av	
18.2.2	Överensstämmelse med säkerhetspolicyer och säkerhetsstandarder	Chefer skall regelbundet kontrollera att informationsbehandling och förfaranden inom deras ansvarsområde överensstämmer med lämpliga säkerhetspolicyer, standarder och alla andra säkerhetsåtgärder. krav	JA					X		Indikatorer och mål för ISMS
18.2.3	Granskning av teknisk överensstämmelse	Informationssystemen skall regelbundet granskas med avseende på överensstämmelse med organisationens riktlinjer och standarder för informationssäkerhet	JA			X	X	X	En policy med pentester och teknisk granskning hjälper till att identifiera avvikelser	Skanningsrapport