Trustteam

Statement Of Applicability

D-MSP-002.1

Datum opmaak: 04/03/2018

Datum herziening: 28/04/2022

nr.	Clausule ISO/IEC 27001:2013 Annex A controls	Controle	Van toepas	reden uitsluiting	Uitleg of referentie naar controle
A.5	Informatieveiligheidsbeleid				
A.5.1	Beleidssturing voor informatieveiligheid	[2]			
A.5.1.1	Beleid voor informatieveiligheid	Een set van beleidsplannen voor informatiebeveiliging wordt vastgesteld, goedgekeurd door het management, gepubliceerd en meegedeeld aan medewerkers en relevante externe partijen.	ja		Wordt toegepast.
A.5.1.2	Beoordeling informatieveiligheidsbeleid	Het informatiebeveiligingsbeleid wordt op geregelde tijdstippen beoordeeld of als er belangrijke wijzigingen voordoen om de continue geschiktheid, adequaatheid en doeltreffendheid ervan te garanderen.	ja		Wordt toegepast.
A.6	Organisatie van informatiebeveiliging				
A.6.1	Interne organisatie				
A.6.1.1	Rollen en verantwoordelijkheden informatieveiligheid	Alle verantwoordelijkheden omtrent informatiebeveiliging worden vastgesteld en toegewezen.	ja		Wordt toegepast.
A.6.1.2	Scheiding van taken	Tegenstrijdige taken en bevoegdheden moeten worden gescheiden om de mogelijkheden voor ongeoorloofde of onbedoelde wijziging of misbruik van de data van de organisatie te verminderen.	ja		Wordt toegepast.
A.6.1.3	Contact met overheidsinstanties	De nodige contacten met de relevante autoriteiten worden gehandhaafd.	ja		Wordt toegepast.
A.6.1.4	Contact met stakeholders	De nodige contacten met belangengroepen en andere gespecialiseerde security forums en beroepsorganisaties worden gehandhaafd.	ja		Wordt toegepast.
A.6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging wordt ook meegenomen in het projectmanagement, ongeacht het type van het project.	ja		Wordt toegepast.
A.6.2	Mobiele apparatuur en teleworking				
A.6.2.1	Beleid mobiele apparatuur	Een beleid en ondersteunende veiligheidsmaatregelen worden genomen om de risico's geïntroduceerd door het gebruik van mobiele apparaten te beheren.	ja		Wordt toegepast.

A.6.2.2	Teleworking	Een beleid en ondersteunende veiligheidsmaatregelen moeten worden geïmplementeerd om informatie te beschermen waartoe toegang verschaft wordt of dat verwerkt of opgeslagen wordt bij telewerken.	ja		Wordt toegepast.
A.7	Veiligheid personeelszaken				
A.7.1	Voorafgaand aan de tewerkstelling				
A.7.1.1	Screening	Achtergrondcontroles van alle kandidaten voor werkgelegenheid, aannemers en andere derde partijen worden uitgevoerd in overeenstemming met de relevante wet- en regelgeving en ethiek, en evenredig aan de bedrijfseisen, de toegang tot informatie die samenhangt met de opdracht en de waargenomen risico's.	ja		Wordt toegepast.
A.7.1.2	Arbeidsvoorwaarden	De contractuele afspraken met werknemers en contractanten nemen zijn verantwoordelijkheden en deze van de organisatie op voor informatiebeveiliging.	ja		Wordt toegepast.
A.7.2	Tijdens de tewerkstelling				
A.7.1.1	Directieverantwoordelijkheden	Het bestuur stelt medewerkers, aannemers en derde partijen aan om de veiligheid toe te passen in overeenstemming met het vastgestelde beleid en de procedures van de organisatie.	ja		Wordt toegepast.
A.7.2.2	Bewustzijn, opleiding en training t.a.v. informatieveiligheid	Alle medewerkers van de organisatie en, indien van toepassing, aannemers en derde partijen zullen passende bewustwordingstraining en regelmatige updates in organisatorisch beleid en procedures krijgen, voor zover deze relevant zijn voor hun functie.	ja		Wordt toegepast.
A.7.2.3	Tuchtprocedure	Er moet een formele disciplinaire procedure zijn voor werknemers die een inbreuk op de beveiliging hebben begaan	ja		Wordt toegepast.
A.7.3	Beëindigen of wijzigen van tewerkstelling				
A.7.3.1	Beëindigen of wijzigen van tewerkstellingsverantwoordelijkheden	Er moet een formele disciplinaire procedure zijn voor werknemers die een inbreuk op de beveiliging hebben gepleegd.	ja		Wordt toegepast.
A.8	Beheer van bedrijfsmiddelen				

A.8.1	Verantwoordelijkheid voor bedrijfsmiddelen				
A.8.1.1	Inventaris van bedrijfsmiddelen	Informatie, andere middelen met informatie en informatieverwerkingsfaciliteiten moeten worden geïdentificeerd en een inventaris van deze middelen moet opgesteld en bijgehouden worden.	ja		Wordt toegepast.
A.8.1.2	Eigendom van bedrijfsmiddelen	Middelen, opgenomen in de inventaris, moeten voorzien zijn van een eigenaar.	ja		Wordt toegepast.
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van informatie en het gebruik van middelen in verband met de verwerking van informatie moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	ja		Wordt toegepast.
A.8.1.4	Teruggeven van bedrijfsmiddelen	Alle medewerkers, aannemers en derde partijen zullen alle middelen van de organisatie in hun bezit teruggeven bij beëindiging van het dienstverband, contract of overeenkomst.	ja		Wordt toegepast.
A.8.2	Informatieclassificatie				
A.8.2.1	Classificeren van informatie	Informatie wordt ingedeeld in termen van wettelijke voorschriften, waarde, kritikaliteit en gevoeligheid voor ongeoorloofde openbaarmaking of wijziging.	ja		Wordt toegepast.
A.8.2.2	Informatie labelen	Een passende reeks procedures om informatie te labelen worden ontwikkeld en uitgevoerd in overeenstemming met de door de organisatie aangenomen informatie-indeling.	ja		Wordt toegepast.
A.8.2.3	Omgaan met bedrijfsmiddelen	Procedures voor de behandeling van bedrijfsmiddelen worden ontwikkeld en geïmplementeerd in overeenstemming met de door de organisatie aangenomen informatie-indeling.	ja		Wordt toegepast.
A.8.3	Omgaan met media				
A.8.3.1	Beheer van verwijderbare media	Procedures worden geïmplementeerd voor het beheer van verwijderbare media in overeenstemming met de door de organisatie aangenomen informatie-indeling.	ja		Wordt toegepast.
A.8.3.2	Verwijderen van media	Media moeten veilig worden verwijderd d.m.v. het gebruik van formele procedures wanneer zij niet langer nodig zijn.	ja		Wordt toegepast.

A.8.3.3	Fysieke overdracht van media	Media die informatie bevat, moet wordenbeschermd tegen ongeautoriseerde toegang, misbruik of beschadiging tijdens het transport.	ja		Wordt toegepast.
A.9	Toegangsbeveiliging				
A.9.1	Bedrijfseisen voor toegangsbeveiliging				
A.9.1.1	Toegangsbeveiligingsbeleid	Een toegangscontrole beleid moet worden opgesteld, gedocumenteerd en beoordeeld op basis van zakelijke en informatiebeveiligingseisen.	ja		Wordt toegepast.
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers mogen alleen worden voorzien van toegang tot het netwerk en de netwerkdiensten waarvoor zij speciaal gemachtigd zijn om te gebruiken.	ja		Wordt toegepast.
A.9.2	Beheer gebruikerstoegang				
A.9.2.1	Registratie en uitschrijven gebruikers	Een formeel gebruikersregistratie- en de-registratieproces wordt uitgevoerd om de toewijzing van toegangsrechten mogelijk te maken.	ja		Wordt toegepast.
A.9.2.2	Gebruikerstoegang voorzien	Een formele gebruikerstoegang voorzieningsproces worden uitgevoerd om de toegangsrechten toe te kennen of in te trekken voor elk type gebruiker en voor alle systemen en diensten.	ja		Wordt toegepast.
A.9.2.3	Beheer van bijzondere toegangsrechten	De toewijzing en het gebruik van bevoorrechte toegangsrechten worden beperkt en gecontroleerd.	ja		Wordt toegepast.
A.9.2.4	Beheer van geheime identificatie-informatie van gebruikers	De toewijzing van geheime idintificatie-informatie wordt gecontroleerd door middel van een formeel proces.	ja		Wordt toegepast.
A.9.2.5	Beoordeling toegangsrechten gebruikers	Eigenaars van bedrijfsmiddelen herzien de toegangsrechten van de gebruikers op regelmatige tijdstippen.	ja		Wordt toegepast.
A.9.2.6	Beoordeling of aanpassing toegangsrechten	De toegangsrechten van alle medewerkers en derde partijen tot informatie en informatieverwerkingsvoorzieningen moeten bij beëindiging van het dienstverband, contract of overeenkomst, worden verwijderd of aangepast bij verandering.	ja		Wordt toegepast.
A.9.3	Gebruikersverantwoordelijkheden				
A.9.3.1	Gebruik van geheime identificatie-informatie	Gebruikers zijn verplicht om de praktijken van de organisatie te volgen in het gebruik van geheime identificatie-informatie.	ja		Wordt toegepast.
A.9.4	Toegangsbeveiliging van systemen en applicaties				
A.9.4.1	Beperking toegang tot informatie	Toegang tot informatie en de toepassing van systeemfuncties wordt beperkt in overeenstemming met het toegangscontrolebeleid.	ja		Wordt toegepast.
A.9.4.2	Beveiligde inlogprocedures	Indien vereist door het toegangscontrolebeleid, wordt de toegang tot systemen en toepassingen gecontroleerd door een beveiligde log-on procedure.	ja		Wordt toegepast.
A.9.4.3	Systeem voor wachtwoordbeheer	Het wachtwoordbeleid is interactief en draagt zorg voor de kwaliteit van wachtwoorden.	ja		Wordt toegepast.

A.9.4.4	Bijzondere systeemhulpmiddelen gebruiken	Het gebruik van hulpprogramma's die in staat zijn om systemen en applicatie controles te overrulen, worden beperkt en streng gecontroleerd.	ja		Wordt toegepast.
A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de broncode van een programma wordt beperkt.	ja		Wordt toegepast.
A.10	Cryptografie				
A.10.1	Cryptografische controles				
A.10.1.1	Beleid inzake gebruik van cryptografische controles	Een beleid inzake het gebruik van cryptografische controles voor de bescherming van gegevens worden ontwikkeld en uitgevoerd.	ja		Wordt toegepast.
A.10.1.2	Sleutelbeleid	Een beleid op het gebruik, de beveiliging en de levensduur van de cryptografische sleutels worden ontwikkeld en geïmplementeerd door hun hele levenscyclus.	ja		Wordt toegepast.
A.11	Fysicke en omgevingsbeveiliging				
A.11.1	Beveiligde omgeving				
A.11.1.1	Fysieke beveiligingsperimeter	Veiligheidsperimeters worden gedefinieerd en gebruikt om gebieden die ofwel gevoelige of kritieke informatie en informatieverwerkingsfaciliteiten bevatten te beschermen.	ja		Wordt toegepast.
A.11.1.2	Fysieke ingangscontrole	Beveiligde gebieden worden door passende controles bij binnenkomst beschermd om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	ja		Wordt toegepast.
A.11.1.3	Beveiliging van kantoren, ruimtes en faciliteiten	Fysieke beveiliging voor kantoren, kamers en faciliteiten worden ontwikkeld en toegepast.	ja		Wordt toegepast.
A.11.1.4	Bescherming tegen externe en omgevingsgerelateerde bedreigingen	Fysieke bescherming tegen natuurrampen, kwaadaardige aanvallen of ongelukken moeten zo worden ontworpen en toegepast.	ja		Wordt toegepast.
A.11.1.5	Werken in een beveiligde omgeving	Procedures voor het werken in veilige gebieden worden ontworpen en toegepast.	ja		Wordt toegepast.
A.11.1.6	Laad- en losruimte	Toegangspunten, zoals de levering- en laadplaatsen van gebieden en andere plaatsen waar onbevoegden het terrein kunnen betreden, moeten worden gecontroleerd en, indien mogelijk, geïsoleerd van informatieverwerkingsfaciliteiten om onbevoegde toegang te voorkomen.	ja		Wordt toegepast.
A.11.2	Uitrusting				
A.11.2.1	Situering en bescherming van de uitrusting	De apparatuur moet worden geplaatst en beschermd om de risico's van de bedreigingen voor het milieu en de risico's en kansen voor onbevoegde toegang te beperken.	ja		Wordt toegepast.
A.11.2.2	Nutsvoorzieningen	De apparatuur moet worden beschermd tegen stroomstoringen en andere storingen veroorzaakt door storingen in het ondersteunen van nutsbedrijven.	ja		Wordt toegepast.

A.11.2.3	Beveiliging van bekabeling	Energie- en telecommunicatiebekabeling die gegevens vervoeren of informatiediensten ondersteunen worden beschermd tegen onderschepping of beschadiging.	ja		Wordt toegepast.
A.11.2.4	Onderhoud van de uitrusting	Apparatuur moet correct worden gehandhaafd om de voortdurende beschikbaarheid en integriteit te garanderen.	ja		Wordt toegepast.
A.11.2.5	Verwijderen van bedrijfsmiddelen	Apparatuur, informatie of software mag niet off-site worden meegenomen zonder voorafgaande toestemming.	ja		Wordt toegepast.
A.11.2.6	Beveiliging van uitrusting en bedrijfsmiddelen buiten het terrein	Beveiliging wordt toegepast op off-site bedrijfsmiddelen, waarbij rekening wordt gehouden met de verschillende risico's van het werken buiten de kantoren van de organisatie.	ja		Wordt toegepast.
A.11.2.7	Veilig verwijderen of hergebruiken van uitrustingen	Alle onderdelen van de uitrusting die opslagmedia bevatten, moet worden gecontroleerd om ervoor te zorgen dat alle gevoelige gegevens en software onder licentie is verwijderd of veilig overgeschreven voorafgaand aan verwijdering of hergebruik.	ja		Wordt toegepast.
A.11.2.8	Onbeheerde uitrusting	Gebruikers zorgen ervoor dat onbewaakte apparatuur op een passende wijze beschermd is.	ja		Wordt toegepast.
A.11.2.9	Clear desk' en 'clear screen' beleid	Een duidelijke desk policy voor papier en verwijderbare opslagmedia en een helder scherm beleid worden vastgesteld voor verwerkingsinstanties.	ja		Wordt toegepast.
A.12	Operationele veiligheid				
A.12.1	Operationele procedures en verantwoordelijkheden				
A.12.1.1	Gedocumenteerde operationele procedures	Operationele procedures moeten worden gedocumenteerd, onderhouden en ter beschikking gesteld van alle gebruikers die ze nodig hebben.	ja		Wordt toegepast.
A.12.1.2	Veranderingsmanagement	Wijzigingen in de organisatie, bedrijfsprocessen, informatieverwerkingsfaciliteiten en systemen die informatiebeveiliging beïnvloeden, moeten worden gecontroleerd.	ja		Wordt toegepast.
A.12.1.3	Capaciteitsbeheer	Het gebruik van de middelen moeten worden gemonitord, afgestemd en projecties gemaakt van de toekomstige benodigde capaciteit om de vereiste prestaties van het systeem te waarborgen.	ja		Wordt toegepast.
A.12.1.4	Scheiding van ontwikkeling, testing en productieomgevingen	Ontwikkelings-, testings- en operationele omgevingen worden gescheiden om de risico's van onbevoegde toegang of wijzigingen in de operationele omgeving te verminderen.	ja		Wordt toegepast.
A.12.2	Bescherming tegen malware				
A.12.2.1	Controles tegen malware	Detectie, preventie en herstel controles om te beschermen tegen malware worden uitgevoerd in combinatie met een gepast bewustzijn bij de gebruiker.	ja		Wordt toegepast.
A.12.3	Back-up				

A.12.3.1	Informatieback-up	Back-ups van de informatie, software en het systeem worden genomen en regelmatig getest in overeenstemming met een overeengekomen backup beleid of procedure.	ja		Wordt toegepast.
A.12.4	Registreren en beoordelen				
A.12.4.1	Gebeurtenissen registreren	Event logs die activiteiten van gebruikers, uitzonderingen, fouten en informatiebeveiligingsgebeurtenissen registreert, worden geproduceerd, onderhouden en regelmatig beoordeeld.	ja		Wordt toegepast.
A.12.4.2	Beschermen van informatie in logbestanden	Logging faciliteiten en log gegevens worden beschermd tegen sabotage en toegang door onbevoegden.	ja		Wordt toegepast.
A.12.4.3	Beheerder en gebruiker van logbestanden	Systeembeheerder- en netbeheerdersactiviteiten worden geregistreerd en de logboeken worden beschermd en regelmatig beoordeeld.	ja		Wordt toegepast.
A.12.4.4	kloksynchronisatie	De klokken van alle relevante informatiesystemen binnen een organisatie of securitydomein worden gesynchroniseerd met één enkele tijdsbron.	ja		Wordt toegepast.
A.12.5	Controle van de operationele software				
A.12.5.1	Software installeren op operationele systemen	Procedures worden uitgevoerd om de installatie van de software te controleren op operationele systemen.	ja		Wordt toegepast.
A.12.6	Beheer van technische kwetsbaarheden				
A.12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen moet tijdig worden verkregen, blootstelling van de organisatie aan dergelijke kwetsbaarheden geëvalueerd en passende maatregelen genomen om de bijbehorende risico's aan te pakken.	ja		Wordt toegepast.
A.12.6.2	Beperkingen op software-installatie	Regels voor de installatie van de software door de gebruikers moet worden vastgesteld en uitgevoerd.	ja		Wordt toegepast.
A.12.7	Overwegingen audit informatiesystemen				
A.12.7.1	Controle op audit informatiesystemen	Controle-eisen en activiteiten met betrekking tot de verificatie van de operationele systemen moeten zorgvuldig worden gepland en afgesproken om verstoringen van de bedrijfsprocessen te minimaliseren.	ja		Wordt toegepast.
A.13	Beveliging van communicatie				
A.13.1	Beheer netwerkbeveiliging				
A.13.1.1	Netwerkcontroles	Netwerken worden beheerd en gecontroleerd om informatie in systemen en applicaties te beschermen.	ja		Wordt toegepast.
A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, service levels en beleidseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in de overeenkomsten met de netwerkdiensten, ongeacht of deze diensten in-house of uitbesteed zijn.	ja		Wordt toegepast.

A.13.1.3	Scheiden van netwerken	Groepen van informatie-diensten, gebruikers en informatiesystemen worden gescheiden op netwerken.	ja		Wordt toegepast.
A.13.2	Informatietransfer				
A.13.2.1	Beleid en procedures voor informatietransfer	Formeel overdrachtsbeleid, procedures en controles moeten worden getroffen om de overdracht van informatie door middel van het gebruik van alle vormen van communicatiefaciliteiten te beschermen.	ja		Wordt toegepast.
A.13.2.2	Overeenkomsten over informatietransfer	Overeenkomsten moeten de veilige overdracht van zakelijke informatie tussen de organisatie en externe partijen aanpakken.	ja		Wordt toegepast.
A.13.2.3	Elektronische berichten	Informatie die betrokken zijn bij elektronische berichtenuitwisseling moet op passende wijze worden beschermd.	ja		Wordt toegepast.
A.13.2.4	Vertrouwelijkheid of geheimhoudingsverklaring	Vereisten voor de vertrouwelijkheid of non-disclosure overeenkomsten als gevolg van de behoeften van de organisatie voor de bescherming van gegevens worden geïdentificeerd, regelmatig herzien en gedocumenteerd.	ja		Wordt toegepast.
A.14	Systeem verwerven, ontwikkelen en onderhouden				
A.14.1	Beveiligingseisen voor informatiesystemen				
A.14.1.1	Analyseren en specifiëren beveiligingseisen	De eisen gerelateerd aan informatiebeveiliging worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen van bestaande informatiesystemen.	ja		Wordt toegepast.
A.14.1.2	Beveiligen applicaties op openbare netwerken	Informatie die d.m.v. het gebruik van toepassingen over openbare netwerken passeren, worden beschermd tegen frauduleuze activiteiten, contractgeschillen en ongeoorloofde bekendmaking en modificatie.	ja		Wordt toegepast.
A.14.1.3	Bescherming applicatietransacties	Informatie m.b.t. applicatietransacties worden beschermd om onvolledige overdracht, onjuiste routering, onbevoegde berichtwijziging, ongeoorloofde openbaarmaking, onbevoegde bericht kopies of herhaling te voorkomen.	ja		Wordt toegepast.
A.14.2	Beveiliging in ontwikkelings- en ondersteunende processen				
A.14.2.1	Ontwikkelingsbeleid i.f.v. veiligheid	Regels voor de ontwikkeling van software en systemen worden vastgesteld en toegepast op de ontwikkelingen binnen de organisatie.	ja		Wordt toegepast.
A.14.2.2	Procedures van controles op systeemverandering	Wijzigingen in systemen binnen de ontwikkelingscyclus worden gecontroleerd door het gebruik van formele procedures van controles op systeemverandering.	ja		Wordt toegepast.
A.14.2.3	Technische beoordeling van applicaties na wijzigingen aan het operationeel platform	Wanneer operatieve platformen gewijzigd zijn, worden bedrijfskritische applicaties beoordeeld en getest om te zorgen dat er geen negatieve invloed is op de organisatorische operaties of beveiliging.	ja		Wordt toegepast.

A.14.2.4	Beperkingen op wijzigingen in softwarepakketten	Wijzigingen aan softwarepakketten worden ontmoedigd, beperkt tot de noodzakelijke veranderingen en alle veranderingen zullen streng worden gecontroleerd.	ja		Wordt toegepast.
A.14.2.5	Principes voor het ontwikkelen van beveiligde systemen	Principes voor het ontwikkelen van beveiligde systemen worden opgesteld, gedocumenteerd, onderhouden en toegepast op alle informatie systeem implementatie inspanningen.	ja		Wordt toegepast.
A.14.2.6	Beveiligde ontwikkelomgeving	Organisaties stellen een adequaat beschermde ontwikkelomgeving voor systeemontwikkeling op en leveren integratie-inspanningen die de hele ontwikkelingscyclus van het systeem dekken.	ja		Wordt toegepast.
A.14.2.7	Uitbestede softwareontwikkeling	De organisatie moet toezicht en controle houden op de activiteit van uitbestede systeemontwikkelingen.	ja		Wordt toegepast.
A.14.2.8	Testen van de systeembeveiliging tijdens ontwikkeling	Het testen van de beveiligingsfunctionaliteit wordt uitgevoerd tijdens de ontwikkeling.	ja		Wordt toegepast.
A.14.2.9	Systeemacceptatietests	Acceptatie testprogramma's en de bijbehorende criteria worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies.	ja		Wordt toegepast.
A.14.3	Testgegevens				
A.14.3.1	Bescherming van testgegevens	Test gegevens zullen zorgvuldig worden gekozen, beschermd en gecontroleerd.	ja		Wordt toegepast.
A.15	Leveranciersrelaties				
A.15.1	Informatieveiligheid in leveranciersrelaties				
A.15.1.1	Informatieveiligheidsbeleid in leveranciersrelaties	Informatiebeveiligingsvereisten voor het verminderen van de risico's die samenhangen met de toegang voor leverancier tot de bedrijfsmiddelen moet met de leverancier worden overeengekomen en gedocumenteerd.	ja		Wordt toegepast.
A.15.1.2	Veiligheid opnemen in leveranciersovereenkomst	Informatiebeveiligingsvereisten voor het verminderen van de risico's die samenhangen met de toegang voor leverancier tot de bedrijfsmiddelen moet met de leverancier worden overeengekomen en gedocumenteerd.	ja		Wordt toegepast.
A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	Alle relevante eisen omtrent informatiebeveiliging worden vastgesteld en overeengekomen met elke leverancier die gegevens van de organisatie kan openen, verwerken, opslaan en communiceren of die IT-infrastructuur componenten aanbiedt.	ja		Wordt toegepast.
A.15.2	Beheer dienstverlening van leveranciers				
A.15.2.1	Opvolgen en beoordelen van leveranciersdiensten	Organisaties zullen regelmatig toezicht, evaluatie en leveranciersaudits uitvoeren.	ja		Wordt toegepast.

A.15.2.2	Omgaan met veranderingen in leveranciersdiensten	Wijzigingen in de dienstverlening door leveranciers, met inbegrip van het behoud en de verbetering van het bestaande informatieveiligheidsbeleid, procedures en controles, worden beheerd, rekening houdend met het kritieke karakter van zakelijke informatie, systemen en processen omtrent de herbeoordeling van de risico's.	ja		Wordt toegepast.
A.16	Informatieveiligheidsincidentenbeheer				
A.16.1	Beheer van informatieveiligheidsincidenten en -verbeteringen				
A.16.1.1	Verantwoordelijkheden en procedures	Beheerstaken en procedures worden vastgesteld om een snelle, effectieve en ordelijke reactie op informatie beveiligingsincidenten te waarborgen.	ja		Wordt toegepast.
A.16.1.2	Rapporteren van gebeurtenissen omtrent informatieveiligheid	Gebeurtenissen omtrent informatiebeveiliging moeten zo snel mogelijk worden gemeld door middel van een passende kanalen.	ja		Wordt toegepast.
A.16.1.3	rapporteren van zwaktes omtrent informatieveiligheid	Werknemers en contractanten zijn verplicht om eventuele geconstateerde of vermoede tekortkomingen in het kader van informatiebeveiliging melden met behulp van de organisatie informatiesystemen en -diensten.	ja		Wordt toegepast.
A.16.1.4	Evalueren en beslissingen nemen over gebeurtenissen omtrent informatieveiligheid	Gebeurtenissen omtrent Informatiebeveiliging worden geëvalueerd en daarna wordt beslist of ze als informatiebeveiligingsincidenten worden geclassificeerd.	ja		Wordt toegepast.
A.16.1.5	Reactie op incidenten omtrent informatieveiligheid	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	ja		Wordt toegepast.
A.16.1.6	Leren van incidenten omtrent informatieveiligheid	De kennis die is opgedaan met het analyseren en oplossen van informatiebeveiligingsincidenten moeten worden gebruikt om de kans op of de gevolgen van incidenten in de toekomst te verminderen.	ja		Wordt toegepast.
A.16.1.7	Verzamelen van bewijzen	De organisatie moet procedures definiëren en toepassen voor de identificatie, inzameling, verwerving en het behoud van informatie, die als bewijs kunnen dienen.	ja		Wordt toegepast.
A.17	Informatieveiligheidsaspecten van bedrijfscontinuïteitsbeheer				
A.17.1	Continuïteit in informatiebeveiliging				
A.17.1.1	Plannen van continuïteit in informatiebeveiliging	De organisatie stelt zijn eisen voor informatiebeveiliging en continuïteit van information security management in ongunstige omstandigheden, bijv. tijdens een crisis of ramp.	ja		Wordt toegepast.

A.17.1.2	Implementeren van continuïteit in informatiebeveiliging	De organisatie moet processen, procedures en controles vaststellen, documenteren, implementeren en onderhouden om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	ja		Wordt toegepast.
A.17.1.3	Verifieer, beoordeel en evalueer continuïteit in informatieveiligheid	De organisatie dient de opstelling en de uitvoering van informatiebeveiliging continuïteitscontroles op regelmatige tijdstippen te controleren om ervoor te zorgen dat ze geldig en effectief zijn tijdens ongunstige omstandigheden.	ja		Wordt toegepast.
A.17.2	Overbodigheid	doel: beschikbaarheid van informatieverwerkingsmiddelen garanderen			
A.17.2.1	Beschikbaarheid van informatieverwerkingsfaciliteiten	Informatieverwerkingsfaciliteiten zullen met net voldoende overbodigheid worden uitgevoerd om aan de beschikbaarheidseisen te voldoen.	ja		Wordt toegepast.
A.18	Compliance				
A.18.1	Naleving legale en contractuele vereisten				
A.18.1.1	Identificatie van toepasbare wetten en contractuele verplichtingen	Alle relevante wettelijke, reglementaire, contractuele vereisten en de aanpak van de organisatie om aan deze eisen te voldoen, moeten expliciet worden geïdentificeerd, gedocumenteerd en up-to-date zijn voor elk informatiesysteem en de organisatie.	ja		Wordt toegepast.
A.18.1.2	Intellectuele eigendomsrechten	Passende procedures worden uitgevoerd om de naleving van wettelijke en contractuele vereisten met betrekking tot de intellectuele eigendomsrechten en het gebruik van gepatenteerde software producten te garanderen.	ja		Wordt toegepast.
A.18.1.3	Bescherming van archieven	De verzamelde gegevens worden beschermd tegen verlies, vernietiging, vervalsing, ongeoorloofde toegang en ongeoorloofde release, in overeenstemming met wettelijke, reglementaire, contractuele en zakelijke behoeften.	ja		Wordt toegepast.
A.18.1.4	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens moet worden verzekerd, zoals vereist in de relevante wet- en regelgeving, indien van toepassing.	ja		Wordt toegepast.
A.18.1.5	Voorschriften cryptografische controles	Cryptografische controles worden gebruikt in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	ja		Wordt toegepast.
A.18.2	Beoordelingen informatieveiligheid				

A.18.2.1	Onafhankelijke beoordeling informatieveiligheid	De aanpak van de organisatie voor het beheer van informatiebeveiliging en de uitvoering daarvan (dat wil zeggen de doelstellingen, controles, beleid, processen en procedures voor informatiebeveiliging) moet onafhankelijk en op geregelde tijdstippen worden beoordeeld of wanneer zich aanzienlijke veranderingen voordoen.	ja		Wordt toegepast.
A.18.2.2	Naleving veiligheidsbeleid en -normen	Managers moeten regelmatig de naleving van informatieverwerking en procedures binnen hun gebied van verantwoordelijkheid nazien met het informatieveiligheidsbeleid, de normen en andere veiligheidseisen.	ja		Wordt toegepast.
A.18.2.3	Beoordeling technische naleving	Informatiesystemen worden regelmatig getoetst op naleving van informatiebeveiligingsbeleid van de organsatie en de normen.	ja		Wordt toegepast.