Checklist verschillen

NEN 7510:2024 - De nieuwe norm

vicoconnect.com

versie 1.05

Checklist verschillen

NEN 7510:2024 - De nieuwe norm

Organisaties, die al zijn gecertificeerd voor NEN 7510, hebben twee jaar de tijd om over te stappen naar de nieuwe norm. Dit betekent dat jouw organisatie voor 20 februari 2027 moet zijn gecertificeerd voor NEN 7510:2024. Weet je niet waar te beginnen? Geen zorgen, wij helpen je op weg en zetten hier de belangrijkste veranderingen op een rij.

Rianne Nijhuis
Lead auditor

T +316 30 38 94 12
E rianne.nijhuis@vicoconnect.com

Charlotte Adama
Lead auditor

T +316 43 20 88 86
E charlotte.adama@vicoconnect.com

Overstap service van Vico

Liever hulp bij het overstappen naar de nieuwe norm? Maak gebruik van de overstap service van Vico. Wij geven onafhankelijk advies en benaderen de overstap pragmatisch. Met oog voor praktijk en resultaat en altijd in samenwerking met jou en je collega's.

Wat verandert er?

De nieuwe NEN 7510-1 norm is opgebouwd volgens de ‘Harmonized Structure (HS)’. Dit betekent o.a. dat hoofdstuk 6.3 “Planning van wijzigingen” is toegevoegd. En dat het ISO-amendement met betrekking tot klimaatverandering, dat is opgenomen in hoofdstuk 4 van de HS, is opgenomen in deze nieuwe versie van de NEN 7510.

Echter vind je de voornaamste wijzigingen terug in ***Bijlage A***. Hier zijn nieuwe beveiligingsmaatregelen geïntroduceerd, aangepast of samengevoegd. Het totaal aantal beheersmaatregelen is van 114 naar 93 gegaan. Het aantal zorgspecifieke maatregelen is van van 3 naar 8 gegaan. En het aantal reguliere beheersmaatregelen met zorgspecifieke aanvulling van 33 naar 14 maatregelen.

Verder is de bijlage uitgebreid met cyberbeveiliging en privacy-aspecten en is de controleterminologie vernieuwd met toegevoegde richtlijnen. Dit alles helpt bedrijven bij risicobeheer, zorgt voor overzicht en waarborgt een effectieve opvolging.

In dit document vind je een overzicht hoe de gespecificeerde beheersmaatregelen uit de oude norm corresponderen met de beheersmaatregelen uit de nieuwe norm. Ben je ook op zoek naar een overzicht van welke stappen je moet doorlopen? Kijk op ***www.vicoconnect.com/nen-7510*** voor een stappenplan.

Checklist verschillen NEN 7510

Onderstaand overzicht is gebaseerd op bijlage B van de NEN 7510-2:2024. De tabel laat zien hoe de gespecificeerde beheersmaatregelen uit de oude norm corresponderen met de beheersmaatregelen uit de nieuwe norm.

NEN 7510-1:2017	NEN 7510-1:2024
A.5 Informatiebeveiligingsbeleid	
A.5.1 Aansturing door de directie van de informatiebeveiliging	
A.5.1.1 Beleidsregels voor informatiebeveiliging	5.1 Beleidsregels voor informatiebeveiliging
A.5.1.2 Beoordelen van het informatie-beveiligingsbeleid	5.1 Beleidsregels voor informatiebeveiliging
A.6 Organiseren van informatiebeveiliging	
A.6.1 Interne organisatie	
A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	**5.2** Rollen en verantwoordelijkheden bij informatie-beveiliging
A.6.1.2 Scheiding van taken	**5.3** Functiescheiding
A.6.1.3 Contact met overheidsinstanties	**5.5** Contact met overheidsinstanties
A.6.1.4 Contact met speciale belangengroepen	**5.6** Contact met speciale belangengroepen
A.6.1.5 Informatiebeveiliging in projectbeheer	**5.8** Informatiebeveiliging in projectmanagement
A.6.2 Mobiele apparatuur en telewerken	
A.6.2.1 Beleid voor mobiele apparatuur	**8.1** 'User endpoint devices'
A.6.2.2 Telewerken	**6.7** Werken op afstand
A.7 Veilig personeel	
A.7.1 Voorafgaand aan het dienstverband	
A.7.1.1 Screening	**6.1** Screening
A.7.1.2 Arbeidsvoorwaarden	6.2 Arbeidsovereenkomst
A.7.2 Tijdens het dienstverband	
A.7.2.1 Directieverantwoordelijkheden	**5.4** Managementverantwoordelijkheden
A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	**6.3** Bewustwording van, opleiding en training in informatiebeveiliging
A.7.2.3 Disciplinaire procedure	**6.4** Disciplinaire procedure
A.7.3 Beëindiging en wijziging van dienstverband	
A.7.3.1 Beëindiging of wijziging van verantwoorde-lijkheden van het dienstverband	**6.5** Verantwoordelijkheden na beëindiging of wijziging van het dienstverband

Vico connect

NEN 7510-1:2017	NEN 7510-1:2024
A.8 Beheer van bedrijfsmiddelen	
A.8.1 Verantwoordelijkheid voor bedrijfsmiddelen	
A.8.1.1 Inventariseren van bedrijfsmiddelen	**5.9** Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen
A.8.1.2 Eigendom van bedrijfsmiddelen	**5.9** Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen
A.8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen	**5.10** Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen
A.8.1.4 Teruggeven van bedrijfsmiddelen	**5.11** Retourneren van bedrijfsmiddelen
A.8.2 Informatieclassificatie	
A.8.2.1 Classificatie van informatie	**5.12** Classificeren van informatie
A.8.2.2 Informatie labelen	**5.13** Labelen van informatie
A.8.2.3 Behandelen van bedrijfsmiddelen	**5.10** Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen
A.8.3 Behandelen van media	
A.8.3.1 Beheer van verwijderbare media	**7.10** Opslagmedia
A.8.3.2 Verwijderen van media	**7.10** Opslagmedia
A.8.3.3 Media fysiek overdragen	**7.10** Opslagmedia
A.9 Toegangsbeveiliging	
A.9.1 Bedrijfseisen voor toegangsbeveiliging	
A.9.1.1 Beleid voor toegangsbeveiliging	**5.15** Toegangsbeveiliging
A.9.1.2 Toegang tot netwerken en netwerkdiensten	**5.15** Toegangsbeveiliging
A.9.2 Beheer van toegangsrechten van gebruikers	
A.9.2.1 Registratie en uitschrijving van gebruikers	**5.16** Identiteitsbeheer
A.9.2.2 Gebruikers toegang verlenen	**5.18** Toegangsrechten
A.9.2.3 Beheren van speciale toegangsrechten	**8.2** Speciale toegangsrechten
A.9.2.4 Beheer van geheime authenticatieinformatie van gebruikers	**5.17** Authenticatie-informatie
A.9.2.5 Beoordeling van toegangsrechten van gebruikers	**5.18** Toegangsrechten
A.9.2.6 Toegangsrechten intrekken of aanpassen	**5.18** Toegangsrechten
A.9.3 Gebruikersverantwoordelijkheden	
A.9.3.1 Geheime authenticatie-informatie gebruiken	**5.17** Authenticatie-informatie

NEN 7510-1:2017	NEN 7510-1:2024
A.9.4 Toegangsbeveiliging van systeem en toepassing	
A.9.4.1 Beperking toegang tot informatie	**8.3** Beperking toegang tot informatie
A.9.4.2 Beveiligde inlogprocedures	**8.5** Beveiligde authenticatie
A.9.4.3 Systeem voor wachtwoordbeheer	**5.17** Authenticatie-informatie
A.9.4.4 Speciale systeemhulpmiddelen gebruiken	**8.18** Gebruik van speciale systeemhulpmiddelen
A.9.4.5 Toegangsbeveiliging op programma-broncode	**8.4** Toegangsbeveiliging op broncode
A.10 Cryptografie	
A.10.1 Cryptografische beheersmaatregelen	
A.10.1.1 Beleid inzake het gebruik van crypto-grafische beheersmaatregelen	8.24 Gebruik van cryptografie
A.10.1.2 Sleutelbeheer	8.24 Gebruik van cryptografie
A.11 Fysieke beveiliging en beveiliging van de omgeving	
A.11.1 Beveiligde gebieden	
A.11.1.1 Fysieke beveiligingszone	7.1 Fysieke beveiligingszones
A.11.1.2 Fysieke toegangsbeveiliging	7.2 Fysieke toegangsbeveiliging
A.11.1.3 Kantoren, ruimten en faciliteiten beveiligen	7.3 Beveiligen van kantoren, ruimten en faciliteiten
A.11.1.4 Beschermen tegen bedreigingen van buitenaf	7.5 Beschermen tegen fysieke en omgevings-dreigingen
A.11.1.5 Werken in beveiligde gebieden	7.6 Werken in beveiligde zones
A.11.1.6 Laad- en loslocatie	7.2 Fysieke toegangsbeveiliging
A.11.2 Apparatuur	
A.11.2.1 Plaatsing en bescherming van apparatuur	**7.8** Plaatsen en beschermen van apparatuur
A.11.2.2 Nutsvoorzieningen	**7.11** Nutsvoorzieningen
A.11.2.3 Beveiliging van bekabeling	**7.12** Beveiligen van bekabeling
A.11.2.4 Onderhoud van apparatuur	**7.13** Onderhoud van apparatuur
A.11.2.5 Verwijdering van bedrijfsmiddelen	**7.10** Opslagmedia
A.11.2.6 Beveiliging van apparatuur en bedrijfsmid-delen buiten het terrein	**7.9** Beveiligen van bedrijfsmiddelen buiten het terrein
A.11.2.7 Veilig verwijderen of hergebruiken van apparatuur	**7.14** Veilig verwijderen of hergebruiken van apparatuur
A.11.2.8 Onbeheerde gebruikersapparatuur	**8.1** 'User endpoint devices'
A.11.2.9 'Clear desk'- en 'clear screen'-beleid	**7.7** 'Clear desk' en 'clear screen'

NEN 7510-1:2017	NEN 7510-1:2024
A.12 Beveiliging bedrijfsvoering	
A.12.1 Bedieningsprocedures en verantwoordelijkheden	
A.12.1.1 Gedocumenteerde bedieningsprocedures	**5.37** Gedocumenteerde bedieningsprocedures
A.12.1.2 Wijzigingsbeheer	**8.32** Wijzigingsbeheer
A.12.1.3 Capaciteitsbeheer	**8.6** Capaciteitsbeheer
A.12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen	**8.31** Scheiding van ontwikkel-, test- en productie-omgevingen
A.12.2 Bescherming tegen malware	
A.12.2.1 Beheersmaatregelen tegen malware	**8.7** Bescherming tegen malware
A.12.3 Back-up	
A.12.3.1 Back-up van informatie	**8.13** Back-up van informatie
A.12.4 Verslaglegging en monitoren	
A.12.4.1 Gebeurtenissen registreren	**8.15** Logging
A.12.4.2 Beschermen van informatie in log-bestanden	**8.15** Logging
A.12.4.3 Logbestanden van beheerders en opera-tors	**8.15** Logging
A.12.4.4 Kloksynchronisatie	**8.17** Kloksynchronisatie
A.12.5 Beheersing van operationele software	
A.12.5.1 Software installeren op operationele systemen	**8.19** Installeren van software op operationele systemen
A.12.6 Beheer van technische kwetsbaarheden	
A.12.6.1 Beheer van technische kwetsbaarheden	**8.8** Beheer van technische kwetsbaarheden
A.12.6.2 Beperkingen voor het installeren van soft-ware	**8.19** Installeren van software op operationele systemen
A.12.7 Overwegingen betreffende audits van informatiesystemen	
A.12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen	**8.34** Bescherming van informatiesystemen tijdens audits
A.13 Communicatiebeveiliging	
A.13.1 Beheer van netwerkbeveiliging	
A.13.1.1 Beheersmaatregelen voor netwerken	**8.20** Beveiliging netwerkcomponenten
A.13.1.2 Beveiliging van netwerkdiensten	**8.21** Beveiliging van netwerkdiensten
A.13.1.3 Scheiding in netwerken	**8.22** Netwerksegmentatie

NEN 7510-1:2017	NEN 7510-1:2024
A.13.2 Informatietransport	
A.13.2.1 Beleid en procedures voor informatie-transport	**5.14** Overdragen van informatie
A.13.2.2 Overeenkomsten over informatietransport	**5.14** Overdragen van informatie
A.13.2.3 Elektronische berichten	**5.14** Overdragen van informatie
A.13.2.4 Vertrouwelijkheids- of geheimhoudings-overeenkomst	**6.6** Vertrouwelijkheids- of geheimhoudingsovereen-komsten
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen	
A.14.1 Beveiligingseisen voor informatiesystemen	
A.14.1.1 Analyse en specificatie van informatie-beveiligingseisen	**5.8** Informatiebeveiliging in projectmanagement
A.14.1.1.1 Zorgontvangers op unieke wijze identificeren	**5.39** HLT – Zorgontvangers op unieke wijze identificeren
A.14.1.1.2 Validatie van outputgegevens	**8.26** Toepassingsbeveiligingseisen
A.14.1.2 Toepassingsdiensten op openbare netwer-ken beveiligen	**8.26** Toepassingsbeveiligingseisen
A.14.1.3 Transacties van toepassingsdiensten beschermen	**8.26** Toepassingsbeveiligingseisen
A.14.1.3.1 Openbaar beschikbare gezondheids-informatie	**5.41** HLT – Openbaar beschikbare gezondheids-informatie
A.14.2 Beveiliging in ontwikkelings- en ondersteunende processen	
A.14.2.1 Beleid voor beveiligd ontwikkelen	**8.25** Beveiligen tijdens de ontwikkelcyclus
A.14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen	**8.32** Wijzigingsbeheer
A.14.2.3 Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	**8.32** Wijzigingsbeheer
A.14.2.4 Beperkingen op wijzigingen aan software-pakketten	**8.32** Wijzigingsbeheer
A.14.2.5 Principes voor engineering van beveiligde systemen	**8.27** Veilige systeemarchitectuur en technische uitgangspunten
A.14.2.6 Beveiligde ontwikkelomgeving	**8.31** Scheiding van ontwikkel-, test- en productie-omgevingen
A.14.2.7 Uitbestede softwareontwikkeling	**8.30** Uitbestede systeemontwikkeling
A.14.2.8 Testen van systeembeveiliging	**8.29** Testen van de beveiliging tijdens ontwikkeling en acceptatie
A.14.2.9 Systeemacceptatietests	**8.29** Testen van de beveiliging tijdens ontwikkeling en acceptatie

NEN 7510-1:2017	NEN 7510-1:2024
A.14.3 Testgegevens	
A.14.3.1 Bescherming van testgegevens	**8.33** Testgegevens
A.15 Leveranciersrelaties	
A.15.1 Informatiebeveiliging in leveranciersrelaties	
A.15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties	**5.19** Informatiebeveiliging in leveranciersrelaties
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	**5.20** Adresseren van informatiebeveiliging in leveranciersovereenkomsten
A.15.1.3 Toeleveringsketen van informatie- en communicatietechnologie	**5.21** Beheren van informatiebeveiliging in de ICT-toeleveringsketen
A.15.2 Beheer van dienstverlening van leveranciers	
A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	**5.22** Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten
A.15.2.2 Beheer van veranderingen in dienstverlening van leveranciers	**5.22** Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten
A.16 Beheer van informatiebeveiligingsincidenten	
A.16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	
A.16.1.1 Verantwoordelijkheden en procedures	**5.24** Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten
A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen	**6.8** Melden van informatiebeveiligingsgebeurtenissen
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	**6.8** Melden van informatiebeveiligingsgebeurtenissen
A.16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	**5.25** Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen
A.16.1.5 Respons op informatiebeveiligingsincidenten	**5.26** Reageren op informatiebeveiligingsincidenten
A.16.1.6 Lering uit informatiebeveiligingsincidenten	**5.27** Leren van informatiebeveiligingsincidenten
A.16.1.7 Verzamelen van bewijsmateriaal	**5.28** Verzamelen van bewijsmateriaal
A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	
A.17.1 Informatiebeveiligingscontinuïteit	
A.17.1.1 Informatiebeveiligingscontinuïteit plannen	**5.29** Informatiebeveiliging tijdens een verstoring
A.17.1.2 Informatiebeveiligingscontinuïteit implementeren	**5.29** Informatiebeveiliging tijdens een verstoring
A.17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	**5.29** Informatiebeveiliging tijdens een verstoring

NEN 7510-1:2017	NEN 7510-1:2024
A.17.2 Redundante componenten	
A.17.2.1 Beschikbaarheid van informatie verwerkende faciliteiten	**8.14** Redundantie van informatie verwerkende faciliteiten
A.18 Naleving	
A.18.1 Naleving van wettelijke en contractuele eisen	
A.18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen	**5.31** Wettelijke, statutaire, regelgevende en contractuele eisen
A.18.1.2 Intellectuele eigendomsrechten	**5.32** Intellectuele-eigendomsrechten
A.18.1.3 Beschermen van registraties	**5.33** Beschermen van registraties
A.18.1.4 Privacy en bescherming van persoonsgegevens	**5.34** Privacy en bescherming van persoonsgegevens
A.18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen	**5.31** Wettelijke, statutaire, regelgevende en contractuele eisen
A.18.2 Informatiebeveiligingsbeoordelingen	
A.18.2.1 Onafhankelijke beoordeling van informatiebeveiliging	**5.35** Onafhankelijke beoordeling van informatiebeveiliging
A.18.2.2 Naleving van beveiligingsbeleid en -normen	**5.36** Naleving van beleid, regels en normen voor informatiebeveiliging
A.18.2.3 Beoordeling van technische naleving	**5.36** Naleving van beleid, regels en normen voor informatiebeveiliging **8.8** Beheer van technische kwetsbaarheden

Overeenstemming tussen
NEN 7510-1:2024 en NEN 7510-1:2017

Hieronder vind je de verschillen tussen de nieuwe norm en de oude norm:

NEN 7510-1:2024	NEN 7510-1:2017
5. Organisatorische beheersmaatregelen	
5.1 Beleidsregels voor informatiebeveiliging	
A.5.1.1 Beleidsregels voor informatiebeveiliging	**A.5.1.1** Beleidsregels voor informatiebeveiliging **A.5.1.2** Beoordelen van het informatie-beveiligingsbeleid
5.2 Rollen en verantwoordelijkheden bij informatie-beveiliging	**A.6.1.1** Rollen en verantwoordelijkheden bij informa-tiebeveiliging
5.3 Functiescheiding	**A.6.1.2** Scheiding van taken
5.4 Managementverantwoordelijkheden	**A.7.2.1** Directieverantwoordelijkheden
5.5 Contact met overheidsinstanties	**A.6.1.3** Contact met overheidsinstanties
5.6 Contact met speciale belangengroepen	**A.6.1.4** Contact met speciale belangengroepen
5.7 Informatie en analyses over dreigingen	***NIEUW***
5.8 Informatiebeveiliging in projectmanagement	**A.6.1.5** Informatiebeveiliging in projectbeheer **A.14.1.1** Analyse en specificatie van informatie-beveiligingseisen
5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	**A.8.1.1** Inventariseren van bedrijfsmiddelen **A.8.1.2** Eigendom van bedrijfsmiddelen
5.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	**A.8.1.3** Aanvaardbaar gebruik van bedrijfsmiddelen **A.8.2.3** Behandelen van bedrijfsmiddelen
5.11 Retourneren van bedrijfsmiddelen	**A.8.1.4** Teruggeven van bedrijfsmiddelen
5.12 Classificeren van informatie	**A.8.2.1** Classificatie van informatie
5.13 Labelen van informatie	**A.8.2.2** Informatie labelen
5.14 Overdragen van informatie	**A.13.2.1** Beleid en procedures voor informatie-transport **A.13.2.2** Overeenkomsten over informatietransport **A.13.2.3** Elektronische berichten
5.15 Toegangsbeveiliging	**A.9.1.1** Beleid voor toegangsbeveiliging **A.9.1.2** Toegang tot netwerken en netwerkdiensten

NEN 7510-1:2024	NEN 7510-1:2017
5.16 Identiteitsbeheer	**A.9.2.1** Registratie en uitschrijving van gebruikers
5.17 Authenticatie-informatie	**A.9.2.4** Beheer van geheime authenticatie informatie van gebruikers **A.9.3.1** Geheime authenticatie-informatie gebruiken **A.9.4.3** Systeem voor wachtwoordbeheer
5.18 Toegangsrechten	**A.9.2.2** Gebruikers toegang verlenen **A.9.2.5** Beoordeling van toegangsrechten van gebruikers **A.9.2.6** Toegangsrechten intrekken of aanpassen
5.19 Informatiebeveiliging in leveranciersrelaties	**A.15.1.1** Informatiebeveiligingsbeleid voor leveranciersrelaties
5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten	**A.15.1.2** Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
5.21 Beheren van informatiebeveiliging in de ICT-toeleveringsketen	**A.15.1.3** Toeleveringsketen van informatie- en communicatietechnologie
5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	**A.15.2.1** Monitoring en beoordeling van dienstverlening van leveranciers **A.15.2.2** Beheer van veranderingen in dienstverlening van leveranciers
5.23 Informatiebeveiliging voor het gebruik van clouddiensten	***NIEUW***
5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	**A.16.1.1** Verantwoordelijkheden en procedures
5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	**A.16.1.4** Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
5.26 Reageren op informatiebeveiligingsincidenten	**A.16.1.5** Respons op informatiebeveiligingsincidenten
5.27 Leren van informatiebeveiligingsincidenten	**A.16.1.6** Lering uit informatiebeveiligingsincidenten
5.28 Verzamelen van bewijsmateriaal	**A.16.1.7** Verzamelen van bewijsmateriaal
5.29 Informatiebeveiliging tijdens een verstoring	**A.17.1.1** Informatiebeveiligingscontinuïteit plannen **A.17.1.2** Informatiebeveiligingscontinuïteit implementeren **A.17.1.3** Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren
5.30 ICT-gereedheid voor bedrijfscontinuïteit	***NIEUW***

NEN 7510-1:2024	NEN 7510-1:2017
5.31 Wettelijke, statutaire, regelgevende en contractuele eisen	**A.18.1.1** Vaststellen van toepasselijke wetgeving en contractuele eisen **A.18.1.5** Voorschriften voor het gebruik van cryptografische beheersmaatregelen
5.32 Intellectuele-eigendomsrechten	**A.18.1.2** Intellectuele eigendomsrechten
5.33 Beschermen van registraties	**A.18.1.3** Beschermen van registraties
5.34 Privacy en bescherming van persoonsgegevens	**A.18.1.4** Privacy en bescherming van persoonsgegevens
5.35 Onafhankelijke beoordeling van informatiebeveiliging	**A.18.2.1** Onafhankelijke beoordeling van informatiebeveiliging
5.36 Naleving van beleid, regels en normen voor informatiebeveiliging	**A.18.2.2** Naleving van beveiligingsbeleid en -normen
	A.18.2.3 Beoordeling van technische naleving
5.37 Gedocumenteerde bedieningsprocedures	**A.12.1.1** Gedocumenteerde bedieningsprocedures
5.38 HLT – Analyse en specificatie van informatiebeveiligingseisen	***NIEUW***
5.39 HLT – Zorgontvangers op unieke wijze identificeren	**14.1.1.1** Zorgontvangers op unieke wijze identificeren
5.40 HLT – Validatie van getoonde/geprinte gegevens	**14.1.1.2** Validatie van outputgegevens
5.41 HLT – Openbaar beschikbare gezondheidsinformatie	**14.1.3.1** Openbaar beschikbare gezondheidsinformatie
5.42 HLT – Communicatie in noodsituaties	***NIEUW***
5.43 HLT – Incidenten extern melden	***NIEUW***

NEN 7510-1:2024	NEN 7510-1:2017
6. Mensgerichte beheersmaatregelen	
6.1 Screening	**A.7.1.1** Screening
6.2 Arbeidsovereenkomst	**A.7.1.2** Arbeidsvoorwaarden
6.3 Bewustwording van, opleiding en training in informatiebeveiliging	**A.7.2.2** Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
6.4 Disciplinaire procedure	**A.7.2.3** Disciplinaire procedure
6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	**A.7.3.1** Beëindiging of wijziging van verantwoordelijkheden van het dienstverband
6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten	**A.13.2.4** Vertrouwelijkheids- of geheimhoudingsovereenkomst
6.7 Werken op afstand	**A.6.2.2** Telewerken
6.8 Melden van informatiebeveiligingsgebeurtenissen	**A.16.1.2** Rapportage van informatiebeveiligingsgebeurtenissen **A.16.1.3** Rapportage van zwakke plekken in de informatiebeveiliging
6.9 HLT – Managementtraining	***NIEUW***
7. Fysieke beheersmaatregelen	
7.1 Fysieke beveiligingszones	**A.11.1.1** Fysieke beveiligingszone
7.2 Fysieke toegangsbeveiliging	**A.11.1.2** Fysieke toegangsbeveiliging **A.11.1.6** Laad- en loslocatie
7.3 Beveiligen van kantoren, ruimten en faciliteiten	**A.11.1.3** Kantoren, ruimten en faciliteiten beveiligen
7.4 Monitoren van fysieke beveiliging	***NIEUW***
7.5 Beschermen tegen fysieke en omgevingsdreigingen	**A.11.1.4** Beschermen tegen bedreigingen van buitenaf
7.6 Werken in beveiligde zones	**A.11.1.5** Werken in beveiligde gebieden
7.7 'Clear desk' en 'clear screen'	**A.11.2.9** 'Clear desk'- en 'clear screen'-beleid
7.8 Plaatsen en beschermen van apparatuur	**A.11.2.1** Plaatsing en bescherming van apparatuur
7.9 Beveiligen van bedrijfsmiddelen buiten het terrein	**A.11.2.6** Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein
7.10 Opslagmedia	**A.8.3.1** Beheer van verwijderbare media **A.8.3.2** Verwijderen van media **A.8.3.3** Media fysiek overdragen **A.11.2.5** Verwijdering van bedrijfsmiddelen
7.11 Nutsvoorzieningen	**A.11.2.2** Nutsvoorzieningen
7.12 Beveiligen van bekabeling	**A.11.2.3** Beveiliging van bekabeling
7.13 Onderhoud van apparatuur	**A.11.2.4** Onderhoud van apparatuur
7.14 Veilig verwijderen of hergebruiken van apparatuur	**A.11.2.7** Veilig verwijderen of hergebruiken van apparatuur

NEN 7510-1:2024	NEN 7510-1:2017
8. Technologische beheersmaatregelen	
8.1 'User endpoint devices'	**A.6.2.1** Beleid voor mobiele apparatuur **A.11.2.8** Onbeheerde gebruikersapparatuur
8.2 Speciale toegangsrechten	**A.9.2.3** Beheren van speciale toegangsrechten
8.3 Beperking toegang tot informatie	**A.9.4.1** Beperking toegang tot informatie
8.4 Toegangsbeveiliging op broncode	**A.9.4.5** Toegangsbeveiliging op programmabroncode
8.5 Beveiligde authenticatie	**A.9.4.2** Beveiligde inlogprocedures
8.6 Capaciteitsbeheer	**A.12.1.3** Capaciteitsbeheer
8.7 Bescherming tegen malware	**A.12.2.1** Beheersmaatregelen tegen malware
8.8 Beheer van technische kwetsbaarheden	**A.12.6.1** Beheer van technische kwetsbaarheden **A.18.2.3** Beoordeling van technische naleving
8.9 Configuratiebeheer	***NIEUW***
8.10 Wissen van informatie	***NIEUW***
8.11 Maskeren van gegevens	***NIEUW***
8.12 Voorkomen van gegevenslekken (data leakage prevention)	***NIEUW***
8.13 Back-up van informatie	**A.12.3.1** Back-up van informatie
8.14 Redundantie van informatieverwerkende faciliteiten	**A.17.2.1** Beschikbaarheid van informatieverwerkende faciliteiten
8.15 Logging	**A.12.4.1** Gebeurtenissen registreren **A.12.4.2** Beschermen van informatie in logbestanden **A.12.4.3** Logbestanden van beheerders en operators
8.16 Monitoren van activiteiten	***NIEUW***
8.17 Kloksynchronisatie	**A.12.4.4** Kloksynchronisatie
8.18 Gebruik van speciale systeemhulpmiddelen	**A.9.4.4** Speciale systeemhulpmiddelen gebruiken
8.19 Installeren van software op operationele systemen	**A.12.5.1** Software installeren op operationele systemen **A.12.6.2** Beperkingen voor het installeren van software
8.20 Beveiliging netwerkcomponenten	**A.13.1.1** Beheersmaatregelen voor netwerken
8.21 Beveiliging van netwerkdiensten	**A.13.1.2** Beveiliging van netwerkdiensten
8.22 Netwerksegmentatie	**A.13.1.3** Scheiding in netwerken
8.23 Toepassen van webfilters	***NIEUW***
8.24 Gebruik van cryptografie	**A.10.1.1** Beleid inzake het gebruik van cryptografische beheersmaatregelen **A.10.1.2** Sleutelbeheer
8.25 Beveiligen tijens de ontwikkelcyclus	**A.14.2.1** Beleid voor beveiligd ontwikkelen

NEN 7510-1:2024	NEN 7510-1:2017
8.26 Toepassingsbeveiligingseisen	**A.14.1.2** Toepassingsdiensten op openbare netwerken beveiligen **A.14.1.3** Transacties van toepassingsdiensten beschermen
8.27 Veilige systeemarchitectuur en technische uitgangspunten	**A.14.2.5** Principes voor engineering van beveiligde systemen
8.28 Veilig coderen	***NIEUW***
8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie	**A.14.2.8** Testen van systeembeveiliging **A.14.2.9** Systeemacceptatietests
8.30 Uitbestede systeemontwikkeling	**A.14.2.7** Uitbestede softwareontwikkeling
8.31 Scheiding van ontwikkel-, test- en productieomgevingen	**A.12.1.4** Scheiding van ontwikkel-, test- en productieomgevingen **A.14.2.6** Beveiligde ontwikkelomgeving
8.32 Wijzigingsbeheer	**A.12.1.2** Wijzigingsbeheer **A.14.2.2** Procedures voor wijzigingsbeheer met betrekking tot systemen **A.14.2.3** Technische beoordeling van toepassingen na wijzigingen bedieningsplatform **A.14.2.4** Beperkingen op wijzigingen aan softwarepakketten
8.33 Testgegevens	**A.14.3.1** Bescherming van testgegevens
8.34 Bescherming van informatiesystemen tijdens audits	**A.12.7.1** Beheersmaatregelen betreffende audits van informatiesystemen
8.35 HLT – Zero trust-beginselen	***NIEUW***

Over Vico Connect

Vico Connect helpt organisaties met het behalen en behouden van (ISO) certificeringen. Wij maken een vertaalslag van certificeringseisen en zorgen voor een werkbare toepassing. Dit doen wij met pragmatische adviseurs en eigen proces-management software.

Wij zijn ervaren Lead auditors met een bedrijfskundige achter-grond. Onze kennis over (ISO) certificeringen is altijd up-to-date. Wij ontwerpen de benodigde managementsystemen voor jouw organisatie en begeleiden je bij de implementatie.

Ons advies is pragmatisch. Wij zorgen ervoor dat onze oplossingen aansluiten op de huidige werkwijze van jouw organisatie, dus geen grote veranderingen. Met onze kennis en software maken we de bedrijfsvoering makkelijker en plezieriger binnen wetgeving en normeisen.

Wij laten ons inspireren door de Italiaanse filosoof Giambattista Vico. Hij pleitte voor het gebruik van metaforen om complexe zaken duidelijk te maken.

Wij gebruiken ons procesmodel als metafoor om de organisatie helder in kaart te brengen. Dit model geeft inzicht en overzicht voor iedereen. Ons geoptimaliseerde procesmodel fungeert als de verbindende schakel tussen medewerkers en de systemen die zij gebruiken.

Vico connect

Vico Connect B.V.

T +31 55 303 49 79

E info@vicoconnect.com

vicoconnect.com