Aanvullende auditverklaring en onderbouwende rapportage

|  |  |
| --- | --- |
| Organisatie (kandidaat-) deelnemer: | Invulling : |
| Datum: | Invulling : |
| Auditor: | Invulling : |
| CBI: | Invulling : |

**Inleiding**

Alle deelnemers in het MedMij afsprakenstelsel dienen in het bezit te zijn van een geldige NEN 7510-certificering, ongeacht hun grootte en of ze dienstverlener in het persoonsdomein of zorgaanbiedersdomein zijn. Ook de beheerorganisatie zal voor de uitvoering van haar diensten binnen het MedMij netwerk gebonden zijn aan de NEN 7510-norm. Gebruik van NEN 7510:2011 voor certificatiedoeleinden onder accreditatie blijft mogelijk tot medio 2020, te weten 2 jaar na publicatie van het certificatieschema NCS 7510:2018. Dit nieuwe certificatieschema behorend bij NEN 7510:2017 is begin juni 2018 gepubliceerd. MedMij stelt de volgende eisen aan een NEN 7510-certificering voor deelnemers:

* De Dienstverlener zorgaanbieder moet de zorgaanbieders als belangrijke belanghebbenden hebben geïdentificeerd in het uitvoeren/herijken van de risicoanalyse (zie ook hetgeen over de rollen en verantwoordelijkheden ten opzichte van de verwerking van persoonsgegevens is opgenomen in de [Juridische context](https://afsprakenstelsel.medmij.nl/display/PUBLIC/Juridische+context));
* Het MedMij Afsprakenstelsel moet onder, dan wel binnen, de scope van het NEN 7510-certificaat vallen;
* Bij de selectie van de van toepassing zijnde maatregelen dienen ten minste de maatregelen uit het Normenkader informatiebeveiliging te zijn opgenomen;
* Indien de maatregel een implementatie voorschrijft, dient de maatregel op deze wijze te worden geïmplementeerd. De deelnemer heeft dit middels een self assessment gecontroleerd en onderbouwd. Hiervoor kan het format voor de onderbouwende rapportage als hulpmiddel dienen.

De deelnemer toont jaarlijks met een **aanvullende auditverklaring met een onderbouwende rapportage**aan te voldoen aan het Normenkader informatiebeveiliging MedMij. Voor de onderbouwende rapportage bij de auditverklaring wordt door MedMij dit format beschikbaar gesteld. Bij de beoordeling kan gebruik gemaakt worden van het tevens gepubliceerde beoordelingskader. In de rapportage is ruimte om aan te geven of de betreffende partij conform de norm werkt. Er wordt vooral een toelichting vereist bij non-conformiteit. Blijkt uit de aanvullende auditverklaring dat de deelnemer niet (meer) voldoet, dan beoordeelt de Stichting MedMij op basis van de onderbouwende rapportage of en op welke manier het [Nalevingsbeleid](https://afsprakenstelsel.medmij.nl/display/PUBLIC/Nalevingsbeleid) moet worden toegepast.

De NEN 7510-certificering en de aanvullende auditverklaring met rapportage dienen te worden afgegeven door een Conformiteit Beoordelende Instelling (CBI), die NEN 7510 geaccrediteerd is door de Raad voor Accreditatie of een NEN 7510 licentieovereenkomst heeft met NEN. Tevens dient het NEN 7510 certificaat te zijn opgenomen in het door NEN beheerde nationale certificatenregister NEN 7510. Voor het NEN 7510 certificaat gelden de door NEN aangehouden termijnen voor hercertificering.

**ALGEMEEN**

##### Organisatiegegevens

Naam organisatie: Invulling :

Adres (hoofdlocatie): Invulling :

Invulling :

Vertegenwoordigd door: Invulling :

Rol:DVP/DVZA

##### Certificatiegegevens NEN 7510

Norm: Invulling :

Scope: Invulling :

Vervaldatum certificaat:  Invulling :

Certificaatnummer: Invulling :

##### Auditgegevens

Bezochte locatie(s): Invulling :

Auditdata: Invulling :

Lead Auditor: Invulling :

Teamleden: Invulling :

##### Rapportgegevens

Datum rapport: Invulling :

Status rapport: Invulling :

##### Bijlagen bij dit rapport

Bijlage 1: Invulling :

**Verklaring**

Hierbij verklaart ***“Naam Conformiteit Beoordelende Instelling”*** (CBI) dat **“*Naam Organisatie”*** wel/niet\*[[1]](#footnote-1) voldoet aan het aanvullend normenkader informatiebeveiliging, [release 1.1](https://afsprakenstelsel.medmij.nl/display/PUBLIC/Normenkader+informatiebeveiliging).1 MedMij afsprakenstelsel, zoals door Stichting MedMij is uitgegeven.

***“Datum”***

***“Naam auditor”***

***“Handtekening auditor”***

***“Naam vertegenwoordiger CBI”***

***“Handtekening vertegenwoordiger CBI”***

**Onderbouwende rapportage**

|  |  |  |
| --- | --- | --- |
| **A.5.1.1** | **Beleidsregels voor informatiebeveiliging** | |
| **Deze maatregel borgt dat het Afsprakenstelsel wordt toegepast in beleid en maatregelen bij de deelnemers.** | | |
| De beleidsdocumenten van deelnemers dienen de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek te benoemen. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.6.1.1** | **Rollen en verantwoordelijkheden bij informatiebeveiliging** | |
| **Deze maatregel borgt dat bij (dreiging van) calamiteiten door alle partijen daadkrachtig kan worden gereageerd. Zie ook A.12.4.1 Gebeurtenissen registreren en A.16.1.1 Verantwoordelijkheden en procedures.** | | |
| Elke deelnemer en de beheerorganisatie dient (eind)verantwoordelijkheid voor informatiebeveiliging te beleggen. Deze functionaris(sen) dient/dienen mandaat te hebben om bij een (dreiging van een) crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren, eventueel door een onderaannemer.  De verantwoordelijke en operationele functionaris(sen) (inclusief eventuele onderaannemers) dient/dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur. (Conform de betreffende Deelnemersovereenkomsten). | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.7.2.2** | **Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging** | |
| **Deze maatregel borgt dat medewerkers zich bewust zijn van de werking van MedMij en de ketenverantwoordelijkheden.** | | |
| Elke contactpersoon van de deelnemer die werkzaamheden verricht gerelateerd aan MedMij dient deelgenomen te hebben aan de training over de algemene werking van het stelsel. Deze training wordt door de beheerorganisatie beheerd en gefaciliteerd.  Overige medewerkers van de deelnemer die werkzaamheden verrichten gerelateerd aan MedMij dienen een training te hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen. Deze training mag door de contactpersoon van de deelnemer zelf beheerd en gefaciliteerd worden. Deze norm mag ook ingevuld worden doordat de medewerkers deelnemen aan de training gegeven door de beheerorganisatie.  *Opmerking: de genoemde ‘contactpersoon’ betreft in principe een ‘eindverantwoordelijke functionaris’ zoals genoemd in norm A.6.1.1.* | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.8.2.1** | **Classificatie van informatie** | |
| **Deze maatregel borgt dat informatie die binnen het stelsel wordt gebruikt, door deelnemers met dezelfde voorzichtigheid wordt behandeld.** | | |
| De gegevens die de deelnemer binnen het stelsel verwerkt en uitwisselt, worden behandeld conform het Informatieclassificatiebeleid (van MedMij). | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.9.1.1** | **Beleid voor toegangsbeveiliging** | |
| **Deze maatregel borgt dat persoonlijke gezondheidsgegevens alleen toegankelijk zijn voor de zorgaanbieder en de zorggebruiker (zie ook A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen).** | | |
| Het inzien van persoonlijke gezondheidsgegevens door (medewerkers van) deelnemers en door de beheerorganisatie is niet toegestaan. Er dienen passende technische maatregelen te worden genomen om dit te voorkomen. De deelnemer dient minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stelen dat deze technische maatregelen nog effectief zijn.  In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens wellicht niet te voorkomen. Hiervoor dient de deelnemer een (nood)procedure te documenteren. Deze procedure dient in te gaan op:   * Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris. * Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze. * Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij afsprakenstelsel. * Vastlegging en verantwoording van de getroffen acties. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.9.2.5** | **Beoordeling van toegangsrechten van gebruikers** | |
| **Deze maatregel borgt dat partijen regelmatig controleren of alleen gerechtigde gebruikers toegang hebben tot relevante IT-componenten (waaronder servers, databases en netwerkinfrastructuur).** | | |
| Twee-factor authenticatie wordt afgedwongen op IT-componenten die persoonlijke gezondsheidsgegevens opslaan of verwerken. Let op: Het betreft toegang tot IT-componenten, geen toegang tot de persoonlijke gezondheidsgegevens zelf.  Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden opgeslagen of worden verwerkt dienen (minimaal) maandelijks te worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers. Hierbij dient functiescheiding gewaarborgd te zijn.  Daarnaast dient het gebruik van deze toegangsrechten betrouwbaar te worden gelogd. Deze logging dient tevens (minimaal) maandelijks te worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers. Hierbij dient functiescheiding gewaarborgd te zijn. Tijdens deze controle moet aandacht zijn voor:   * onterecht/onnodig gebruik door medewerkers (met aantoonbare opvolging) * medewerkers die geen gebruik (meer) maken van de toegangsrechten. Deze rechten kunnen dus mogelijk worden verwijderd). | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.9.4.1** | **Beperking toegang tot informatie** | |
| **Deze maatregel borgt dat authenticatie van personen en autorisatie tot hun persoonlijke gegevens betrouwbaar plaatsvindt.** | | |
| Authenticatie van personen (eindgebruikers) vindt plaats op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.10.1.1** | **Beleid inzake het gebruik van cryptografische beheersmaatregelen** | |
| **Deze maatregel borgt dat bij het versleutelen van persoonlijke gezondheidsgegevens gebruik wordt gemaakt van als veilig aangemerkte algoritmen.** | | |
| Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van disk-level en/of database-level encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de ENCRYPT-CSA aanbevelingen, zie hieronder.  Een overzicht van publicaties is te vinden op https://www.keylength.com/ Er kan gebruik gemaakt worden van de ENCRYPT-CSA aanbevelingen en/of die van het BSI. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.12.1.2** | **Wijzigingsbeheer** | |
| **Deze maatregel borgt dat wijzigingen binnen de keten beheerst verlopen. Zie ook A.12.5.1 Software installeren op operationele systemen.** | | |
| De IT-beheerprocessen van deelnemers en de beheerorganisatie dienen aan te sluiten op het MedMij Change- en releasebeleid.  Wijzigingen worden conform het gedocumenteerde proces afgehandeld.  Indien significante code wijzigingen zullen worden doorgevoerd, dan laten de deelnemer en beheerorganisatie vooraf een code review uitvoeren door een externe, onafhankelijke organisatie. Voor toetreding heeft deze minimaal al een keer plaatsgevonden. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.12.1.3** | **Capaciteitsbeheer** | |
| **Deze maatregel borgt dat alle systemen in de keten voldoen aan de afgesproken eisen omtrent beschikbaarheid.** | | |
| Maatregelen zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in “Gegevens en performance in UCI Verzamelen en UCI Delen” | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.12.3.1** | **Back-up van informatie** | |
| **Deze maatregel borgt dat deelnemers gegevens van personen binnen aanvaardbare tijd hersteld kunnen worden.** | | |
| De dienstverlener persoon dient maatregelen te hebben geïmplementeerd te hebben waardoor het gegevensverlies van een persoon maximaal 24 uur bedraagt.  Daarnaast dient een herstelprocedure te zijn ingericht waardoor de gegevens van de persoon binnen 24 uur terug kunnen worden geplaatst in geval van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.12.4.1** | **Gebeurtenissen registreren** | |
| **Deze maatregel borgt dat relevante security gebeurtenissen in systemen van de deelnemers en de beheerorganisatie (zoals het verlenen van toestemming aan zorgaanbieder door de zorggebruiker, het inzien of wijzigen van een PGO of het wijzigen aan loggen van gebruikers aan hun PGO) ten minste 12 maanden inzichtelijk blijven.** | | |
| 1. Logging moet plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Processen en informatie onder Logging)  2. Daarnaast worden de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar gelogd:   * De actie waarbij de persoon via de PGO bij de DVZA gegevens wil opvragen. * De acties waarbij de persoon toestemming geeft voor de uitwisseling. te worden vastgelegd. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.12.4.4** | **Kloksynchronisatie** | |
| **Deze maatregel borgt dat tijdsvermeldingen in logbestanden gelijklopen, wanneer deze worden gebruikt om misbruik in de keten op te sporen. Zie ook A.16.1.7 Verzamelen van bewijsmateriaal.** | | |
| De klokken van IT componenten die communiceren via MedMij en logging in het kader van MedMij bijhouden moeten worden gesynchroniseerd met pool.ntp.org. Het is toegestaan te synchroniseren met een lokale NTP-server, zolang deze ten minste 1x per 24 uur synchroniseert met bovengenoemde NTP-server. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.12.5.1** | **Software installeren op operationele systemen** | |
| **Deze maatregel borgt dat er altijd twee medewerkers betrokken zijn bij werkzaamheden aan systemen (configuratiewijzigingen, onderhoud, installatie van updates) die direct impact (kunnen) hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten. De maatregel vermindert het risico op onbeschikbaarheid van of kwetsbaarheden binnen de keten.** | | |
| Niet-standaard wijzigingen op de IT componenten die gebruikt worden in relatie tot MedMij dienen op basis van het vier-ogen-principe te worden uitgevoerd. | | |
| **Beoordeling** | | |
| Invulling : | | Non-conformiteit |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.12.6.1** | **Beheer van technische kwetsbaarheden** | |
| **Deze maatregel borgt dat deelnemers in staat zijn tijdig te reageren op meldingen van (vermeende) kwetsbaarheden in het MedMij stelsel.**  **Zie ook A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging.** | | |
| Deelnemers dienen een procedure in te richten zodat technische kwetsbaarheden worden beheerst conform de operationele processen in het afsprakenstelsel. De procedure dient minimaal in te gaan op de volgende stappen: identificeren van kwetsbaarheden, onderzoeken van relevantie voor de eigen systemen, terugkoppeling naar de beheerorganisatie en het patchen van systemen (of anderzijds mitigeren van de kwetsbaarheid, zie ook (zie A.12.5.1 Software installeren op operationele systemen), en het tijdig kunnen doorlopen van de gehele procedure bij hoog risico kwetsbaarheden. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.14.2.1** | **Beleid voor beveiligd ontwikkelen** | |
| **Deze maatregel borgt dat deelnemers en beheerorganisatie beveiligingsstandaarden toepassen bij het ontwikkelen van software en systemen die aan het internet gekoppeld worden. Dit voorkomt dat bekende programmeerfouten worden gemaakt.** | | |
| Voor ontwikkelde webapplicaties ten behoeve van de MedMij dienstverlening worden minimaal de ICT- Beveiligingsrichtlijnen voor webapplicaties van het NCSC gehanteerd. In het bijzonder zijn dan de maatregelen uit het "Uitvoeringsdomein" van belang, <https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html>.  *Opmerking: voor mobiele applicaties kunnen in aanvulling hierop de volgende richtlijnen van het NCSC worden gehanteerd: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-mobiele-apps.html.* | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.16.1.1** | **Verantwoordelijkheden en procedures** | |
| **Deze maatregel borgt dat deelnemers en beheerorganisatie volgens hetzelfde proces handelen in geval van incidenten en calamiteiten. Zie ook A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging.** | | |
| Deelnemers dienen een procedure in te richten zodat incidenten en calamiteiten worden beheerst conform de operationele processen in het afsprakenstelsel. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.16.1.3** | **Rapportage van zwakke plekken in de informatiebeveiliging** | |
| **Deze maatregel borgt dat alle partijen elkaar tijdig op de hoogte brengen wanneer zij kennis hebben over kwetsbaarheden, die relevant kan zijn voor het MedMij stelsel. Het kan hier bijvoorbeeld gaan om informatie verkregen via het NCSC, penetratietesten of een Responsible Disclosure-melding). Zie ook A.12.6.1 Beheer van technische kwetsbaarheden.** | | |
| Er is een meldplicht voor alle deelnemers en de beheerorganisatie om kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel binnen 48 uur te melden bij centrale incident management team. Zie Deelnemersovereenkomsten. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.16.1.7** | **Verzamelen van bewijsmateriaal** | |
| **Deze maatregel borgt dat alle partijen moeten meewerken aan forensische onderzoeken, bijvoorbeeld in de nasleep van een stelselincident of fraude. Het zal meestal gaan om het opleveren van logfiles (zie A.12.4.1 Gebeurtenissen registreren).** | | |
| Deelnemers en de beheerorganisatie dienen medewerking te verlenen aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

|  |  |  |
| --- | --- | --- |
| **A.18.2.3** | **Beoordeling van technische naleving** | |
| **Deze maatregel borgt dat deelnemers en de beheerorganisatie met regelmaat (en gebruikmakend van verschillende partijen) hun software, systemen en infrastructuur laten toetsen op bekende kwetsbaarheden.** | | |
| 1. Tenminste jaarlijks laten de deelnemers en de beheerorganisatie whitebox applicatiepenetratietesten uitvoeren op de externe koppelvlakken door een externe, onafhankelijke organisatie. Voor toetreding heeft deze minimaal al een keer plaatsgevonden.  Naar aanleiding van het resultaat stellen de deelnemers en de beheerorganisatie een adequaat actieplan op voor minimaal de hoge en midden risico's relevant voor de MedMij dienstverlening. Deelnemers sturen dit actieplan zo spoedig mogelijk (beveiligd) naar de beheerorganisatie. De deelnemer voert de corrigerende maatregelen tijdig door.  Bij eerste toetreding mogen er geen hoog en middel risico bevindingen openstaan op externe MedMij koppelvlakken.  2.Tenminste jaarlijks laat de beheerorganisatie blackbox infrastructuur penetratietesten uitvoeren op de externe koppelvlakken van de deelnemers ten behoeve van het MedMij stelsel. Naar aanleiding van het resultaat stelt de beheerorganisatie een adequaat actieplan op voor minimaal de hoge en midden risico's relevant voor de MedMij dienstverlening. De beheerorganisatie en waar relevant de deelnemers voeren de corrigerende maatregelen tijdig door. | | |
| **Beoordeling** | | |
| Invulling : | | Conform wel/ niet |
|  |
| **Evidence** | | |
| Invulling : | | |

**Kruisverwijzing NEN 7510:2017 – NEN 7510:2011**

|  |  |  |  |
| --- | --- | --- | --- |
| NEN 7510:2017 | Titel NEN 7510:2017 | NEN 7510:2011 | Titel NEN 7510:2011 |
| A.5.1.1 | Beleidsregels voor informatiebeveiliging | **A.5.1.1** | Beleidsdocument voor informatiebeveiliging |
| A.6.1.1 | Rollen en verantwoordelijkheden bij informatiebeveiliging | **A.6.1.3** | Toewijzing van verantwoordelijkheden voor informatiebeveiliging |
|  |  | **A.8.1.1** | Rollen en verantwoordelijkheden |
| A.7.2.2 | Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging | **A.8.2.2** | Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging |
| A.8.2.1 | Classificatie van informatie | **A.7.2.1** | Richtlijnen voor classificatie |
| A.9.1.1 | Beleid voor toegangsbeveiliging | **A.11.1.1** | Toegangsbeleid |
| A.9.2.5 | Beoordeling van toegangsrechten van gebruikers | **A.11.2.4** | Beoordeling van toegangsrechten van gebruikers |
| A.9.4.1 | Beperking toegang tot informatie | **A.11.5.2** | Gebruikersindentificatie en -authenticatie |
| A.10.1.1 | Beleid inzake het gebruik van cryptografische beheersmaatregelen | **A.12.3.1** | Beleid voor het gebruik van cryptografische beheersmaatregelen |
| A.12.1.2 | Wijzigingsbeheer | **A.10.1.2** | Wijzigingsbeheer |
| A.12.1.3 | Capaciteitsbeheer | **A.10.3.1** | Capaciteitsbeheer |
| A.12.3.1 | Back-up van informatie | **A.10.5.1** | Reservekopieën (back-ups) |
| A.12.4.1 | Gebeurtenissen registreren | **A.10.10.1** | Aanmaken audit-logbestanden |
| A.12.4.4 | Kloksynchronisatie | **A.10.10.6** | Synchronisatie van systeemklokken |
| A.12.5.1 | Software installeren op operationele systemen | **A.12.4.1** | Beheersing van operationele programmatuur |
| A.12.6.1 | Beheer van technische kwetsbaarheden | **A.12.6.1** | Beheersing van technische kwetsbaarheden |
| A.14.2.1 | Beleid voor beveiligd ontwikkelen | **Deze maatregel bestond nog niet in NEN 7510:2011** | |
| A.16.1.1 | Verantwoordelijkheden en procedures | **A.13.2.1** | Verantwoordelijkheden en procedures |
| A.16.1.3 | Rapportage van zwakke plekken in de informatiebeveiliging | **A.13.1.2** | Rapportage van zwakke plekken in de beveiliging |
| A.16.1.7 | Verzamelen van bewijsmateriaal | **A.13.2.3** | Verzamelen van bewijsmateriaal |
| A.18.2.3 | Beoordeling van technische naleving | **A.15.2.2** | Controle op technische naleving |

# **Disclaimer**

De uitkomsten van deze toetsing zijn vermeld in dit rapport en zijn tijdens de eindbespreking ter inzage verstrekt aan en besproken met het management van de klant.

Het conceptrapport is door de klant beoordeeld alvorens het definitieve rapport door de Conformiteit Beoordelende Instelling aan de klant ter beschikking wordt gesteld.

Het is verboden dit document op enige manier te wijzigen of op te splitsen.

De Conformiteit Beoordelende Instelling is niet aansprakelijk voor enige directe, indirecte, bijkomstige of gevolgschade ontstaan door of bij het gebruik van de informatie of gegevens uit dit document of door onmogelijkheid die informatie of gegevens te gebruiken.

De audit is gebaseerd op een proces opzet, bestaan en werking op basis van steekproeven uit de beschikbare informatie. De audit betreft geen opzichzelfstaande certificering en is onlosmakelijk verbonden met de NEN 7510-certificering.

De inhoud van dit document mag slechts als één geheel aan derden kenbaar worden gemaakt, voorzien van bovengenoemde aanduidingen met betrekking tot auteursrechten, aansprakelijkheid, aanpassingen en rechtsgeldigheid.

De Conformiteit Beoordelende Instelling aanvaardt geen verantwoordelijkheid of aansprakelijkheid jegens derden aangezien het rapport niet is opgesteld, en ook niet is bestemd, voor enig ander doel dan hiervoor omschreven.

1. \* doorhalen wat niet van toepassing is. [↑](#footnote-ref-1)