Verklaring van Toepasselijkheid

NEN-EN-ISO/IEC 27001:2022

Colofon

Dit is een uitgave van CINOP

Titel:	Verklaring van Toepasselijkheid
Auteur:	Team ISO
Status:	Definitief
Datum:	3 juni 2025
Project:	Managementsysteem
Classificatie:	Publiek
Pagina's:	13

CINOP volgt de voortdurend veranderende wereld met nieuwsgierige ogen. Wij zien leren en ontwikkelen als hét fundament waarop iedereen kan meedoen én bijdragen aan een inclusieve, veerkrachtige samenleving. Daar zetten we ons dagelijks voor in. Al meer dan 30 jaar!

CINOP B.V.

Postbus 1585

5200 BP 's-Hertogenbosch

Tel: 073-6800800

www.cinop.nl

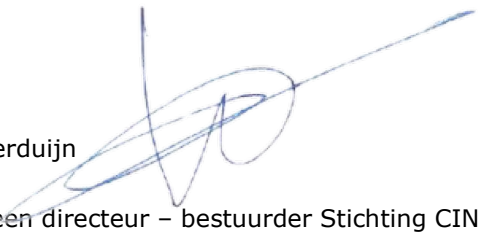
info@cinop.nl

Versiebeheer (geschiedenis document)

Versie	Wijzigingsdatum	Wijziging	Gewijzigd door
0.1	3 juni 2025	Opstellen Vvt ISO 27001:2022	KC
1.0	16 juli 2025	Tekenen VvT	LM
2.0	13 oktober 2025	Tekenen directie	EV

Versiebeheer

Akkoord beleidsstuk te ’s-Hertogenbosch d.d. 13 oktober 2025



Eric Verduijn

Algemeen directeur – bestuurder Stichting CINOP – ecbo.

INHOUD

HOOFDSTUK 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 27001:2022. 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. 3/06/2025 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.

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

HOOFDSTUK 2 – BEHEERSMAATREGEL NIET VAN TOEPASSING

Control	Beheersmaatregels	Reden
A.8.4	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd	CINOP ontwikkelt geen software
A.8.25	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast	CINOP ontwikkelt geen software
A.8.27	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen	CINOP ontwikkelt geen software
A.8.28	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling	CINOP ontwikkelt geen software
A.8.30	De organisatie moet activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen	CINOP ontwikkelt geen software

HOOFDSTUK 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:

- Risicoanalyse (RA);
- Wet & regelgeving (WR);
- Organisatiebeleid (OB).

Control	Beheersmaatregel	RA	WR	OB
Organisatorische maatregelen				
A.5.1	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels behoren te worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	x		x
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie	x		x
A.5.3	Conflicterende taken en conflicterende verantwoordelijkheden voor informatiebeveiliging verminderen	x		x
A.5.4	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid	x		x
A.5.5	De organisatie moet contact met de relevante instanties leggen en onderhouden	x		x
A.5.6	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden	x		x
A.5.7	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren	x		x
A.5.8	Informatiebeveiliging moet worden geïntegreerd in projectmanagement	x		x
A.5.9	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden	x		x
A.5.10	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd	x		x

A.5.11	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	x		x
A.5.12	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden	x		x
A.5.13	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met de informatieclassificatieschema dat is vastgesteld door de organisatie	x		x
A.5.14	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen	x		x
A.5.15	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen	x		x
A.5.16	De volledige levenscyclus van identiteiten moet worden beheerd	x		x
A.5.17	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheersproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	x		x
A.5.18	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden versterkt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie	x		x
A.5.19	Er moeten processen en andere procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen	x		x
A.5.20	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	x		x
A.5.21	Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen	x		
A.5.22	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren	x		x
A.5.23	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld	x		x
A.5.24	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren	x	x	x

A.5.25	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten	x		x
A.5.26	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures	x		x
A.5.27	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren	x		x
A.5.28	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen	x		x
A.5.29	De organisatie moet plannen maken voor het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring	x		x
A.5.30	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen	x		x
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden	x		x
A.5.32	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beheersen	x	x	x
A.5.33	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave	x	x	x
A.5.34	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen		x	x
A.5.35	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld	x		x
A.5.36	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld	x		x
A.5.37	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft	x		x
Mensgerichte beheersmaatregelen				
A.6.1	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's	x		x

A.6.2	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging	x		x
A.6.3	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen	x		x
A.6.4	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid	x		x
A.6.5	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden	x		x
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden	x		x
A.6.7	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen	x		x
A.6.8	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden	x		x
Fysieke beheersmaatregelen				
A.7.1	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken	x		x
A.7.2	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten	x		x
A.7.3	Voor kantoren, ruimten en faciliteiten moeten fysieke beveiliging worden ontworpen en geïmplementeerd	x		x
A.7.4	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde toegang	x		x
A.7.5	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd	x		x
A.7.6	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd	x		x

A.7.7	Er moeten 'clear desk'- regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen	x		x
A.7.8	Apparatuur moet veilig worden geplaatst en beschermd	x		x
A.7.9	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd	x		x
A.7.10	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie	x		x
A.7.11	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen	x		x
A.7.12	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging	x		x
A.7.13	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen	x		x
A.7.14	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt	x		x
Technologische beheersmaatregelen				
A.8.1	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd	x		x
A.8.2	Het toewijzen van het gebruik van speciale toegangsrechten moet worden beperkt en beheerd	x		x
A.8.3	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging	x		x
A.8.4	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd			
A.8.5	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging	x		x
A.8.6	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen	x		x
A.8.7	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn	x		x
A.8.8	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blotstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen	x		x

A.8.9	Configuratie, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld	x		x
A.8.10	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is	x	x	x
A.8.11	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie , rekening houdend met de toepasselijke wetgeving	x	x	x
A.8.12	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd	x		x
A.8.13	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups	x		x
A.8.14	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen	x		x
A.8.15	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd	x		x
A.8.16	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren	x		x
A.8.17	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen	x		x
A.8.18	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moeten worden beperkt en nauwkeurig worden gecontroleerd	x		x
A.8.19	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren	x		x
A.8.20	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen	x		x
A.8.21	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord	x		x
A.8.22	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd	x		x
A.8.23	De toegang tot externe websites moet worden beheerst om de blootstelling aan kwaadaardige inhoud te beperken	x		x
A.8.24	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd	x		x
A.8.25	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast			

A.8.26	Er moeten eisen an informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen	x		x
A.8.27	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen			
A.8.28	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling			
A.8.29	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus	X		X
A.8.30	De organisatie moet activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen			
A.8.31	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd	X		X
A.8.32	Wijzingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer	x		x
A.8.33	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd	x		x
A.8.34	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management			x