TOOLS4EVER

Whitepaper V2.0 / 08 04 2025

NEN 7510: 2024

en de rol van Identity Management

Inhoudsopgave

Inleiding 1
Van ISO 27001 en ISO 27002 naar NEN 7510 2
Controls en overheidsmaatregelen 3
Identity Management en NEN 7510 3
Provisioning van gebruiksaccounts en -rechten 3
Automation: standaardisatie met ruimte voor uitzonderingen 4
Access Management 5
Cloud based Identity Management met hoge beschikbaarheid 5
Governance 6
Meer weten? 6
Over Tools4ever 7
Bijlage 8
Checklist NEN 7510:2024 - HelloID 8

Inleiding

NEN 7510 is een Nederlandse informatiebeveiligingsnorm die specifiek is bedoeld voor organisaties die persoonlijke gezondheidsinformatie verwerken. Voor cliënten en patiënten is het natuurlijk enorm belangrijk dat medische gegevens zorgvuldig worden beheerd en dat zorgmedewerkers alleen toegang hebben tot zulke gegevens ten behoeve van de behandeling en zorg. De Autoriteit Persoonsgegevens rangschikt patiëntgegevens dan ook onder de categorie 'bijzondere persoonsgegevens' die extra beschermd moeten worden.

Tegelijkertijd zijn voor de beveiliging van medische gegevens natuurlijk ook veel beveiligingsmaatregelen nodig die ook al voor 'gewone gegevens' worden gebruikt. Bovendien verwerken zorgorganisaties natuurlijk niet alleen maar bijzondere persoonsgegevens. Men zocht dus voor medische organisaties naar beveiligingsrichtlijnen die zo goed mogelijk aansluiten op algemeen geaccepteerde informatiebeveiligingsnormen. NEN 7510 is daarom ontwikkeld als een naadloze aanvulling op ISO 27001, de internationale standaard voor informatiebeveiliging.

ISO 27001 helpt organisaties een managementsysteem voor informatiebeveiliging in te richten met daarin alle noodzakelijke beveiligingsmaatregelen. NEN 7510 vult deze basisrichtlijnen aan met aanvullende (of meer gedetailleerde) maatregelen waarmee ook de specifieke medische gegevens voldoende worden beveiligd. De maatregelen richten zich vooral op een zorgvuldige omgang met patiëntgegevens, een veilige toegang tot die gegevens en een goede registratie van alle handelingen met de data. Ook gaat het niet alleen om de verwerking van medische gegevens binnen een zorginstelling, maar ook de uitwisseling van gegevens tussen zorginstellingen onderling en met toeleveranciers en externe dienstverleners. Ook zulke niet-medische organisaties zullen in dat geval vaak moeten voldoen aan NEN 7510.

In deze whitepaper geven we eerst een overzicht van de NEN 7510 standaard. Vervolgens tonen we welke rol Identity Management speelt bij het NEN 7510 compliant maken van organisaties .

Van ISO 27001 en ISO 27002 naar NEN 7510

NEN 7510 is dus gebaseerd op ISO 27001. Deze internationale standaard richt zich op informatiebeveiliging managementsystemen en beschrijft vooral hoe informatiebeveiliging procesmatig ingericht moet worden, zodat de vertrouwelijkheid, beschikbaarheid en integriteit van informatie is gegarandeerd. Het uitgangspunt is daarbij een uitgebreide risico analyse naar mogelijke dreigingen en de impact ervan. Aan de hand hiervan wordt bepaald welke maatregelen nodig zijn en welke resterende risico's nog acceptabel zijn. Informatiebeveiliging gaat dus niet om het simpelweg afvinken van een standaard lijst met maatregelen; de grootste risico's moeten daadwerkelijk de hoogste prioriteit krijgen. Ook moet er een Plan-Do-Check-Act cyclus zijn geïmplementeerd waarin voortdurend wordt gemonitord of de bestaande beveiligingsmaatregelen nog voldoen of moeten worden aangepast.

Vervolgens bevat ISO 27001 een bijlage met concrete aanbevelingen voor beheersmaatregelen. Deze 93 maatregelen (ook wel 'controls' genoemd) zijn nog verder in detail uitgewerkt in de ISO 27002 standaard. De ISO certificering van organisaties betreft altijd de ISO 27001 standaard, maar de ISO 27002 geeft dus een concretere invulling.

Op soortgelijke wijze bestaat de NEN 7510 norm ook uit twee delen, de 7510-1 en de 7510-2. Het eerste deel is vergelijkbaar met ISO 27001 en omschrijft de feitelijke norm. 7510-2 biedt net als ISO 27002 inhoudelijke aanbevelingen waarbij voor NEN 7510-2 het 'comply or explain' principe geldt; men moet de NEN 7510-2 richtlijnen volgen of toelichten waarom en hoe je een maatregel anders hebt ingevuld.

De hoofdtekst van NEN 7510-1 (en specifiek de hoofdstukken 4 t/m 10) lijkt sterk op de ISO 27001 hoofdtekst en richt zich op de bestuurlijke en procesmatige inbedding van de informatiebeveiliging; wel is de tekst aangepast en uitgebreid met zaken die specifiek gelden binnen de Nederlandse zorg. Daarnaast bevat NEN 7510-1 een bijlage met beheersmaatregelen die verder worden uitgewerkt in NEN 7510-2. Ook hier vormen de bestaande beheersmaatregelen van ISO 27001 en 27002 het uitgangspunt. Daarbij zijn 14 van de bestaande 93 ISO 27001 maatregelen uitgebreid om deze 'zorg-proof' te maken. Ook zijn er nog 8 aanvullende zorgspecifieke beheersmaatregelen toegevoegd. Voor die zorgspecifieke input is onder andere gebruik gemaakt van de ISO 27799 standaard die richtlijnen geeft voor informatiebeveiliging binnen de gezondheidszorg.

Hieronder vind je een voorbeeld van zo'n zorg-specifieke aanvulling:

A.5.15	Toegangsbeveiliging	*Beheersmaatregel* 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. *Zorgspecifieke beheersmaatregel (aanvullend)* Er moet beleid voor op rollen gebaseerde toegangsbeveiliging gelden voor de toegang tot persoonlijke gezondheidsinformatie

In bovenstaand voorbeeld – beheersmaatregel A.5.15. voor toegangsbeveiliging – vind je onder de koptekst 'Beheersmaatregel' de algemene ISO 27001 richtlijn op dit gebied. De NEN 7510 aanvulling vind je onder het rode kopje 'zorgspecifieke beheersmaatregel'. In dit specifieke voorbeeld stelt NEN 7510 dat voor de toegang tot medische gegevens een op rollen gebaseerde toegangsbeveiliging moet gelden.

Controls en overheidsmaatregelen

In eerdere versies van ISO 27001 waren de beheersmaatregelen ingedeeld in 14 verschillende categorieën. In de meest recente versie van de standaard – en dus ook in NEN 7510:2024 - is dit vereenvoudigd tot vier heldere categorieën:

- Organisatorische beheersmaatregelen: Dit zijn 43 beheersmaatregelen gericht op de organisatorische vraagstukken. Bijvoorbeeld de eis dat toegangsrechten rolgebaseerd moeten worden verstrekt en beheerd.
- Mensgerichte beheersmaatregelen: Een kleinere set beheersmaatregelen (9) met bijvoorbeeld strikte richtlijnen over de screening van medewerkers.
- Fysieke beheersmaatregelen: Hier gaat het om 14 beheersmaatregelen met richtlijnen voor bijvoorbeeld de fysieke toegangsbeveiliging tot gebouwen, ruimtes en andere faciliteiten.
- Technologische beheersmaatregelen: Dit is een set van 35 beheersmaatregelen om onder andere software, data en digitale apparaten te beveiligen.

Identity Management en NEN 7510

NEN 7510 vult dus de standaard ISO controls aan met maatregelen die een zorg organisatie moet implementeren om alle informatie – inclusief medische informatie en patiëntgegevens - goed te beveiligen. Het beheer van eindgebruikers en hun rechten worden daarbij steeds belangrijker. Zorgmedewerkers, partners en patiënten mogen alleen toegang krijgen tot applicaties en data op een 'need to know' basis. Ook is het noodzakelijk dat alle IT activiteiten zijn te traceren tot het niveau van individuele gebruikers. Het maakt Identity Management een belangrijk gereedschap bij de realisatie van een 'zorg-proof' informatiebeveiliging. In dit hoofdstuk beschrijven we hoe we met een state-of-the-art Identity Management oplossing verschillende NEN 7510 maatregelen kunnen faciliteren. Dit illustreren we aan de hand van onze eigen HelloID cloudbased Identity & Access Management (IAM) platform.

Provisioning van gebruiksaccounts en -rechten

Groepsaccounts zijn in het algemeen binnen de zorg niet toegestaan, evenals het 'copy user' principe voor nieuw binnenkomende medewerkers. Toegangsrechten moeten vandaag de dag eenduidig zijn gekoppeld aan individuele gebruikersaccounts. Er moet op ieder moment duidelijk zijn wie er toegang heeft tot specifieke (patiënt)data en applicaties en wie bepaalde handelingen uitvoert. En natuurlijk moeten de accountgegevens en toegangsrechten altijd up-to-date zijn. Dus steeds in lijn met iemands huidige rol en positie binnen de organisatie. Professioneel en geautomatiseerd gebruikersaccountmanagement is daarvoor cruciaal.

Binnen HelloID borgen we dit door middel van geautomatiseerde provisioning. Hiermee zijn iemands digitale identiteit en toegangsrechten altijd in lijn met de informatie zoals geregistreerd in het HR systeem. Dankzij een rechtstreekse koppeling tussen dat HR systeem en HelloID ontvangt de nieuwe medewerker bij onboarding direct een gebruikersaccount met daaraan gekoppeld de faciliteiten en rechten die passen bij diens rol. Ook tijdens het verdere dienstverband houden we dit automatisch actueel. Verandert iemands rol, dan past HelloID ook direct de toegangsrechten aan. En verlaat iemand de organisatie, dan zorgt HelloID dat automatisch het account wordt geblokkeerd en de vertrekkende medewerker geen toegang meer heeft. Stapeling van rechten en accounts die per ongeluk toegankelijk blijven, zijn niet langer mogelijk. Ook kunnen we specifieke accountbeheer processen inrichten voor tijdelijke krachten en flex-werkers.



Automation: standaardisatie met ruimte voor uitzonderingen

Goede informatiebeveiliging leunt op duidelijke beleidsregels, heldere processen en weinig ruimte voor individueel en ongecontroleerd maatwerk. Om dat te borgen willen we identity management processen zoveel als mogelijk standaardiseren en automatiseren. Daarbij moet het mogelijk zijn concepten als Role Based access te ondersteunen en processen te implementeren met een duidelijke scheiding van rollen. Tegelijkertijd zijn er altijd uitzonderingen en moet iedere organisatie een eigen balans zoeken tussen gebruiksvriendelijkheid en bedrijfsveiligheid. Automatisch te veel rechten verstrekken, leidt tot ongewenste beveiligingsrisico's. Maar medewerkers steeds onnodig laten wachten op hun toegangsrechten belemmert hun werk.



HelloID biedt die gewenste combinatie van standaardisatie en uitzonderingen:

- Standaard kun je binnen HelloID rechten toekennen met behulp van de zogenaamde Attribute Based Access Control (ABAC) functionaliteit. De organisatiestructuur met rollen en bijbehorende werkzaamheden vertalen we in HelloID naar configureerbare business rules die automatisch bepalen welke toegangsrechten een medewerker krijgt. Vanaf de automatisch onboarding bij indiensttreding tot en met de vertrekprocedure bij vertrek.
- Het merendeel van de rechten wordt dus volledig geautomatiseerd uitgegeven, maar zo'n standaard rollenmatrix is nooit volledig dekkend en daarom voorziet HelloID ook in uitzonderingen. Voor specifiekere en moeilijker automatisch uitdeelbare rechten kun je self-service processen ontwerpen. Gebruikers kunnen hiermee zelf online toegang vragen tot applicaties of datashares waarbij automatisch de juiste goedkeuringsstappen worden gevolgd. Na goedkeuring zorgt het geautomatiseerde proces voor de verdere activering zonder risicovolle uitzonderingen of vergissingen.

Geautomatiseerde configuratieregels zorgen dat de dienstencatalogus automatisch up-to-date blijft. Een nieuwe share wordt bijvoorbeeld direct zichtbaar in de catalogus. Op ieder moment kan het systeem een overzicht geven van welke medewerkers actief zijn en welke licenties, applicaties, shares, et cetera zij in gebruik hebben. Service Automation kan ook worden gebruikt om de gebruikersaccounts en rechten voor flexibele en tijdelijke medewerkers veilig te beheren.

Access management

Een state-of-the-art toegangsmanagement zorgt dat medewerkers - en zo nodig ook partners en cliënten - eenvoudig en uniform toegang krijgen tot applicaties en data. Zoals hiervoor toegelicht is het uitgangspunt dat iedere gebruiker één persoonlijk gebruikersaccount krijgt. Met een concept als Single Sign-On zorg je vervolgens dat mensen maar één keer hoeven in te loggen. Juist zo'n combinatie van gebruiksvriendelijke én veilige toegangsoplossingen voorkom je dat medewerkers onveilige work-arounds verzinnen.



HelloID ondersteunt alle gangbare Single Sign-On protocollen om gebruikers per applicatie te authentiseren. Voor toegang tot applicaties zonder ingebouwde SSO faciliteiten biedt HelloID andere methodes om de toegang te verzorgen. Voor de primaire authenticatie kunnen we HelloID integreren met de Active Directory en andere zogenaamde Identity Providers zoals Entra ID, Google, Salesforce, SAML en OpenID. Ook ondersteunt het platform extra beveiligingsopties die NEN 7510 voorschrijft, zoals Two Factor Authentication (2FA). HelloID herkent contextuele factoren zoals de inloglocatie en het tijdstip en kan afhankelijk daarvan de gebruiker vragen om een extra authenticatie. Naast soft of hard tokens en sms biedt HelloID ook verschillende one time passwords (OTP's) als tweede factor.

Cloud based Identity Management met hoge beschikbaarheid

Steeds meer zorginstellingen migreren hun bestaande IT dienstverlening naar de cloud en ook voor Identity en Access Management zoekt men dus een cloud-based oplossing. De beschikbaarheid, betrouwbaarheid en veiligheid is daarbij cruciaal. Als centrale schakel binnen de dienstverlening moet de 'identity management' keten altijd functioneren en mag de toegangsbeveiliging nooit worden 'kortgesloten'.

HelloID verzorgt Identity & Access Management vanuit de cloud met als voordeel lagere investeringen, een snelle installatie en configuratie terwijl Tools4ever het technische beheer verzorgt, inclusief automatische updates. De oplossing wordt gerealiseerd met behulp van maximaal beveiligde Microsoft Azure- en Google Cloudomgevingen, die bovendien iedere zes maanden grondig wordt gecontroleerd door Deloitte Risk Services. Ook is Tools4ever ISO 27001 gecertificeerd, ondersteunen we de relevante NEN 7510 maatregelen en beschikt Tools4ever over een SOC 2 Type II auditverklaring waarin onze dienstverlenende processen zijn beoordeeld met de focus op zaken als beveiliging, beschikbaarheid en vertrouwelijkheid. Compliance aan de strenge security-eisen is dan ook gewaarborgd. De dienstverlening heeft bovendien een zeer hoge beschikbaarheid dankzij de ingebouwde redundantie.

Governance

Binnen zorginstellingen is registratie en rapportage essentieel. Als organisatie moet je kunnen aantonen dat de verschillende processen conform de relevante wet- en regelgeving worden uitgevoerd. Ook moet je bij een beveiligingsincident zoals een datalek kunnen traceren welke gebruikers binnen het netwerk welke handelingen hebben uitgevoerd.

Als Identity-as-a-Service moet HelloID voldoen aan steeds strengere wet- en regelgeving op het gebied van audits en beveiliging. Alle toegangspogingen, geautomatiseerde en handmatige processen, en het gebruik van ons platform worden daarom geregistreerd en inzichtelijk gemaakt. Zo wordt het authenticatieproces automatisch gemonitord en is via rapportages altijd inzichtelijk wie welke applicaties heeft geraadpleegd, op welk moment en vanaf welke locatie. Dit geeft niet alleen een gedetailleerd beeld van het doorlopen authenticatietraject, maar toont bijvoorbeeld ook inlogpogingen vanaf verdachte IP-adressen. Mogelijke dreigingen kunnen tijdig worden herkend om tegenmaatregelen te nemen.



Extra onderscheidend is dat binnen HelloID de volledige identity lifecycle per systeem én per gebruiker auditable is. Alle uitgevoerde acties worden gelogd, zoals het creëren, inschakelen, updaten, verplaatsen, disablen en verwijderen van accounts. Hetzelfde geldt voor het toekennen en intrekken van permissies. Zijn rechten ad hoc toegekend (buiten de reguliere rollenmatrix) dan is via HelloID precies te zien wie dit heeft aangevraagd, welke persoon het verzoek heeft goedgekeurd en tot welke exacte wijzigingen in achterliggende systemen dit heeft geleid. Daarmee is het HelloID proces volledig transparant, toetsbaar en aanpasbaar. Ook biedt HelloID nu een Governance module aan. Waar een gangbare IAM-oplossing zorgt dat de organisatie 'in control kómt' zorgen we met aanvullende functionaliteit dat je ook 'in control blijft'. Met features als onder andere reconciliation, recertification en toxic rules beheer voorkomen we interne mismatches tussen het IAM platform en doelsystemen, houden we meer grip op het gebruik van onder andere self-service producten en kunnen we conflicterende business rules herkennen en automatisch oplossen.

Meer weten?

Identity Management vormt vandaag de dag een centrale rol binnen je IT beveiliging. Medewerkers, partners en cliënten mogen alleen nog met een eigen account toegang krijgen tot applicaties en data. Rechten moeten altijd worden verstrekt op een 'need to know' basis. We moeten bovendien alle IT activiteiten tot het niveau van individuele gebruikers kunnen traceren. Het maakt je Identity Management platform een belangrijk element bij het inrichten van je NEN 7510 compliant informatiebeveiligingssysteem en we adviseren je uiteraard graag hoe je daarbij HelloID optimaal kan inzetten.

Een handig startpunt daarbij is onze checklist NEN 7510 - HelloID die je als bijlage vindt bij deze whitepaper. Bij een behoorlijk deel van de NEN 7510 beheersmaatregelen speelt identity management direct of indirect een rol. Voor die beheersmaatregelen beschrijven we in de checklist kort hoe HelloID jouw organisatie kan helpen die maatregelen effectief te implementeren.

Over Tools4ever

Tools4ever is een Nederlands softwarebedrijf. We ontwikkelen innovatieve en gestandaardiseerde Identity as a Service (IDaaS)-oplossingen. De hedendaagse IDaaS-oplossingen zijn complex, daarom hebben wij onszelf toegelegd op het ontwikkelen en leveren van IDaaS-oplossingen die eenvoudig te implementeren en beheren zijn. Van 2013 tot en met 2020 hebben we maximaal geïnvesteerd om deze doelstelling te realiseren. HelloID is van scratch opgebouwd waarbij gebruikgemaakt wordt van de modernste softwaretechnieken. De eerste release van HelloID is begin 2020 met veel enthousiasme ontvangen. HelloID is een mooi product waar onze gebruikers blij van worden. We voelen ons verplicht om voor een eerlijke vergoeding, excellente service te verlenen, en te blijven investeren in verdere ontwikkeling van HelloID.



Bijlage

checklist NEN 7510:2024 – HelloID

Deze kolom toont welke HelloID functionaliteit een bijdrage levert om de organisatie als geheel compliant te maken met de NEN 7510-2024 beheersmaatregelen. Het gaat hier dus niet om de vraag of het HelloID platform voldoet aan specifieke beheersmaatregelen in NEN 7510. Voorbeeld: het rol-based toegangsbeheer van HelloID maakt dat alle systemen beter beveiligd zijn. Het feit dat HelloID back-ups maakt betekent enkel dat HelloID zelf aan de eisen voldoet.

HelloID bijdrage aan NEN 7510-2024 compliancy

A.5	**Informatiebeveiligingsbeleid**	
A.5.1.	Beleidsregels voor informatiebeveiliging	Beleidsregels met betrekking tot de verstrekking van accounts en toegangsrechten op basis van gebruikersattributen (zoals functie, afdeling etc.) worden binnen HelloID eenduidig beheerd als business rules. HelloID vormt voor deze regels als een Single Point of Truth
A.5.3	Functiescheiding	Uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control is een hulpmiddel bij de implementatie van rolscheiding. Daarnaast kan men voor de verschillende self-service processen goedkeuringsprocedures configureren met een duidelijke scheiding van taken.
A.5.4		HelloID helpt specifiek het Principle of Least Privilege af te dwingen binnen de organisatie. Men krijgt alleen toegang tot applicaties en rechten die voor de eigen taken nodig zijn
A.5.7	Informatie en analyses over dreigingen	HelloID genereert logs/informatie over de volgende zaken: 1) Access Management inlogpogingen etc.; 2) Provisioning business rules waarmee medewerkers aan rechten worden gekoppeld; 3) Service Automation logs van toegangsverzoeken en de afhandeling en status hiervan 4) Governance functionaliteit geeft inzicht in o.a. inconcistenties, suboptimalisaties etc.
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	HelloID onderhoudt automatisch een registratie van applicaties en shares waar medewerkers toegang toe kunnen krijgen
A.5.10	Aanvaardbaar gebruik van informatie andere gerelateerde bedrijfsmiddelen	Door de attribuut/rol gebaseerde toegang hebben medewerkers automatisch alleen toegang tot applicaties en data die men in het kader van iemands rol nodig heeft.
A.5.11	Retourneren van bedrijfsmiddelen	HelloID zorgt dat toegangsrechten en accounts worden gedeactiveerd en verwijderd als medewerkers deze niet langer nodig hebben. Ook kan i.s.m. IT Service Management systemen tijdig notificaties worden verstuurd voor intrekken bedrijfsmiddelen
A.5.12	Classificeren van informatie	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast biedt HelloID service managementprocessen tbv de verstrekking van individuele toegangsrechten. Toegangsrechten kunnen ook beperkingen bevatten over specifieke dataklassen binnen een applicatie.

A.5.14	Overdragen van informatie	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast biedt HelloID service managementprocessen tbv de verstrekking van individuele toegangsrechten. Toegangsrechten kunnen ook beperkingen bevatten mbt de overdracht van informatie
A.5.15	Toegangsbeveiliging	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast biedt HelloID service managementprocessen tbv de verstrekking van individuele toegangsrechten.
A.5.16	Identiteitsbeheer	HelloID service provisioning functionaliteit zorgt dat gedurende de volledige lifecycle medewerkers op ieder moment de relevante accounts en rechten hebben
A.5.17	Authenticatie-informatie	Authenticatieinformatie wordt versleuteld opgeslagen in een Identiteitsprovider (IdP). HelloID kan zelf fungeren als IdP, maar gebruikelijker is dat HelloID gebruik maakt van bestaande IdP's zoals de lokale Active Directory of EntraID.
A.5.18	Toegangsrechten	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast biedt HelloID service managementprocessen tbv de verstrekking van individuele toegangsrechten. Daarbij is de goedkeuring door relevante functionarissen geborgd via configureerbare workflows
A.5.24	Plannen en voorbereiden van het	HelloID genereert logs/informatie over de volgende zaken: 1) Access Management inlogpogingen etc.; 2) Provisioning business rules waarmee medewerkers aan rechten worden gekoppeld; 3) Service Automation logs van toegangsverzoeken en de afhandeling en status hiervan 4) Governance functionaliteit geeft inzicht in o.a. inconcistenties, suboptimalisaties etc.
A.5.28	Verzamelen van bewijsmateriaal	HelloID genereert logs/informatie over de volgende zaken: 1) Access Management inlogpogingen etc.; 2) Provisioning business rules waarmee medewerkers aan rechten worden gekoppeld; 3) Service Automation logs van toegangsverzoeken en de afhandeling en status hiervan 4) Governance functionaliteit geeft inzicht in o.a. inconcistenties, suboptimalisaties etc.
A.5.34	Privacy en bescherming van	Deze bescherming komt in essentie erop neer dat het Principle of Least Privilege wordt ondersteund. HelloID borgt dit principe
A.5.35	Onafhankelijke beoordeling van	De HelloID werkt met transparante business rules en beschikt daarnaast over overzichten van de individueel verstrekte toegangsrechten (en wie deze heeft goedgekeurd).
A.5.36	informatiebeveiliging	De HelloID werkt met transparante business rules en beschikt daarnaast over overzichten van de individueel verstrekte toegangsrechten (en wie deze heeft goedgekeurd).
A.5.43	Naleving van beleid, regels en	HelloID genereert logs/informatie over de volgende zaken: 1) Access Management inlogpogingen etc.; 2) Provisioning business rules waarmee medewerkers aan rechten worden gekoppeld; 3) Service Automation logs van toegangsverzoeken en de afhandeling en status hiervan 4) Governance functionaliteit geeft inzicht in o.a. inconcistenties, suboptimalisaties etc.

A.6	**Mensgerichte beheersmaatregelen**	
A.6.1	Screening	Screening van kandidaten valt buiten de scope van HelloID. Wel kunnen specifieke criteria (bijv. certificaten) worden geregistreerd in het personeelsdossier in het HR systeem. Omdat HelloID provisioning gekoppeld kan worden aan het HR systeem, is het mogelijk bij de uitgifte van rechten aan medewerkers hiermee rekening te houden.
A.6.2	Arbeidsovereenkomst	De contractuele afspraken m.b.t. informatiebeveiliging kunnen vastgelegd zijn in het persneelsdossier. Dankzij de koppeling van HelloID en het HR systeem kan automatisch worden geborgd dat een nieuwe medewerker sommige rechten pas krijgt als de medewerker specifieke beveiligingsafspraken heeft bevestigd.
A.6.4	Disciplinaire procedure	Als de uitkomst van disciplinaire procedures leiden tot intrekken van bevoegdheden in iemands HR dossier, kan dit via de koppeling van het HR systeem en HelloID automatisch leiden tot ingeperkte toegangsrechten.
A.6.5	Verantwoordelijkheden na	Bij het einde van het arbeidsverband, worden verplichtingen voor de ex-medewerker (zoals geheimhouding etc.) ondersteund omdat ook automatisch toegangsrechten automatisch worden beëindigd.
A.6.7	beëindiging of wijziging van het	HelloID Access Management ondersteunt contextuele factoren waaronder toegang vanaf externe netwerkomgevingen. Afhankelijk van de context kunnen bepaalde mogelijheden worden geblokkeerd of alleen toegankelijk na een extra authenticatie. Naast soft of hard tokens en sms biedt HelloID ook verschillende one time passwords (OTP's) als tweede factor.
A.7	**Fysieke beheersmaatregelen**	
A.7.2	Fysieke toegangsbeveiliging	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Door de koppeling van HelloID aan beheersystemen van toegangspasjes kan ook het fysieke toegangsbeheer in lijn worden gebracht met de functie/ afdeling/locatie van medewerkers.
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Door de koppeling van HelloID aan beheersystemen van toegangspasjes kan ook het fysieke toegangsbeheer in lijn worden gebracht met de functie/ afdeling/locatie van medewerkers.
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	HelloID kan borgen (via Attribute Based Access Control) dat bij einde van iemands dienstverband of bij een nieuwe functie/ afdeling etc. accounts en toegangsrechten in doelsystemen worden gedeactiveerd en verwijderd.
A.8	**Beheer van bedrijfsmiddelen**	
8.1	User endpoint devices'	HelloID beheert accounts en toegangsrechten, ongeacht de gebruikte toegangsapparaten (laptops, smartphones etc.).

8.2	Speciale toegangsrechten	Voor het toewijzen van speciale rechten (dus bovenop algemene, attribute based rechten), kunnen individuele rechten worden toegekend. De processen hiervoor kunnen klantspecifiek worden geconfigureerd, inclusief goedkeuringsprocedures (door een of meerdere functionarissen)
8.3	Beperking toegang tot informatie	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast biedt HelloID service managementprocessen tbv de verstrekking van individuele toegangsrechten.
8.4	Toegangsbeveiliging op broncode	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast biedt HelloID service managementprocessen tbv de verstrekking van individuele toegangsrechten. Hiermee kunnen we ook de toegang tot ontwikkeltools beheren.
8.5	Beveiligde authenticatie	HelloID access management ondersteunt onder andere Multi-Factor Authenticatie en One-Time Password (OTP)
8.12	Voorkomen van gegevenslekken (data leakage prevention)	HelloID ondersteunt de uitgifte van accounts en toegangsrechten op basis van Attribute Based Access Control. Daarnaast biedt HelloID service managementprocessen tbv de verstrekking van individuele toegangsrechten. Hiermee borgen we het Principle of Least Privilege, een belangrijke preventieve maatregel tegen datalekken.
8.15	Logging	HelloID genereert logs/informatie over de volgende zaken: 1) Access Management inlogpogingen etc.; 2) Provisioning business rules waarmee medewerkers aan rechten worden gekoppeld; 3) Service Automation logs van toegangsverzoeken en de afhandeling en status hiervan 4) Governance functionaliteit geeft inzicht in o.a. inconcistenties, suboptimalisaties etc.

TOOLS4EVER

Adres	Amalialaan 126c 3743 KJ Baarn Nederland
Telefoon	+31 (0) 35 54 832 55
Website	Tools4ever.nl
Mail	info@tools4ever.com
Sales	sales@tools4ever.com
Support	tools4ever.nl/support