|  |
| --- |
| Beoordelingskader:  Aanvullende auditverklaring en 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. | | |
| **Auditmethode:** | | * Stel vast dat in de beleidsdocumenten het privacy en informatiebeveiligingsbeleid van MedMij specifiek is opgenomen. * Stel vast dat dit beleid is uitgewerkt in maatregelen. * Stel minimaal door middel van interviews met de betrokken medewerkers vast of de maatregelen worden toegepast. Dit geldt ook voor eventuele onderaannemers. |
| **Verificatie:** | | - Welke beleidsdocumenten (incl. versienummer) zijn onderzocht.  - Welke documenten zijn onderzocht die de maatregelen beschrijven.  - Met wie gesproken is ter bevestiging van toepassing van de maatregelen. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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). | | |
| **Auditmethode:** | | - Stel op basis van evidence vast dat de genoemde functionaris(sen) is/zijn aangewezen.  - Stel vast dat een procedure is ingericht zodat de genoemde beschikbaarheid, tijdens kantooruren binnen een uur en buiten kantooruren binnen drie uur, te allen tijde gegarandeerd is op dit onderwerp. Indien van toepassing dient deze procedure onderaannemers te omvatten.  De beschikbaarheid dient tevens gegarandeerd te zijn bij geplande en ongeplande afwezigheid.  - Stel door middel van interviews vast dat de functionaris(sen) op de hoogte is/zijn van hun taken en verantwoordelijkheden t.a.v. de beschikbaarheid en het juiste mandaat hebben. |
| **Verificatie:** | | - In welke documentatie de verantwoordelijkheden en bevoegdheden zijn belegd.  - Welke procedure (incl. versienummer) is ingezien m.b.t. de beschikbaarheid  - Met wie gesproken is ter bevestiging van de implementatie. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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.* | | |
| **Auditmethode:** | | - Verkrijg een overzicht van alle contactpersonen die betrokken zijn bij MedMij gerelateerde werkzaamheden en stel op basis van het bewijs van deelname vast dat alle personen de training gegeven door de beheerorganisatie hebben gevolgd.  - Verkrijg een overzicht van alle overige medewerkers die betrokken zijn bij MedMij gerelateerde werkzaamheden. Stel op basis van het bewijs van deelname vast dat deze personen ofwel de training hebben gevolgd die wordt gegeven door de beheerorganisatie, ofwel een training hebben gevolgd gegeven door de contactpersoon.  - Indien van toepassing, stel vast dat de training gegeven door de contactpersoon de volgende aspecten voldoende behandeld: de werking van MedMij, de ketenverantwoordelijkheden en de voor de medewerker van toepassing zijnde beveiligingsmaatregelen. |
| **Verificatie:** | | - Het overzicht van contactpersonen en overige medewerkers - Evidence m.b.t. de gevolgde training. |
| **Rapportage** | | Leg vast hoeveel medewerkers betrokken zijn bij de werking van MedMij en hoeveel medewerkers de training, en op welke wijze zij deze, hebben gevolgd. |

|  |  |  |
| --- | --- | --- |
| **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) | | |
| **Auditmethode:** | | - Stel vast dat de classificatie van gegevens binnen de organisatie, voor de gegevens die binnen het stelsel worden uitgewisseld, overeenstemt met de classificatie zoals door MedMij benoemd in het Informatieclassificatiebeleid van MedMij.  - Stel vast dat de verwerking van de gegevens door de deelnemer daadwerkelijk plaatsvindt conform het Informatieclassificatiebeleid van MedMij. Hierbij ligt de focus op: gezondheidsgegevens, metagegevens, operationele gegevens, risicoanalyses, pentestrapporten en de whitelist. Dit geldt ook voor eventuele onderaannemers. |
| **Verificatie:** | | - Welke versie van het Informatieclassificatieschema is ingezien. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel vast dat het technisch onmogelijk is gemaakt dat (medewerkers van) partijen zich inzage kunnen verschaffen in persoonlijke gezondheidsgegevens. Dit geldt ook voor eventuele onderaannemers.  - Stel vast dat de self assessment minimaal elk halfjaar en na grote wijzigingen is uitgevoerd.  - Stel vast dat de (nood)procedure is opgesteld en effectief is (m.a.w. geen toegang is verkregen zonder toepassing van de procedure).  - Indien inzage heeft plaatsgevonden: Controleer de vastlegging en verantwoording |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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). | | |
| **Auditmethode:** | | - Stel op basis van de procedures en systeemobservaties vast dat twee-factor authenticatie wordt afgedwongen op servers, databases en netwerkinfrastructuur die persoonlijke gezondsheidsgegevens opslaan of verwerken.  - Stel op basis van de procedures vast dat toegangsrechten op servers, databases en netwerkinfrastructuur waar persoonlijke gezondheidsgegevens worden opgeslagen of worden verwerkt maandelijks gecontroleerd worden. Dit geldt ook voor de logging van deze IT-componenten en ook voor eventuele onderaannemers..  Stel vast dat de functionaris(sen) die deze controle uitvoert/uitvoeren geen toegangsrechten verstrekken en/of zelf (beheer)toegang hebben tot de IT-componenten.  De controle van toegangsrechten en logging mag ook geautomatiseerd plaatsvinden. Stel dan vast dat configureren van de geautomatiseerde controle(s) juist en volledig plaatsvindt. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel vast dat (minimaal) twee factor authenticatie van personen technisch afgedwongen wordt.  - Stel vast dat voldoende maatregelen zijn ingericht die waarborgen dat na succesvolle authenticatie de personen alleen toegang krijgen tot hun eigen persoonlijke gezondheidsgegevens. Ondersteunende evidence omvat bijvoorbeeld gedocumenteerde use-cases, het uitvoeren van een ‘walk through’ vanuit het perspectief van de eindgebruiker en de uitkomsten van de code-review en penetratietest. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel op basis van de architectuurdiagrammen vast of er wordt voldaan aan de aanbevelingen die gelden voor 'near term protection' en 'long-term protection’ volgens de ENCRYPT-CSA aanbevelingen.  - Stel op basis van een steekproef vast of aanbevelingen ook daadwerkelijk geïmplementeerd zijn. |
| **Verificatie:** | | - Welke versie van de aanbevelingen is gehanteerd.  - Welke versie van de architectuurdiagrammen zijn ingezien.  - Evidence m.b.t. de daadwerkelijke implementatie. |
| **Rapportage** | | - Beschrijf de uitgevoerde controles en de omvang van de steekproef. |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel vast dat IT-beheerprocessen van de organisatie aansluiten op het Change- en releasebeleid van MedMij.  - Stel op basis van een steekproef vast dat de IT-beheerprocessen voor MedMij juist worden uitgevoerd. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien.  - Evidence m.b.t. de daadwerkelijke implementatie. |
| **Rapportage** | | - Benoem welke recente Change/Release beoordeeld is. |

|  |  |  |
| --- | --- | --- |
| **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” | | |
| **Auditmethode:** | | - Stel op basis van IT-monitoring en/of service level rapportages vast dat over een periode van drie maanden voorafgaand aan de auditdatum voldaan is aan de beschikbaarheidseisen. |
| **Verificatie:** | | - Evidence m.b.t. de rapportages. |
| **Rapportage** | | - Benoem de betreffende percentages. |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel vast dat de organisatie maatregelen heeft ingericht waardoor gegevensverlies is beperkt tot maximaal 24 uur. Dit zijn bijvoorbeeld backups en/of heet repliceren van gegevens.  - Stel vast dat de herstelprocedure binnen 24u uitgevoegd kan worden en minimaal jaarlijks wordt getest.  -stel daaarnaast via monitoring en rapportages vast dat de leverancier voldoet |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien.  - Evidence m.b.t. de (minimaal) jaarlijkse test. |
| **Rapportage** | | - Benoem de datum van de meest recente recovery procedures test. - Benoem het resultaat de test. |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | 1) Stel vast of de logbestanden voldoen aan de voorwaarden van het afsprakenstelsel (zie Processen en informatie onder Logging).  2) Stel vast hoe de onweerlegbaarheid en controleerbaarheid van de logs over personen is ingericht. Stel vast dat deze altijd minimaal 12 maanden beschikbar blijven.  Zie toelichting bij punt 8 en 9 onder "Architectuur en technische specificaties\Applicatie\ Gegevens en performance in UCI Verzamelen en UCI Delen" |
| **Verificatie:** | | - Evidence m.b.t. de logbestanden.  - Evidence m.b.t. aansluiting. |
| **Rapportage** | | - Benoem de gehanteerde bewaartermijn van de logbestanden. |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel voor de relevante systemen voor het MedMij afsprakenstelsel vast via  de logging\* en/ of configuratie instellingen dat de synchronisatie met pool.ntp.org ten minste 1x per 24 uur plaats vindt. Dan wel middels een verklaring van een lokale NTP server over de synchronisatieprocedure met genoemde NTP-server.  \* Meting over een periode van 7 dagen voorafgaand aan de auditdatum. |
| **Verificatie:** | | - Evidence m.b.t. de logbestanden en/ of configuratie instellingen. |
| **Rapportage** | | - Benoem over welke periode de controle heeft plaats gevonden. |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel vast dat een overzicht van standaard en niet-standaard wijzigingen is gedocumenteerd. Ga na of standaardwijzigingen geen midden/hoog risico hebben op op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten.  -Stel vast dat vier-ogen-principe is ingericht voor niet-standaard wijzigingen.  - Stel door middel van interview met de betrokken medewerkers vast of de procedures worden nageleefd. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien.  - Met wie gesproken is ter bevestiging van de implementatie. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | Stel vast dat de organisatie in haar procedures aansluit op het proces van beheren van technische kwetsbaarheden uit het afsprakenstelsel van MedMij.   Stel door middel van interview met de betrokken medewerkers vast of de procedures worden nageleefd. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien.  - Met wie gesproken is ter bevestiging van de implementatie. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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.* | | |
| **Auditmethode:** | | Stel vast dat de organisatie in haar procedures met betrekking tot de ontwikkeling, de door MedMij gedefinieerde minimale beveiligingsstandaarden (‘Uitvoeringsdomein’) heeft opgenomen.  Stel op basis van evidence vast dat bij de ontwikkeling de procedures met betrekking tot de toepassing van minimale beveilingsstandaarden (‘Uitvoeringsdomein’) zijn toegepast. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien  - Met wie gesproken is ter bevestiging van de toepassing van de procedures. |
| **Rapportage** | | - Benoem welke versies van beveiligingsrichtlijnen in de procedures zijn opgenomen.  - Beschrijf de gehanteerde wijze van controle voor het vaststellen of de procedures met betrekking tot de minimale beveiligingsrichtlijnen zijn toegepast bij de ontwikkeling. |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | Stel vast dat de organisatie in haar procedures aansluit op het proces van incidenten en calamiteiten uit het afsprakenstelsel van MedMij.   Stel door middel van interview met de betrokken medewerkers en waar mogelijk onderbouwd met evidence vast of de procedures worden nageleefd. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien  - Met wie gesproken is ter bevestiging van de implementatie.  - Evidence m.b.t. de daadwerkelijke implementatie. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel vast dat de organisatie in haar procedures aansluit op het proces van incidenten en calamiteiten en proces beheren technische kwetsbaarheden uit het afsprakenstelsel van MedMij.  - Stel door middel van interview met de betrokken medewerkers en waar mogelijk onderbouwd met evidence vast of de procedures worden nageleefd.  - Stel door middel van interview en evidence vast of de deelnemer alle ontdekte kwetsbaarheden tijdig heeft gemeld aan MedMij. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien.  - Met wie gesproken is ter bevestiging van de implementatie.  - Evidence m.b.t. ondekte kwetsbaarheden en tijdige melding aan MedMij. |
| **Rapportage** | | - Benoem of er kwetsbaarheden zijn ontdekt door de deelnemer en of deze tijdig zijn gemeld. |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | Stel vast dat de organisatie in haar procedures het verlenen van medewerking aan (forensische) onderzoeken heeft opgenomen.   Stel door middel van interview met de betrokken medewerkers en waar mogelijk onderbouwd met evidence vast of de procedures worden nageleefd. |
| **Verificatie:** | | - Welke procedures (incl. versienummers) zijn ingezien.  - Met wie gesproken is ter bevestiging van de implementatie.  - Evidence m.b.t. de implementatie. |
| **Rapportage** | |  |

|  |  |  |
| --- | --- | --- |
| **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. | | |
| **Auditmethode:** | | - Stel op basis van de meest recente rapportages vast of er wordt voldaan aan de jaarlijkse whitebox applicatiepenetratietesten op de externe koppelvlakken conform de architectuur en specificaties van MedMij (en louter binnen de scope van het MedMij afsprakenstelsel). Bij toetreding hebben deze testen minimaal al een keer plaatsgevonden.  - Stel door middel van evidence vast of de kwetsbaarheden bij de beheerorganisatie zijn gemeld. Ook dienen de midden/hoog risico’s tijdig te zijn verholpen.  - Stel op basis van de meest recente rapportages vast of er wordt voldaan aan de jaarlijkse blackbox infrastructuur penetratietesten op de externe koppelvlakken conform de architectuur en specificaties van MedMij (en louter binnen de scope van het MedMij afsprakenstelsel). |
| **Verificatie:** | | - Evidence m.b.t. de uitgevoerde jaarlijkse testen.  - Met wie gesproken is ter bevestiging van de implementatie.  - Evidence m.b.t. het melden van kwetsbaarheden |
| **Rapportage** | | - Benoem de datum van de meest recente uitgevoerde testen.  - Benoem de resultaten van de test. |

**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 |