CINOP

leren met impact

Verklaring van Toepasselijkheid

NEN-EN-ISO/IEC 27001:2017+A11:2020

Colofon

Titel	Verklaring van Toepasselijkheid
Auteur	Dennis Klatt
Versie	1.0 (publiek)
Datum	15-6-2023

Stichting CINOP realiseert oplossingen voor complexe vraagstukken in onderwijs en arbeidsmarkt. Oplossingen met impact. Wij zetten ons in voor een optimale deelname van iedereen aan de samenleving, vandaag en morgen. We professionaliseren en flexibiliseren leerprocessen, samen met onze partners in onderwijs, overheid en bedrijfsleven. We zijn gespecialiseerd in vraagstukken rondom flexibel onderwijs, professionalisering in het beroepsonderwijs en arbeidsmarktleren: een leven lang ontwikkelen. Ook internationaal zijn we actief: samen met onze partners dragen we bij aan mobiliteit, Europese leermogelijkheden en onderwijsprojecten voor capaciteitsontwikkeling in Europa, Afrika, Azië en Latijns Amerika.

CINOP B.V.
Postbus 1585
5200 BP ’s-Hertogenbosch
Tel: 073-6800800
www.cinop.nl

© CINOP B.V. 2020
Niets uit deze uitgave mag worden vermenigvuldigd of openbaar gemaakt door middel van druk, fotokopie, op welke andere wijze dan ook, zonder vooraf schriftelijke toestemming van de uitgever.

Inhoudsopgave

1 Verklaring van Toepasselijkheid 1

2 Beheersmaatregel niet van toepassing 2

3 Beheersmaatregel van toepassing 3

1 Verklaring van Toepasselijkheid

Voor u ligt de definitieve Verklaring van Toepasselijkheid (VVT) van Stichting CINOP - ecbo waarin de borging is beschreven van het informatieveiligheidsbeleid conform NEN-EN-ISO/IEC 27001:2017+A11:2020. De VVT beschrijft het normenkader waar de organisatie zich aan committeert en beschrijft eventuele redenen van uitsluiting.

Scope
De VVT strekt zich uit over de gehele Stichting CINOP - ecbo en richt zich op het beveiligen van informatie tot:

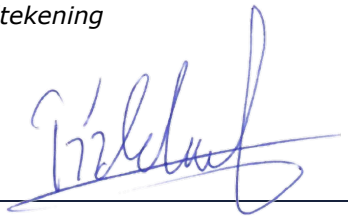
Het leveren van advies en uitvoeren van onderzoek op het gebied van leren, ontwikkelen en het professionaliseren van organisaties:

- Project- en programmamanagement
- Het ontwikkelen en verzorgen van trainingen

Conform de verklaring van toepasselijkheid d.d. 15/06/2023 versie 1.0, waarin is gespecificeerd welke activiteiten, producten of diensten zijn uitbesteed.

Deze VVT is bestemd voor alle werknemers van Stichting CINOP - ecbo en haar stakeholders. Het gehanteerde Information Security Management System (ISMS) is van toepassing op de bedrijfsprocessen.

Verantwoordelijkheden
De reikwijdte van de VVT is vastgesteld in samenspraak met bestuur en directie. Met het ondertekenen is het de verantwoordelijkheid van bestuur en directie om de maatregelen te treffen die noodzakelijkerwijs volgen uit het ISMS. Om het ISMS doeltreffend en efficiënt te houden treft de organisatie jaarlijks de nodige maatregelen en acties met de benodigde resources. Toetsing van het ISO 27001 ISMS vindt plaats door geaccrediteerde certificatie instelling.

Namens de Stichting CINOP - ecbo		
Naam	R.H. Koldenhof	*Handtekening* 
Functie	Algemeen directeur / bestuurder	
Plaats	's-Hertogenbosch	
Datum	15 juni 2023	

MET DE ONDERTEKENING ACTIVEERT EN BORGT STICHTING CINOP - ecbo HET NORMENKADER ALS VOLGT:

2 Beheersmaatregel niet van toepassing

ISO 27001:2017 - Annex A

Hoofdstuk 14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Par.	Beheersdoelstelling en beheersmaatregelen	Reden voor niet selecteren
14.2.1	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	CINOP ontwikkelt geen software of systemen en besteed dit ook niet uit. Er wordt gewerkt met SaaS oplossingen.
14.2.2	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	CINOP ontwikkelt geen software of systemen en besteed dit ook niet uit. Er wordt gewerkt met SaaS oplossingen.
14.2.5	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	CINOP ontwikkelt geen software of systemen en besteed dit ook niet uit. Er wordt gewerkt met SaaS oplossingen.
14.2.6	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	CINOP ontwikkelt geen software of systemen en besteed dit ook niet uit. Er wordt gewerkt met SaaS oplossingen.
14.2.7	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	CINOP ontwikkelt geen software of systemen en besteed dit ook niet uit. Er wordt gewerkt met SaaS oplossingen.
14.2.8	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	CINOP ontwikkelt geen software of systemen en besteed dit ook niet uit. Er wordt gewerkt met SaaS oplossingen.

3 Beheersmaatregel van toepassing

Op basis van risicoanalyse is vastgesteld dat de normeisen in onderstaande tabel van toepassing en geïmplementeerd zijn voor Stichting CINOP - ecbo. De tabel beschrijft naast de beheersmaatregelen ook de context die op de eis van toepassing is binnen Stichting CINOP - ecbo, als het gaat om:

- Wet & regelgeving (WR);
- Contractuele verplichtingen (CO);
- Bedrijfseisen (de eigen uitgangspunten en doelstellingen) (BR);
- Risicoanalyse (RA).

ISO 27001:2017 - Annex A

Hoofdstuk 5 Beveiligingsbeleid

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
5.1.1	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.			■	
5.1.2	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.			■	

Hoofdstuk 6 Organiseren van informatiebeveiliging

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.			■	■
6.1.2	Conflicterende taken en verantwoordelijkheden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.			■	■

Hoofdstuk 7 Veilig personeel

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA

6.1.2	Conflicterende taken en verantwoordelijkheden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.			■	■

Hoofdstuk 8 Beheer van bedrijfsmiddelen

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
8.1.1	Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.			■	■
8.1.2	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.		■		
8.1.3	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.		■		
8.1.4	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.		■		
8.2.1	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.				■
8.2.2	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.				■
8.2.3	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.				■
8.3.1	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	■			
8.3.2	Media moeten op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.				■
8.3.3	Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.				■

Hoofdstuk 9 Toegangsbeveiliging

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
9.1.1	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.				■
9.1.2	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.				■
9.2.1	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.				■
9.2.2	Een formele gebruiker-toegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.				■
9.2.3	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.				■
9.2.4	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.				■
9.2.5	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.				■
9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.				■
9.3.1	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.		■	■	
9.4.1	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.				■
9.4.2	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.		■		
9.4.3	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	■		■	■
9.4.4	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.		■		
9.4.5	Toegang tot de programmabroncode moet worden beperkt.	■		■	

Hoofdstuk 10 Cryptografie

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
10.1.1	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.		■		
10.1.2	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.				■

Hoofdstuk 11 Fysieke beveiliging en beveiliging van de omgeving

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
11.1.1	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.				■
11.1.2	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.		■		■
11.1.3	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.		■		■
11.1.4	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.				■
11.1.5	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.				■
11.1.6	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.				■
11.2.1	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.				■
11.2.2	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.				■
11.2.3	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.				■

11.2.4	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.				■
11.2.5	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.		■		
11.2.6	Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.				■
11.2.7	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.				■
11.2.8	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.				■
11.2.9	'Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.				■

Hoofdstuk 12 Beveiliging bedrijfsvoering

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
12.1.1	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.				■
12.1.2	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.				■
12.1.3	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.		■	■	
12.1.4	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.			■	
12.2.1	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.				■
12.3.1	Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.		■	■	■

12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.		■	■	
12.4.2	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.		■		
12.4.3	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.		■		
12.4.4	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.		■		
12.5.1	Om het op operationele systemen installeren van software en moeten procedures worden geïmplementeerd.				■
12.6.1	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.			■	
12.6.2	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.			■	
12.7.1	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.				■

Hoofdstuk 13 Communicatiebeveiliging

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
13.1.1	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.			■	
13.1.2	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.				■
13.1.3	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.				■

13.2.1	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.				■
13.2.2	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.				■
13.2.3	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.				■
13.2.4	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.			■	

Hoofdstuk 14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
14.1.1	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.			■	
14.1.2	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.			■	
14.1.3	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.			■	
14.2.3	Als besturingsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.				■
14.2.4	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.				■
14.2.9	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.				■
14.3.1	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.		■	■	

Hoofdstuk 15 Leveranciersrelaties

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
15.2.1	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.				■
15.2.2	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.				■

Hoofdstuk 16 Beheer van informatie-beveiligingsincidenten

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
16.1.1	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.				■
16.1.2	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.		■		
16.1.3	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.		■		
16.1.4	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.				■
16.1.5	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.				■
16.1.6	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.				■
16.1.7	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.		■		

Hoofdstuk 17 Informatie-beveiligingsaspecten van bedrijfscontinuïteitsbeheer

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
17.1.1	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.		■		
17.1.2	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.		■		
17.1.3	De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.		■		
17.2.1	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.			■	

Hoofdstuk 18 Naleving

Par.	Beheersdoelstelling en beheersmaatregelen	WR	CO	BR	RA
18.1.1	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.		■		
18.1.2	Conflicterende taken en verantwoordelijkheden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.		■		
18.1.3	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.		■		
18.1.4	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.		■		
18.1.5	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.		■		■
18.2.1	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.				■

18.2.2	De directie moet regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	■
18.2.3	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	■