TRUSTOOL

Verklaring van Toepasselijkheid

ISO27001:2023
Versie datum: 10 februari 2026
Versie: 1.0

Scope
TrusTool B.V. houdt zich bezig met het ontwerpen, ontwikkelen en onderhouden van een software applicatie ten behoeve van vertrouwenspersonen.

Dit document bevat een overzicht van alle ISO 27001:2023 Annex A beheersmaatregelen, waarbij voor iedere beheersmaatregel is aangegeven of deze van toepassing is en geïmplementeerd is onze organisatie.
Als een beheersmaatregel out of scope is verklaard is een korte verklaring opgenomen.

Nummer ISO 27001:20222	Omschrijving norm	Wet	Contract	Best Practice	Risico analyse	Van toepassing Ja/ Nee	Geïmplementeerd? Ja/Nee	Reden voor uitsluiting
A05	**Organisatorische maatregelen**							
A5.1	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.			Ja	Ja	Ja	Ja	
A5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie			Ja	Ja	Ja	Ja	
A5.3	Conflicterende taken en conflicterende verantwoordelijkheden voor informatiebeveiliging verminderen			Ja	Ja	Ja	Ja	

A5.4	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid			Ja	Ja	Ja	Ja	
A5.5	De organisatie moet contact met de relevante instanties leggen en onderhouden	Ja		Ja	Ja	Ja	Ja	
A5.6	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden			Ja	Ja	Ja	Ja	
A5.7	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren			Ja	Ja	Ja	Ja	
A5.8	Informatiebeveiliging moet worden geïntegreerd in projectmanagement			Ja	Ja	Ja	Ja	
A5.9	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden			Ja	Ja	Ja	Ja	
A5.10	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd			Ja	Ja	Ja	Ja	
A5.11	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.		Ja	Ja	Ja	Ja	Ja	
A5.12	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden			Ja	Ja	Ja	Ja	
A5.13	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met de informatieclassificatieschema dat is vastgesteld door de organisatie			Ja	Ja	Ja	Ja	
A5.14	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			Ja	Ja	Ja	Ja	
A5.15	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			Ja	Ja	Ja	Ja	
A5.16	De volledige levenscyclus van identiteiten moet worden beheerd			Ja	Ja	Ja	Ja	

A5.17	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.			Ja	Ja	Ja	Ja	
A5.18	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			Ja	Ja	Ja	Ja	
A5.19	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			Ja	Ja	Ja	Ja	
A5.20	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.			Ja	Ja	Ja	Ja	
A5.21	Er moten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen			Ja	Ja	Ja	Ja	
A5.22	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren			Ja	Ja	Ja	Ja	
A5.23	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld			Ja	Ja	Ja	Ja	
A5.24	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			Ja	Ja	Ja	Ja	
A5.25	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten			Ja	Ja	Ja	Ja	
A5.26	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures			Ja	Ja	Ja	Ja	
A5.27	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren			Ja	Ja	Ja	Ja	

A5.28	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen			Ja	Ja	Ja	Ja	
A5.29	De organisatie moet plannen maken voor het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring			Ja	Ja	Ja	Ja	
A5.30	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen			Ja	Ja	Ja	Ja	
A5.31	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	Ja	Ja	Ja	Ja	Ja	Ja	
A5.32	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beheersen			Ja	Ja	Ja	Ja	
A5.33	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave			Ja	Ja	Ja	Ja	
A5.34	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	Ja	Ja	Ja	Ja	Ja	Ja	
A5.35	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			Ja	Ja	Ja	Ja	
A5.36	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld			Ja	Ja	Ja	Ja	
A5.37	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft			Ja	Ja	Ja	Ja	
A06	**Mensgerichte maatregelen**							
A6.1	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			Ja	Ja	Ja	Ja	

A6.2	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging			Ja	Ja	Ja	Ja	
A6.3	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			Ja	Ja	Ja	Ja	
A6.4	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			Ja	Ja	Ja	Ja	
A6.5	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		Ja	Ja	Ja	Ja	Ja	
A6.6	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		Ja	Ja	Ja	Ja	Ja	
A6.7	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			Ja	Ja	Ja	Ja	
A6.8	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden			Ja	Ja	Ja	Ja	
A07	**Fysieke maatregelen**							
A7.1	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken			Ja	Ja	Ja	Ja	
A7.2	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten			Ja	Ja	Ja	Ja	
A7.3	Voor kantoren, ruimten en faciliteiten moeten fysieke beveiliging worden ontworpen en geïmplementeerd			Ja	Ja	Ja	Ja	
A7.4	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde toegang			Ja	Ja	Ja	Ja	

A7.5	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd			Ja	Ja	Ja	Ja	
A7.6	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd			Ja	Ja	Ja	Ja	
A7.7	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			Ja	Ja	Ja	Ja	
A7.8	Apparatuur moet veilig worden geplaatst en beschermd			Ja	Ja	Ja	Ja	
A7.9	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd			Ja	Ja	Ja	Ja	
A7.10	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie			Ja	Ja	Ja	Ja	
A7.11	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen			Ja	Ja	Ja	Ja	
A7.12	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging			Ja	Ja	Ja	Ja	
A7.13	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen			Ja	Ja	Ja	Ja	
A7.14	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			Ja	Ja	Ja	Ja	
A08	**Technische maatregelen**							
A8.1	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd			Ja	Ja	Ja	Ja	
A8.2	Het toewijzen van het gebruik van speciale toegangsrechten moet worden beperkt en beheerd			Ja	Ja	Ja	Ja	
A8.3	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging			Ja	Ja	Ja	Ja	

A8.4	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd			Ja	Ja	Ja	Ja	
A8.5	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging			Ja	Ja	Ja	Ja	
A8.6	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen			Ja	Ja	Ja	Ja	
A8.7	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn			Ja	Ja	Ja	Ja	
A8.8	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			Ja	Ja	Ja	Ja	
A8.9	Configuratie, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld			Ja	Ja	Ja	Ja	
A8.10	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is			Ja	Ja	Ja	Ja	
A8.11	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			Ja	Ja	Ja	Ja	
A8.12	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd			Ja	Ja	Ja	Ja	
A8.13	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups			Ja	Ja	Ja	Ja	
A8.14	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen			Ja	Ja	Ja	Ja	
A8.15	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd			Ja	Ja	Ja	Ja	
A8.16	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren			Ja	Ja	Ja	Ja	
A8.17	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen			Ja	Ja	Ja	Ja	

A8.18	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moeten worden beperkt en nauwkeurig worden gecontroleerd			Ja	Ja	Ja	Ja	
A8.19	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren			Ja	Ja	Ja	Ja	
A8.20	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen			Ja	Ja	Ja	Ja	
A8.21	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord			Ja	Ja	Ja	Ja	
A8.22	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd			Ja	Ja	Ja	Ja	
A8.23	De toegang tot externe websites moet worden beheerst om de blootstelling aan kwaadaardige inhoud te beperken			Ja	Ja	Ja	Ja	
A8.24	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd			Ja	Ja	Ja	Ja	
A8.25	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast							De software ontwikkeling is volledig uitbesteed aan een derde met ISO 27001:2022 certificering
A8.26	Er moeten eisen aan informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen			Ja	Ja	Ja	Ja	
A8.27	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen							De software ontwikkeling is volledig uitbesteed aan een derde met ISO 27001:2022 certificering
A8.28	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling							De software ontwikkeling is volledig uitbesteed aan een derde met ISO 27001:2022 certificering
A8.29	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus							De software ontwikkeling is volledig uitbesteed aan een derde met ISO 27001:2022 certificering
A8.30	De organisatie moet activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen			Ja	Ja	Ja	Ja	
A8.31	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd							De software ontwikkeling is volledig uitbesteed aan een

								derde met ISO 27001:2022 certificering
A8.32	Wijzingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer			Ja	Ja	Ja	Ja	
A8.33	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd							De software ontwikkeling is volledig uitbesteed aan een derde met ISO 27001:2022 certificering
A8.34	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management							De software ontwikkeling is volledig uitbesteed aan een derde met ISO 27001:2022 certificering