cegid

Erklæring om anvendelighed ISO27001:2013

Version af 23/02/2023
Klassificering: Offentlig

Ændret af: Sikkerhedsteamet

ISO27001:2013

		Implementeret løsning	Beviser og leverancer
4	**Organisationens kontekst**		
4.1	Forståelse af organisationen og dens kontekst	Omfanget af SaaS Security Management System (SEPO12)	SELI030 - SOA
4.2	Forståelse af de interesserede parters behov og forventninger		
4.3	Fastlæggelse af omfanget af ledelsessystemet for informationssikkerhed		
4.4	Ledelsessystem for informationssikkerhed		
5	**Ledelse**		
5.1	Ledelse og engagement	Ledelse af styring, roller og ansvar for ISMS (SEPS4)	Tilsagnsbrev fra ledelsen
5.2	Politik		Referater af møder i informationssikkerhedsstrukturer
5.3	Organisatoriske roller, ansvar og beføjelser		
6	**Planlægning**		
6.1	Tiltag til håndtering af risici og muligheder	Risikovurdering og behandlingsproces (SEPS5)	Resultater af risikoanalyse og RTP
6.2	Mål for informationssikkerhed og planlægning for at nå dem		
7	**Støtte**		
7.1	Ressourcer	Sikkerhed for menneskelige ressourcer	HR-processer og -dokumenter
7.2	Kompetence		
7.3	Bevidsthed		
7.4	Kommunikation	(SEPO9) ISMS-kommunikationsproces	Sikkerhedsudvalgets møddereferater
7.5	Dokumenterede oplysninger		Elektronisk dokumenthåndteringsproces
8	**Betjening**		
8.1	Operationel planlægning og kontrol	Proces til styring af dokumentation (SEPS2)	Referat af møde i sikkerhedsudvalget
8.2	Risikovurdering af informationssikkerhed	Politik for kontrol, overvågning og forbedring	Resultater af risikoanalyse og risikohåndteringsplan
8.3	Behandling af informationssikkerhedsrisici	(SEPO17) Risikostyringsproces (SEPS5)	
9	**Evaluering af præstationer**		
9.1	Overvågning, måling, analyse og evaluering	Kontrol-, overvågnings- og forbedringspolitik (SEPO17)	Sikkerhedsudvalgets møddereferater
9.2	Intern revision	Compliance- og revisionsstyring (SEPO10)	Revisionsplanlægning
9.3	Ledelsens gennemgang	Ledelse af styring, roller og ansvar for ISMS (SEPS4)	Ledelsens gennemgang
10	**Forbedring**		
10.1	Afvigelser og korrigerende handlinger	Compliance og revisionsstyring (SEPO10)	Planlægning af revision
10.2	Kontinuerlig forbedring	Politik for kontrol, overvågning og forbedring (SEPO17)	Referater fra sikkerhedsudvalgets møder Referater fra ledelsens gennemgang

LO = Juridiske forpligtelser
CO = Kontraktlige forpligtelser
BC = Forretningsforpligtelse
BP = Bedste praksisser
RA = Risikoanalyse

Implementeringen af de sikkerhedskontroller, der er defineret i erklæringen om anvendelighed, har til formål at reducere de sikkerhedsrisici, der kan være i ISMS'et.

ISO27001:2013 Bilag A

Krav			Inkluderet	LO	CO	BC	BP	RA	Implementeret løsning	Beviser og leverancer
5	**Politikker for informationssikkerhed**									**SEPO16 - Cegid Cloud Factory informationssikkerhedspolitik**
	5.1	**Ledelsens retningslinjer for informationssikkerhed**	**Give ledelsen retning og støtte til information sikkerhed i overensstemmelse med forretningskrav og relevante love og bestemmelser**	**Inkluderet**	**LO**	**CO**	**BC**	**BP**	**RA**	
5.1.1		Politikker for informationssikkerhed	Et sæt politikker for informationssikkerhed skal defineres, godkendes af ledelsen, offentliggøres og kommunikeres til medarbejderne og relevante eksterne parter.	JA				X	X	Der er udarbejdet en informationssikkerhedspolitik Den gennemgås årligt og godkendes af Cloud Services Department.
5.1.2		Gennemgang af politikkerne for informationssikkerhed	Politikkerne for informationssikkerhed skal gennemgås på planlagte tidspunkter. intervaller, eller hvis der sker væsentlige ændringer, for at sikre deres fortsatte egnethed, tilstrækkelighed og effektivitet.	JA				X		Tilsagnsbrev fra ledelsen
6	**Organisering af informationssikkerhed**									**SEPS4 - Ledelse af styring, roller og ansvar i forbindelse med ISMS**
	6.1	**Intern organisation**	**Etablere en ledelsesramme til at initiere og kontrollere implementering og drift af informationssikkerhed i organisationen**	**Inkluderet**	**LO**	**CO**	**BC**	**BP**	**RA**	
6.1.1		Roller og ansvar for informationssikkerhed	Alle ansvarsområder for informationssikkerhed skal defineres og fordeles.	JA				X		Koncernens sikkerhedsteam er organiseret på tværs af funktioner. Det er hierarkisk og operationelt uafhængigt af ISMS-aktiviteterne.
6.1.2		Adskillelse af opgaver	Modstridende opgaver og ansvarsområder skal adskilles for at reducere mulighederne for uautoriserede eller utilsigtede ændring eller misbrug af nogen af organisationens aktiver.	JA				X		DevOps-lignende organisering af opgaver og teams
6.1.3		Kontakt med myndigheder	Der skal opretholdes passende kontakter med relevante myndigheder.	JA		X		X		Cegids sikkerhedsteam har regelmæssige udvekslinger med CNIL og ANSSI.
6.1.4		Kontakt med særlige interessegrupper	Passende kontakter med særlige interessegrupper eller andre specialister sikkerhedsfora og faglige sammenslutninger skal opretholdes.	JA				X		Medarbejderne i Cegid Security Team er medlemmer af følgende organisationer: CLUSIR / CLUSIF /Club ISO 27001
6.1.5		Informationssikkerhed i projektledelse	Informationssikkerhed skal behandles i projektledelse, uanset hvilken type projekt der er tale om.	JA				X	X	Organisering af teams og processer i agil tilstand (Azure DevOps) til overvejelse af sikkerhed i infrastruktur og udvikling i alle projekter relateret til ISMS
	6.2	**Mobile enheder og telearbejde**	**Sørg for sikkerheden ved telearbejde og brug af mobile enheder**	**Inkluderet**	**LO**	**CO**	**BC**	**BP**	**RA**	**SEOP7- Mobile enheder og telearbejde**
6.2.1		Politik for mobile enheder Sikkerhedsforanstaltninger for at håndtere	Der skal vedtages en politik og understøttende de risici, der er forbundet med at bruge mobile enheder	JA				X	X	Kryptering af medarbejdernes bærbare diske Filtre til beskyttelse af personlige oplysninger MFA og VPN i mobilitetssituationer
6.2.2		Telearbejde	Der skal implementeres en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der tilgås, behandles eller opbevares på distancearbejdspladser.	JA				X	X	
7	**Sikkerhed for menneskelige ressourcer**									**SEPO9 - Sikkerhed for menneskelige ressourcer**

Organisering af AzurDevOps-teams
Sikkert udviklingscharter Cloud/Dev
intern serviceaftale Sikkerhed i infrastrukturprojekter

7.1	**Før ansættelse**	**Sørg for, at medarbejdere og entreprenører forstår deres ansvarsområder og er egnede til de roller, som de er taget i betragtning.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
7.1.1	Screening	Baggrundskontrol af alle kandidater til ansættelse skal udføres i overensstemmelse med relevante love, regler og etik o g skal stå i et rimeligt forhold til forretningskravene, klassifikationen af de oplysninger, der skal tilgås, og de opfattede risici.	JA			X		X	Et tjek af referencer (eksamensbeviser, straffeattest osv.) udføres af koncernens rekrutteringsteam.	Koncernens HR-rekrutteringsprocedurer Aftale om SaaS/HR-tjenester
7.1.2	Vilkår og betingelser for ansættelse	De kontraktlige aftaler med medarbejdere og entreprenører skal angive deres og organisationens ansvar for information sikkerhed	JA			X		X	Ansættelseskontrakten, som de nye medarbejdere underskriver, indeholder en fortrolighedsklausul og en konkurrenceklausul.	
7.2	**Under ansættelsen**	**Sikre, at medarbejdere og entreprenører er opmærksomme på og opfylde deres ansvar for informationssikkerhed**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
7.2.1	Ledelsens ansvar	Ledelsen skal kræve, at alle medarbejdere og entreprenører anvender informationssikkerhed i overensstemmelse med organisationens etablerede politikker og procedurer.	JA				X		Formelt engagement fra Cloud Services-afdelingen gennem de forskellige udvalg, møder og kommunikation omkring sikkerhed og ISMS.	Tilsagnsbrev fra ledelsen
7.2.2	Bevidsthed om informationssikkerhed, uddannelse og træning	Alle medarbejdere i organisationen og, hvor det er relevant, entreprenører skal modtage passende læring og bevidsthedstræning og regelmæssige opdateringer i organisationens politikker og procedurer, som er relevante for deres jobfunktion.	JA			X	X	X	Sikkerhedstræning for nye medarbejdere gennemføres systematisk Der udarbejdes e n årlig bevidsthedsplan	Uddannelsesplaner og -indhold Bevidstgørende indhold og resultater
7.2.3	Disciplinær proces	Der skal være en formel og kommunikeret disciplinær proces på plads til at gribe ind over for medarbejdere, der har begået en brud på informationssikkerheden.	JA			X	X	X	Der kan indledes en disciplinær proces i tilfælde af brud på ISSP eller charteret for brug af IT-værktøjer og udstyr.	Interne regler Ansættelseskontrakt Udvidet fortrolighedsklausul
7.3	**Opsigelse og ændring af ansættelsesforhold**	**Beskytte organisationens interesser som en del af processen med at ændre eller opsige ansættelsen.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
7.3.1	Opsigelse eller ændring af ansættelsesansvar	Ansvar og pligter i forbindelse med informationssikkerhed, som forbliver gyldige efter opsigelse eller ændring af ansættelsesforhold, skal defineres, kommunikeres til medarbejderen eller leverandøren og håndhæves.	JA	X	X			X	Medarbejderne informeres om deres ansvar i tilfælde af en ændring, opsigelse eller kontraktudløb af deres HR-korrespondent.	Ansættelseskontrakt
8	**Forvaltning af aktiver**									**SEPO5-Asset management**
8.1	**Ansvar for aktiver**	**Identificere organisatoriske aktiver og definere passende ansvar for beskyttelse**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
8.1.1	Opgørelse over aktiver	Aktiver forbundet med informations- og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes en fortegnelse over disse aktiver. udarbejdet og vedligeholdt.	JA				X	X	Fortegnelsen over aktiver gennemgås og opdateres i risikoanalyseværktøjet.	Liste over aktiver
8.1.2	Ejerskab af aktiver	Aktiver, der opbevares i fortegnelsen, skal være ejet.	JA				X	X	Aktiverne er Cloud Services-afdelingens ejendom.	Definere ejeren af fysiske aktiver og ejerens rolle
8.1.3	Acceptabel brug af aktiver	Regler for acceptabel brug af information og af aktiver forbundet med information og informationsbehandlingsfaciliteter skal være identificeret, dokumenteret og implementeret.	JA		X		X	X	En politik for acceptabel brug er blevet udarbejdet og kommunikeret til medarbejderne.	Politik for acceptabel brug
8.1.4	Afkast af aktiver	Alle medarbejdere og eksterne brugere skal aflevere alle de organisatoriske aktiver, de er i besiddelse af, når deres ansættelsesforhold ophører. ansættelse, kontrakt eller aftale.	JA		X		X		Returnering af aktiver i henhold til opgørelsen af medarbejderens opsigelsesformular under lederens ansvar	Cegid Group Human Resources afdelingsark
8.2	**Klassificering af information**	**Sikre, at information får et passende niveau af beskyttelse i overensstemmelse med dens betydning for organisation.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		**SEPS2-Dokumentationsstyring**
8.2.1	Klassificering af information	Information skal klassificeres i forhold til lovkrav, værdi, kritikalitet og følsomhed over for uautoriseret offentliggørelse eller ændring.	JA				X		Oplysningerne er klassificeret efter 5 kriterier	RCNT7- Klientdiskens livscyklus
8.2.2	Mærkning af information	Et passende sæt procedurer for informationsmærkning skal udvikles og implementeres i overensstemmelse med den informationsklassifikationsordning, som organisationen har vedtaget.	JA				X		Alle aktiver (dokumenter, `kundeaktiver`) er underlagt politikken for forvaltning af aktiver. Denne politik tager højde for klassifikationsniveauet for aktiver, der er forbundet med deres udbredelsesniveau og den kryptering, der er nødvendig for deres udbredelse.	
8.2.3	Håndtering af aktiver	Procedurer for håndtering af aktiver skal udvikles og implementeres i overensstemmelse med den informationsklassifikationsordning, der er vedtaget af organisationen.	JA				X			
8.3	**Håndtering af medier**	**Forhindre uautoriseret offentliggørelse, ændring, fjernelse eller ødelæggelse af oplysninger, der er gemt på medier.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
8.3.1	Håndtering af flytbare medier	Der skal implementeres procedurer for håndtering af flytbare medier i overensstemmelse med den klassifikationsordning, der er vedtaget af organisation.	JA			X			Begrænsning af medarbejdernes brug af flytbare medier (USB) DC-leverandør Procedure for flytbare medier til opbevaring af kundedata	Charter for brug af IS-værktøjer
8.3.2	Bortskaffelse af medier	Medier skal bortskaffes på sikker vis, når de ikke længere er nødvendige, ved hjælp af formelle procedurer.	JA	X	X	X		X	Formatering på lavt niveau af lagringsmedier på medarbejdernes arbejdsstationer DC-leverandørernes fysiske destruktion af kundens datalagringsmedier	Bevis for datadestruktion ved SaaS-produktion/adgang til makulator
8.3.3	Overførsel af fysiske medier	Medier, der indeholder information, skal beskyttes mod uautoriseret adgang, misbrug eller forvanskning under transport.	JA		X	X		X	Kryptering af flytbare lagringsmedier i tilfælde af overførsel af kundedata Sporing af kvitteringer og forsendelser med Chronopost	RCNT7- Klientdiskens livscyklus
9	**Adgangskontrol**									**SEPO1-Adgangskontrol**
9.1	**Forretningskrav til adgangskontrol**	**Begræns adgangen til information og informationsbehandling faciliteter**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		

9.1.1	Politik for adgangskontrol	En adgangskontrolpolitik skal etableres, dokumenteres og revideres baseret på forretnings- og informationssikkerhedskrav.	JA		X		X	X	X	Politik for adgangskontrol gennemgås årligt	
9.1.2	Adgang til netværk og netværkstjenester	Brugere skal kun have adgang til det netværk og de netværkstjenester, som de specifikt er blevet autoriseret til at bruge.	JA				X	X		En rettighedsmatrix sikrer styringen af brugerrettigheder og adgang til ressourcer. Denne matrix revideres mindst en gang om året.	Rettighedsmatrix
9.2	**Administration af brugeradgang**	**Sikre autoriseret brugeradgang og forhindre uautoriseret adgang adgang til systemer og tjenester**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**			
9.2.1	Registrering og afregistrering af brugere	En formel brugerregistrerings- og afregistreringsproces skal være implementeret for at gøre det muligt at tildele adgangsrettigheder.	JA		X	X	X	X	X	Administration af brugerregistreringer/afregistreringer i vores Cloud Factory-platforms orkestreringsværktøj	Serviceanmodning og workflow stratus
9.2.2	Tildeling af brugeradgang	Der skal implementeres en formel proces for tildeling af brugeradgang for at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	JA		X	X	X	X	X		
9.2.3	Administration af privilegerede adgangsrettigheder	Tildeling og brug af privilegerede adgangsrettigheder skal begrænses. og kontrolleret.	JA				X	X	X	Tildeling af rettigheder efter brugergruppe til de applikationer, der skal bruges	Cegid Cloud Factory rettighedsmatrix
9.2.4	Håndtering af hemmelige autentificeringsoplysninger for brugere	Tildelingen af hemmelige autentificeringsoplysninger skal kontrolleres. gennem en formel ledelsesproces.	JA				X	X	X	Godkendelsesoplysninger kommunikeres i henhold til en formaliseret HR-proces. Det kommunikeres kun, når medarbejderens personnummer er tildelt.	
9.2.5	Gennemgang af brugernes adgangsrettigheder	Ejere af aktiver skal gennemgå brugernes adgangsrettigheder med jævne mellemrum.	JA				X	X	X	Lederne gennemfører en revalidering af teamrettighederne hvert kvartal.	Kvartalsvis liste over revalidering af rettigheder valideret af ledere
9.2.6	Fjernelse eller justering af adgangsrettigheder	Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal fjernes ved ophør af deres ansættelse, kontrakt eller aftale, eller justeres ved ændringer.	JA				X	X	X	Når vi modtager en bekræftelse fra vores HR-værktøjer på, at ansættelsesperioden er afsluttet, behandles anmodningen i vores orkestreringsværktøj.	Serviceanmodning og Stratus Workflow
9.3	**Brugernes ansvar**	**Gør brugerne ansvarlige for at beskytte deres oplysninger om autentificering.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**			
9.3.1	Brug af hemmelige autentificeringsoplysninger	Brugerne skal følge organisationens praksis i forbindelse med brugen af af hemmelig autentificeringsinformation	JA				X	X	X	Regler for brug af hemmelige oplysninger er klart defineret i charteret for brug af it-værktøjer.	SENT14- Politik for administration af adgangskoder Politik for acceptabel brug
9.4	**Adgangskontrol til systemer og applikationer**	**forhindre uautoriseret adgang til systemer og applikationer**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**			
9.4.1	Begrænsning af adgang til information	Adgang til informations- og applikationssystemfunktioner skal være begrænset i overensstemmelse med adgangskontrolpolitikken.	JA				X	X		Rettigheds- og adgangsmatrixen definerer adgang efter forretningsgruppe og efter applikation	Rettighedsmatrix
9.4.2	Sikring af log-on-procedurer	Hvor det kræves af adgangskontrolpolitikken, skal adgangen til systemer og applikationer kontrolleres af en sikker log-on-procedure.	JA					X	X	Cegid Cloud Factory-medarbejdernes forbindelse til produktionsmiljøerne sker via en P.A.M. (Bastion) og via et sikkert fjernadgangssystem (RDM).	PAM-brugervejledning
9.4.3	System til administration af adgangskoder	Systemer til administration af adgangskoder skal være interaktive og skal sikre adgangskoder af høj kvalitet.	JA					X	X	En politik for administration af adgangskoder er defineret for Cegid Cloud Factory-medarbejdere såvel som for kunder. ved hjælp af Cegid SaaS-applikationer	SENT14- Politik for administration af adgangskoder
9.4.4	Brug af privilegerede hjælpeprogrammer	Brugen af hjælpeprogrammer, der kan tilsidesætte system- og applikationskontroller, skal begrænses og kontrolleres nøje.	JA							Et værktøj til administration og begrænsning af skygge-IT bruges til at kontrollere brugen af uautoriserede programmer og applikationer.	Rettighedsmatrix
9.4.5	Adgangskontrol til programmets kildekode	Adgang til programmets kildekode skal begrænses	JA					X	X	Manuskripter opbevares i sikre områder, som kun er tilgængelige for produktionsholdet.	Liste over autoriserede brugere
10	**Kryptografi**										**SEPO12-Informationsoverførsel og kryptering**
10.1	**Kryptografiske kontroller**	**Sikre korrekt og effektiv brug af kryptografi til at beskytte fortroligheden, autenticiteten og/eller integriteten af information.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**			
10.1.1	Politik for brug af kryptografiske kontroller	Der skal udvikles og implementeres en politik for brugen af kryptografiske kontroller til beskyttelse af information.	JA		X	X	X	X		Politik for kryptering af flows og data Denne politik gennemgås regelmæssigt for at give det bedste sikkerhedsniveau i overensstemmelse med standard god praksis.	Årlig gennemgang af denne politik
10.1.2	Nøglehåndtering	En politik for brug, beskyttelse og levetid af kryptografiske nøgler skal udvikles og implementeres gennem hele deres livscyklus.	JA				X	X		Administration af certifikater til HTTPS-adgang i overensstemmelse med god praksis Anerkendt certificeringsmyndighed, opbevaring af nøgler i en nøgleboks Administration af krypteringsnøgler til data gemt i datacentrene	Certifikater administreret af Cegid og udstedt af en anerkendt CA Nøgleadministration af Cegid (Private Cloud) eller af udbyderen (Public Cloud)
11	**Fysisk og miljømæssig sikkerhed**										**SEPO1 Adgangskontrol / SEPO6 Fysisk og miljømæssig sikkerhed**
11.1	**Sikre områder**	**Forhindre uautoriseret fysisk adgang, beskadigelse og indblanding i organisationens information og faciliteter til informationsbehandling.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**			
11.1.1	Fysisk sikkerhedsperimeter	Sikkerhedsperimetre skal defineres og bruges til at beskytte områder, der indeholder enten følsomme eller kritiske oplysninger og informationer. Forarbejdningsanlæg	JA					X		Drifts- og produktionsteams befinder sig i fysisk isolerede lokaler.	Serviceaftale med understøttende forsyningsselskaber
11.1.2	Fysisk adgangskontrol	Sikrede områder skal være beskyttet af passende adgangskontrol for at sikre, at kun autoriseret personale har adgang	JA					X	X	Sikker adgang til produktionslokalerne med badge kun for autoriserede medarbejdere	Månedlig adgangskontrol-liste
11.1.3	Sikring af kontorer, lokaler og faciliteter	Fysisk sikkerhed for kontorer, lokaler og faciliteter skal være designet og anvendt	JA					X	X	Låste døre med alarmer i tilfælde af længerevarende åbning	
11.1.4	Beskyttelse mod eksterne og miljømæssige trusler	Fysiske beskyttelsesforanstaltninger mod naturkatastrofer, ondsindede angreb eller ulykker skal designes og implementeres.	JA			X	X	X	X	Beskyttelse af den bygning, der huser produktionsteamet Strømforsyning, aircondition, netværkskabler osv.	
11.1.5	Arbejde i sikrede områder	Der skal udarbejdes og anvendes procedurer for arbejde i sikrede områder.	JA						X	Beskyttelse af den bygning, der huser produktionsteamet Strømforsyning, aircondition, netværkskabler osv. I Talentsofts mangeårige lokaler arbejdes der ikke i sikrede områder. Dette krav er derfor ikke	Intern leverandørserviceaftale med General Services
11.1.6	Levering og læsning	Adgangssteder som f.eks. leverings- og læsseområder og andre steder, hvor uautoriserede personer kan komme ind i lokalerne, skal kontrolleres og om muligt isoleres fra informationsbehandlingen. faciliteter til at undgå uautoriseret adgang	JA					X	X	Leveringer sker til bygningens sikkerheds-pc. Kontrollen udføres af et privat sikkerhedsfirma under Cegids SG's ansvar.	
11.2	**Udstyr**	**Forebygge tab, beskadigelse, tyveri eller kompromittering af aktiver og afbrydelse af organisationens drift.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**			

11.2.1	Placering og beskyttelse af udstyr	Udstyr skal placeres og beskyttes for at reducere risici fra miljømæssige trusler og farer og muligheder for uautoriseret adgang.	JA					X	X	Følsomt udstyr opbevares i sikre lokaler	Intern leverandørserviceaftale med General Services
11.2.2	Understøttende forsyningsselskaber	Udstyret skal være beskyttet mod strømsvigt og andre afbrydelser forårsaget af fejl i understøttende forsyningsanlæg.	JA						X	Uafhængigt strømforsyningssystem er operationelt i tilfælde af fejl i det generelle system	Vedligeholdelseskontrakt med inverterleverandør
11.2.3	Sikkerhed ved kabling	Strøm- og telekommunikationskabler, der transporterer data eller understøtter Informationstjenester skal beskyttes mod aflytning, forstyrrelse eller beskadigelse.	JA					X	X	SaaS-produktions-LAN'et er et switchet netværk, der er fysisk uafhængigt af resten af virksomheden.	Konfiguration af SaaS-netværksarkitektur og skema
11.2.4	Vedligeholdelse af udstyr	Udstyret skal vedligeholdes korrekt for at sikre dets fortsatte tilgængelighed og integritet	JA					X	X	Vedligeholdelsen af internt udstyr og samarbejdspartnere er udliciteret og formaliseret i en kontrakt. af IT-afdelingen	Intern leverandørserviceaftale med IT-afdelingen
11.2.5	Fjernelse af aktiver	Udstyr, information eller software må ikke tages med væk fra stedet uden at forhåndsgodkendelse	JA						X	Formaliseret i charter for brug af IT-værktøjer og -ressourcer	
11.2.6	Sikkerhed for udstyr og aktiver uden for lokalerne	Der skal anvendes sikkerhed på off-site aktiver under hensyntagen til forskellige risici ved at arbejde uden for organisationens lokaler.	JA					X	X	Diskkryptering, antivirus, sikker fjernforbindelse via access gateway og/eller VPN	Intern leverandørserviceaftale med IT-afdelingen
11.2.7	Sikker bortskaffelse eller genbrug af udstyr	Alt udstyr, der indeholder lagringsmedier, skal kontrolleres for at sikre, at alle følsomme data og licenseret software er fjernet eller sikkert overskrevet før bortskaffelse eller genbrug.	JA		X	X	X	X	X	Destruktion af medier, der indeholder kundedata eller er relateret til sådanne data (medarbejdernes arbejdsstationer)	Bevis for destruktion af data gennem Cloud Contract SaaS-produktion
11.2.8	Uovervåget brugerudstyr	Brugere skal sikre, at udstyr, der ikke er under opsyn, har passende beskyttelse	JA					X	X	Tyverisikringskabel på medarbejdernes arbejdsstationer	Skærme låses efter 15 minutter (AD-strategi)
11.2.9	Politik for ryddet skrivebord og ryddet skærm	Der skal være en klar skrivebordspolitik for papirer og flytbare lagringsmedier og en klar skærmpolitik for informationsbehandlingsfaciliteter. vedtaget	JA					X		Opbevaring af dokumenter i et særligt samarbejdsrum Individuelt opbevaringsskab - Makulator til dokumenter, der skal bortskaffes Automatisk låsning af sessioner i tilfælde af en længere periode med inaktivitet	
12	**Operationel sikkerhed**										**SEPO4 Operationel sikkerhed**
12.1	**Operationelle procedurer og ansvarsområder**	**Sikre korrekt og sikker håndtering af information Forarbejdningsanlæg**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**			
12.1.1	Dokumenterede driftsprocedurer	Driftsprocedurer skal dokumenteres og gøres tilgængelige for alle brugere, der har brug for dem	JA					X	X	Alle driftsprocedurer er dokumenteret og tilgængelige for alle SaaS-medarbejdere i EDM.	Proces for elektronisk dokumenthåndtering
12.1.2	Forandringsledelse	Ændringer i organisation, forretningsprocesser, information behandlingsfaciliteter og systemer, der påvirker informationssikkerheden, skal kontrolleres.	JA					X	X	Der er planlagt et ugentligt møde om forandringsledelse	Referater og håndtering af ændringer i Inside

12.1.3	Kapacitetsstyring	Ressourceforbruget skal overvåges, afstemmes og fremskrives. af fremtidige kapacitetsbehov for at sikre den nødvendige systemydelse	JA			X	X	X	Løbende overvågning af ressourceallokering Månedligt udvalg om infrastruktur og dimensionering af ressourcer	Centreon overvågningskonsol Referat af kapacitetsplanlægningsmøde Tilpasning af HR til aktiviteten
12.1.4	Adskillelse af udviklings-, test- og driftsmiljøer	Udviklings-, test- og driftsmiljøer skal adskilles for at reducere risikoen for uautoriseret adgang til eller ændringer af driftsmiljø	JA			X	X	X	Segregering gennem automatiseret workflow i Azure DevOps	Netværksarkitektur
12.2	**Beskyttelse mod malware**	**Sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
12.2.1	Kontrol mod malware	Der skal implementeres kontroller til detektering, forebyggelse og gendannelse for at beskytte mod malware, kombineret med passende bruger- og bevidsthed	JA				X	X	Centraliseret og administreret antivirus/antimalware til alle ressourcer	Antiviral konsol (opdatering af dokumentet skal ses)
12.3	**Sikkerhedskopiering**	**Beskyt mod tab af data**	**Inkluderet**	**LO**	**BO**	**BC**	**BLO DTR YK**	**RA**		
12.3.1	Sikkerhedskopiering af oplysninger	Sikkerhedskopier af information, software og systembilleder skal tages og testes regelmæssigt i overensstemmelse med en aftalt sikkerhedskopieringspolitik.	JA					X	Backup-politikken tager højde for det specifikke ved hver kundes tilbud. Den tager højde for tilgængelighed, integritet og opbevaring.	Backup-rapporter
12.4	**Logning og overvågning**	**Registrer begivenheder og generer beviser.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
12.4.1	Logning af hændelser	Hændelseslogfiler, der registrerer brugeraktiviteter, undtagelser, fejl og informationssikkerhedshændelser, skal produceres, opbevares og regelmæssigt gennemgås.	JA	X	X	X	X	X	Informationssikkerhedshændelser centraliseres i et logsamlingsværktøj. Dette værktøj er styret af en veldefineret politik	Konsoller til centralisering af logfiler (Splunk)
12.4.2	Beskyttelse af logoplysninger	Logningsfaciliteter og logningsoplysninger skal beskyttes mod Manipulation og uautoriseret adgang	JA	X			X	X	Loghåndteringsværktøjet er hostet i en sikker arkitektur (redundans, kryptering af flows og diske), adgangsstyring, backup)	Konsoller til centralisering af logfiler (Splunk)
12.4.3	Administrator- og operatørlogfiler	Systemadministratorens og systemoperatørens aktiviteter skal logges og logfilerne beskyttes og gennemgås regelmæssigt.	JA		X		X	X	En automatisk rapport over administrator- og operatørlogfiler produceres hver måned.	Rapport om administratorkonti (Splunk)
12.4.4	Synkronisering af ur	Urene for alle relevante informationsbehandlingssystemer inden for en organisation eller et sikkerhedsdomæne skal synkroniseres til et enkelt reference tidskilde	JA		X		X	X	En NTP-synkronisering er konfigureret på alle aktiver.	Gruppestrategier og NTP-dokument
12.5	**Kontrol af driftssoftware**	**Sikre integriteten af de operationelle systemer**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
12.5.1	Installation af software på driftssystemer	Der skal implementeres procedurer til at kontrollere installationen af software på driftssystemer.	JA				X	X	Et værktøj og en centraliseret konsol muliggør lagerstyring af software i drift. Installationsskabeloner bruges til konfiguration af virtuelle servere.	Konsoller til softwareopgørelse
12.6	**Håndtering af tekniske sårbarheder**	**Forhindre udnyttelse af tekniske sårbarheder**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		**Operationel sikkerhed (OPSEU4)**
12.6.1	Håndtering af teknisk sårbarhed	Information om tekniske sårbarheder i anvendte informationssystemer skal indhentes rettidigt, organisationens eksponering for sådanne sårbarheder skal evalueres, og der skal træffes passende foranstaltninger. taget for at håndtere den tilknyttede risiko	JA				X	X	Sårbarhedsstyring sker gennem et scanningsværktøj og gennem advarsler fra CERT'er Politik for håndtering af disse sårbarheder efter omfang i eskaleringstilstand	Referater af IS-sikkerhedsovervågningsmøder
12.6.2	Begrænsninger på softwareinstallation	Regler for brugernes installation af software skal være etableret og implementeret	JA				X	X	Politik for afsløring af skygge-IT Værktøjer på medarbejdernes arbejdsstationer	Charter for brug af værktøjer
12.7	**Overvejelser om revision af informationssystemer**	**Minimere revisionsaktiviteternes indvirkning på driften systemer**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		**Operationel sikkerhed (OPSEU4)**
12.7.1	Revisionskontrol af informationssystemer	Auditkrav og aktiviteter, der involverer verifikation af operationelle systemer, skal planlægges omhyggeligt og aftales for at minimere forstyrrelser. til forretningsprocesser	JA				X	X	De forskellige politikker (Scan) og aftaler (Pentest) tager højde for forretningsområdernes aktivitetsperioder for at minimere påvirkningen.	Skabeloner til revisions- og testaftaler
13	**Kommunikationssikkerhed**									**SEPO14 - Styring af netværkssikkerhed**
13.1	**Administration af netværkssikkerhed**	**Sikre beskyttelse af informationer i netværk og deres understøttende faciliteter til informationsbehandling**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
13.1.1	Kontrol af netværk	Netværk skal administreres og kontrolleres for at beskytte information i systemer og applikationer.	JA				X	X	Netværk og links overvåges af monitoreringsværktøjer. Adgang spores og kontrolleres	Procedure for adskillelse af rettigheder og teams. Adgangskontrol og logfiler på udstyr. Redundans af teams, udstyr og ressourcer. Intern leverandør - IT-afdelingens serviceaftale En serviceaftale, der dækker servicegarantien, anvendes med IT-afdelingen for LAN- og WAN-delen Netværkspartitionering ved at oprette DMZ'er og VLAN'er. Netværk og links overvåges live af monitoreringsværktøjer.
13.1.2	Sikkerhed for netværkstjenester	Sikkerhedsmekanismer, serviceniveauer og styringskrav for alle netværkstjenester skal identificeres og inkluderes i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller outsourcet	JA				X	X	En intern serviceaftale formaliseres årligt med IT-afdelingen Den tager højde for netværkssikkerhed	Netværk og links overvåges live af monitoreringsværktøjer.
13.1.3	Segregering i netværk	Grupper af informationstjenester, brugere og informationssystemer skal være adskilt på netværk	JA				X	X	Opdeling af netværk ved at oprette DMZ'er og VLAN'er.	Dokumenter om netværksarkitektur
13.2	**Overførsel af information**	**Opretholde sikkerheden for information, der overføres inden for en organisation og med enhver ekstern enhed.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		**SEPO2- Informationsoverførsel og kryptering**
13.2.1	Politikker og procedurer for informationsoverførsel	Der skal være formelle overførselspolitikker, -procedurer og -kontroller på plads for at beskytte overførslen af oplysninger gennem brugen af alle typer af kommunikationsfaciliteter	JA				X	X	Der er udarbejdet en politik med regler for kryptering og kommunikationssikkerhed. Den revideres med jævne mellemrum.	
13.2.2	Aftaler om overførsel af information	Aftalerne skal omfatte sikker overførsel af forretningsoplysninger. mellem organisationen og eksterne parter	JA			X	X	X	De sikre udvekslingsprotokoller, der bruges med tredjeparter, gør det muligt at garantere integriteten, fortrolighed og ikke-afvisning af information	

13.2.3	Elektroniske meddelelser	Oplysninger, der indgår i elektroniske meddelelser, skal på passende vis beskyttet	JA				X	X	E-mail bruger kun sikre processer (flow, autentificering)	Konfiguration af e-mailserver
13.2.4	Aftaler om fortrolighed eller hemmeligholdelse	Krav til fortrolighedsforpligtelser eller hemmeligholdelsesaftaler afspejler organisationens behov for beskyttelse af information skal identificeres, regelmæssigt revideres og dokumenteres.	JA			X		X	X	Alle Cegid-medarbejdere, der arbejder med fortrolige data, underskriver en fortrolighedsaftale uden tidsbegrænsning, der indebærer disciplinære foranstaltninger eller retsforfølgelse i tilfælde af manglende overholdelse.	HR-processer
14	**Anskaffelse, udvikling og vedligeholdelse**									**SEPO8-Informationssikkerhedspolitik i projektledelse**
14.1	**Sikkerhedskrav til informationssystemer**	**Sikre, at informationssikkerhed er en integreret del af informationssystemer på tværs af hele livscyklussen. Dette omfatter også kravene til informationssystemer, som levere tjenester over offentlige netværk.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		**SEPO2- Informationsoverførsel og kryptering**
14.1.1	Analyse og specifikation af krav til informationssikkerhed	De informationssikkerhedsrelaterede krav skal indgå i kravene til nye informationssystemer eller forbedringer til eksisterende informationssystemer	JA				X	X	Formaliserede sikkerhedsprocedurer er integreret i alle projekter og i hele projektets livscyklus.	Spørgeskemaer om projektsikkerhedskrav
14.1.2	Sikring af applikationstjenester på offentlige netværk	Oplysninger, der er involveret i applikationstjenester, der passerer over offentlige netværk, skal beskyttes mod svigagtig aktivitet, kontrakttvister og uautoriseret offentliggørelse og ændring.	JA		X		X	X	Perimeterbeskyttelse af offentlig netværksadgang (Firewall, IDS/IPS-probe) Kryptering af flows med certifikater udstedt af et anerkendt certificeringsorgan; nøglerne opbevares i et digitalt pengeskab.	Politik for informationsoverførsel og kryptering
14.1.3	Beskyttelse af applikationstjenesters transaktioner	Oplysninger, der indgår i applikationstjenestetransaktioner, skal beskyttes for at forhindre ufuldstændig transmission, fejlrouting, uautoriseret ændring af meddelelser og uautoriseret offentliggørelse, uautoriseret kopiering eller afspilning af beskeder.	JA				X	X	Brug af sikre protokoller, der sikrer fuldstændig transmission uden mulig ændring af oplysningerne og forbyder uautoriseret ændring, uautoriseret offentliggørelse og uautoriseret kopiering.	
14.2	**Sikkerhed i udviklings- og supportprocesser**	**Sikre, at informationssikkerheden er designet og implementeret i udviklingslivscyklussen for Informationssystemer**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		**SEPO15 - Sikker udviklingspolitik**
14.2.1	Sikker udviklingspolitik	Regler for udvikling af software og systemer skal fastlægges og anvendes på udvikling inden for organisationen.	JA				X	X	En politik beskriver og etablerer en ramme for sikkerheden i udviklingsprocesser.	STRATUS
14.2.2	Procedurer for kontrol af systemændringer	Ændringer af systemer inden for udviklingslivscyklussen skal være kontrolleres ved hjælp af formelle procedurer for ændringskontrol	JA				X		Standardændringer foretages via workflowet i platformens orkestrator. Ikke-standardiserede ændringer er håndteres af forandringsprocessen	
14.2.3	Teknisk gennemgang af applikationer efter ændringer af driftsplatformen	Når driftsplatforme ændres, kan forretningskritiske applikationer skal gennemgås og testes for at sikre, at der ikke er nogen negativ indvirkning på organisationens drift eller sikkerhed.	JA				X	X	Hardware- og/eller systemopgraderinger testes på pilotgrupper, før de anvendes i produktionsmiljøer.	Systemopdateringsproces
14.2.4	Restriktioner på ændringer af softwarepakker	Ændringer af softwarepakker skal frarådes og begrænses til nødvendige ændringer, og alle ændringer skal kontrolleres strengt.	JA				X		Alle ændringer i forbindelse med scripts og automatiske kontrolsystemer logges i en GIT	Ingen ændringer i koden til de anvendte softwarepakker
14.2.5	Principper for sikker systemudvikling	Der skal opstilles principper for udvikling af sikre systemer, dokumenteres, vedligeholdes og anvendes i forbindelse med implementering af informationssystemer.	JA				X	X	Scripts og automatiske kontrolsystemer standardiseres og testes, før de sættes i produktion.	Uddannelse/bevidsthed
14.2.6	Sikkert udviklingsmiljø	Organisationer skal etablere og på passende vis beskytte sikre udviklingsmiljøer til systemudvikling og integration, der dækker hele systemudviklingens livscyklus.	JA				X	X	Administrer via AzureDevOps-workflow og udviklingsservere	Netværksarkitektur
14.2.7	Outsourcet udvikling	Organisationen skal føre tilsyn med og overvåge aktiviteterne hos outsourcet systemudvikling	JA			X		X	En intern serviceaftale med udviklingsenhederne fører tilsyn med og kontrollerer aktiviteterne og applikationer uden for ISMS	
14.2.8	Test af systemsikkerhed	Test af sikkerhedsfunktioner skal udføres under udvikling	JA				X	X	Testfaserne og compliance-tests håndteres i Azure DevOps-workflowet	
14.2.9	Test af systemaccept	Der skal etableres godkendelsestestprogrammer og relaterede kriterier for nye informationssystemer, opgraderinger og nye versioner.	JA				X	X		Resultater af sårbarhedsscanning
14.3	**Testdata**	**Sikre beskyttelse af data, der bruges til test**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
14.3.1	Beskyttelse af testdata	Testdata skal udvælges omhyggeligt, beskyttes og kontrolleres.	JA				X	X	Administrer via AzureDevOps-workflow og udviklingsservere	Logning af kopier
15	**Leverandørforhold**									**SEP013-Leverandørforhold**
15.1	**Informationssikkerhed i leverandørforhold**	**Sikre beskyttelse af organisationens aktiver, som er tilgængelig for leverandører**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
15.1.1	Informationssikkerhedspolitik for leverandørforhold	Krav til informationssikkerhed for at afbøde de risici, der er forbundet med med leverandørens adgang til organisationens aktiver skal aftales. med leverandøren og dokumenteres.	JA		X	X	X	X	X	Sikkerhedspolitikken i leverandørrelationer tager højde for og beskriver sikkerhedskravene og foranstaltninger, der er nødvendige for at overholde Cegids juridiske, lovgivningsmæssige og kontraktlige forpligtelser
15.1.2	Håndtering af sikkerhed i leverandøraftaler	Alle relevante informationssikkerhedskrav skal fastlægges og aftales med hver leverandør, der kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationens oplysninger	JA		X	X		X	X	Cegid sikrer, at dets leverandører er involveret i sikkerheden af den leverede service gennem certificering og kontraktlige forpligtelser.
15.1.3	Forsyningskæde for informations- og kommunikationsteknologi	Aftaler med leverandører skal indeholde krav til håndtering af de informationssikkerhedsrisici, der er forbundet med informations- og kommunikationsteknologitjenester og produktforsyningskæden.	JA		X	X		X	X	Cegid sikrer, at dets leverandører er involveret i sikkerheden af den leverede service gennem certificering og kontraktlige forpligtelser. For Talentsofts historiske aktiviteter er der ikke noget udbud i forbindelse med produktion, som er den Quadrias ansvar. Dette krav er derfor ikke medtaget.
15.2	**Ledelse af leverandørserviceleverancer**	**Opretholde et aftalt niveau af informationssikkerhed og service levering i overensstemmelse med leverandøraftaler**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
15.2.1	Overvågning og gennemgang af leverandørydelser	Organisationer skal regelmæssigt overvåge, gennemgå og revidere leverandørens levering af tjenester	JA		X	X		X	X	Sikkerhedsstyregruppemøder planlægges og organiseres med leverandørerne på en tilbagevendende basis. Audits gør det muligt at vurdere udviklinger og ændringer i de kontraktlige rammer.
15.2.2	Håndtering af ændringer i leverandørtjenester	Ændringer i leverandørernes levering af tjenester, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, -procedurer og -kontroller, skal styres under hensyntagen til den kritiske karakter af de involverede forretningsoplysninger, -systemer og -processer. og revurdering af risici	JA		X	X		X		Referat af møde i Kyndryl/Microsofts sikkerhedsudvalg
16	**Håndtering af informationssikkerhedshændelser**									**SEPS3 - Håndtering af sikkerhedshændelser**

16.1	**Håndtering af informationssikkerhedshændelser og forbedringer**	**Sikre en konsekvent og effektiv tilgang til håndtering af informationssikkerhedshændelser, herunder kommunikation om sikkerhedshændelser og svagheder.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
16.1.1	Ansvarsområder og procedurer	Der skal etableres ledelsesansvar og -procedurer for at sikre en hurtig, effektiv og velordnet reaktion på informationssikkerhed. hændelser	JA		X		X	X	X	
16.1.2	Rapportering af informationssikkerhedshændelser	Informationssikkerhedshændelser skal rapporteres gennem passende	JA		X		X	X	X	Proces til håndtering af sikkerhedshændelser i overensstemmelse med ISO 27035, herunder rapportering af sikkerhedshændelsen
16.1.3	Rapportering af svagheder i informationssikkerheden	Medarbejdere og entreprenører, der bruger organisationens informationssystemer og -tjenester, skal være forpligtet til at notere og rapportere alle observerede eller mistænkte svagheder i informationssikkerheden i systemer og tjenester.	JA		X		X	X	X	Prækvalifikation af begivenheden Kvalifikationsfase Undersøgelse
16.1.4	Vurdering af og beslutning om informationssikkerhedshændelser	Informationssikkerhedshændelser skal vurderes, og det skal besluttes, om de skal klassificeres som informationssikkerhedshændelser.	JA		X		X	X	X	Kommunikation / Rapportering Behandling Feedback
16.1.5	Reaktion på informationssikkerhedshændelser	Der skal reageres på informationssikkerhedshændelser i overensstemmelse med	JA		X		X	X	X	Lukning af hændelsen En RACI-matrix bestemmer roller og ansvar for hver fase En ugentlig gennemgang af hændelser udføres
16.1.6	Læring af hændelser inden for informationssikkerhed	Viden fra analyse og løsning af informationssikkerhedshændelser skal bruges til at reducere sandsynligheden for eller virkningen af fremtidige hændelser.	JA		X		X	X	X	
16.1.7	Indsamling af beviser	Organisationen skal definere og anvende procedurer for identifikation, indsamling, erhvervelse og bevaring af information, som kan tjene som bevis	JA		X		X	X	X	
17	**Informationssikkerhedsaspekter af business continuity management**									**SEIT25-SaaS krisestyring**
17.1	**Kontinuitet i informationssikkerheden**	**Kontinuitet i informationssikkerheden skal være indlejret i organisationens systemer til styring af forretningskontinuitet**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
17.1.1	Planlægning af informationssikkerhedskontinuitet	Organisationen skal fastlægge sine krav til informationssikkerhed og kontinuiteten i informationssikkerhedsstyringen i ugunstige situationer, f.eks. under en krise eller katastrofe.	JA				X	X	X	En forretningskontinuitetspolitik giver en ramme for organisationen og processerne for informationssikkerhedskontinuitet. En "kode rød"-proces regulerer krisehåndtering

17.1.2	Implementering af informationssikkerhedskontinuitet	Organisationen skal etablere, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre det nødvendige niveau af kontinuitet for informationssikkerhed i en ugunstig situation.	JA			X	X	X	Forskellige processer gør det muligt at opretholde informationssikkerheden (sikkerhedskopiering af data, robusthed i infrastruktur og menneskelige ressourcer, administration af sikre fjernproduktionsværktøjer).	Håndtering af hændelser / kode rød
17.1.3	Verificere, gennemgå og evaluere informationssikkerhedskontinuitet	Organisationen skal verificere de etablerede og implementerede kontroller for informationssikkerhedskontinuitet med jævne mellemrum for at sikre, at de er gyldige og effektive i ugunstige situationer.	JA			X	X	X	Kontinuiteten i informationssikkerheden vurderes løbende.	
17.2	**Afskedigelser**	**Sikre tilgængelighed af faciliteter til informationsbehandling**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
17.2.1	Tilgængelighed af informationsbehandlingsfaciliteter	Informationsbehandlingsfaciliteter skal implementeres med tilstrækkelig redundans til at opfylde tilgængelighedskravene.	JA		X	X	X	X	Redundans- og resiliensmekanismer for arkitekturer og teams er aktive fra ende til anden. Der er konstant overvågning af disse mekanismer	SaaS-arkiteturdokumenter
18	**Overholdelse**									**SEPO10-Compliance og revisionsstyring**
18.1	**Overholdelse af juridiske og kontraktlige krav**	**Undgå brud på juridiske, lovmæssige, regulatoriske eller kontraktlige forpligtelser. forpligtelser i forbindelse med informationssikkerhed og sikkerhedskrav.**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
18.1.1	Identifikation af gældende lovgivning og kontraktlige krav	Alle relevante lovgivningsmæssige, regulatoriske og kontraktlige krav o g organisationens tilgang til at opfylde disse krav skal udtrykkeligt identificeres, dokumenteres og holdes ajour for hvert informationssystem og organisationen.	JA		X	X		X	X	Cegid Groups juridiske proces definerer, dokumenterer og opdaterer alle juridiske, lovgivningsmæssige og kontraktmæssige krav, der gælder for ISMS	Juridisk proces
18.1.2	Intellektuelle ejendomsrettigheder	Der skal implementeres passende procedurer for at sikre overholdelse af lovgivningsmæssige, regulatoriske og kontraktlige krav i forbindelse med intellektuelle ejendomsrettigheder og brug af proprietære softwareprodukter.	JA		X	X		X	X	Cegid Cloud Factory er forpligtet til at sikre overholdelse af lovgivningsmæssige, regulatoriske og kontraktlige krav i forbindelse med intellektuelle ejendomsrettigheder og brugen af proprietære softwareprodukter. Software købes fra kendte og velrenommerede kilder for at sikre, at ophavsretten respekteres.	Licensregister
18.1.3	Beskyttelse af optegnelser	Registreringer skal beskyttes mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret frigivelse i overensstemmelse med lovmæssige, regulatoriske, kontraktlige og forretningsmæssige krav.	JA		X	X		X		Registreringer er beskyttet mod tab, ødelæggelse, forfalskning, uautoriseret adgang og uautoriseret offentliggørelse.	
18.1.4	Privatliv og beskyttelse af personligt identificerbare oplysninger	Privatliv og beskyttelse af personligt identificerbare oplysninger skal være sikres som krævet i relevant lovgivning og regulering, hvor det er relevant	JA		X	X		X	X	Den generelle forordning om databeskyttelse har været gældende siden den 25. maj 2018. I den forbindelse har Cegid udpeget en DPO med ansvar for at overvåge emnet på tværs af koncernen.	
18.1.5	Regulering af kryptografiske kontroller	Kryptografiske kontroller skal anvendes i overensstemmelse med alle relevante aftaler, lovgivning og bestemmelser	JA					X		Cegid Cloud Factory overholder de gældende aftaler, love og bestemmelser vedrørende kryptografi. Cegid hverken importerer eller eksporterer nogen kryptografiske løsninger.	
18.2	**Gennemgang af informationssikkerhed**	**Sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer**	**Inkluderet**	**LO**	**CO**	**BC**	**BLO DTR YK**	**RA**		
18.2.1	Uafhængig gennemgang af informationssikkerhed	Organisationens tilgang til styring af informationssikkerhed og dens implementering (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) skal gennemgås uafhængigt med planlagte intervaller, eller når der sker væsentlige ændringer.	JA				X	X	Cegid Cloud Factory gennemfører en intern revision af informationssystemet mindst en gang om året. En ledelsesgennemgang er planlagt i slutningen af	
18.2.2	Overholdelse af sikkerhedspolitikker og -standarder	Ledere skal regelmæssigt undersøge, om informationsbehandlingen og procedurerne inden for deres ansvarsområde er i overensstemmelse med de relevante sikkerhedspolitikker, standarder og andre sikkerhedsstandarder. krav	JA					X		ISMS-indikatorer og -mål
18.2.3	Gennemgang af teknisk overensstemmelse	Informationssystemer skal regelmæssigt kontrolleres for overensstemmelse med organisationens politikker og standarder for informationssikkerhed	JA			X	X	X	En politik med pentests og teknisk auditering hjælper med at identificere afvigelser.	Scanningsrapport