HelloID bijdrage aan ISO 27001 en BIO compliancy

Dit document beschrijft hoe het HelloID Identity Management platform bijdraagt aan het ISO 27001 en BIO compliant maken van klantorganisaties. Het gaat hier dus niet om de vraag of het HelloID platform voldoet aan specifieke richtlijnen in beide richtlijnen. Dit document focust op hoe HelloID organisaties ondersteunt bij het realiseren van de beveiligingsdoelstellingen en de bijbehorend maatregelen. Voorbeeld: het role-based toegangsbeheer van HelloID vormt een centraal element in de toegangsbeveiliging van alle IT systemen binnen een klantorganisatie. Het feit dat HelloID back-ups maakt betekent enkel dat HelloID zelf aan de eisen voldoet. Tools4ever is als ontwikkelaar van IDaaS-oplossing HelloID volledig ISO 27001-gecertificeerd.

A.5 Informatiebeveiligingsbeleid

A.5.1 Aansturing door de directie van de informatiebeveiliging

A.5.1.1	Beleidsregels voor informatiebeveiliging	Veel beleidsregels omvatten vaak duidelijke richtlijnen over de verschillende rollen en de daarbij beheerde rechten. Daarom spelen ook binnen HelloID Business Rules een belangrijke rol.
A.5.1.2	Beoordeling van het informatiebeveiligingsbeleid	HelloID werkt met business rules die eenvoudig geconfigureerd en aangepast kunnen worden. Daarnaast worden alle activiteiten geregistreerd en traceerbaar tot gebruikers. Hiermee helpt HelloID beleidsregels te beoordelen en zonodig aan te passen.

A.6 Organiseren van informatiebeveiliging

A.6.1 Interne organisatie

A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	De binnen informatiebeveiliging gedefinieerde rollen en verantwoordelijkheden kunnen binnen HelloID worden geborgd via verschillende beheerrollen die daarin worden ondersteund.
A.6.1.2	Scheiding van taken	Met HelloID kan men voor de verschillende (self)service processen goedkeuringsprocedures configureren, conform het eigen veiligheidsbeleid en met een duidelijke scheiding van taken. Bovendien worden bij alle wijzigingen binnen HelloID vastgelegd wie deze heeft aangevraagd, welke persoon het verzoek heeft goedgekeurd en tot welke exacte wijzigingen in achterliggende systemen dit heeft geleid.

A.6.2 Mobiele apparatuur en telewerken

A.6.2.1	Beleid voor mobiele apparatuur	HelloID herkent contextuele factoren waaronder het gebruik van een mobiel device. Afhankelijk van de context kunnen bepaalde mogelijkheden 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. Specifieke afspraken over het gebruik van mobiele apparatuur kunnen ook nog apart digitaal worden herbevestigd en 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 accounts of rechten aan medewerkers hiermee rekening te houden.
A.6.2.2	Telewerken	HelloID herkent 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 Veilig personeel

A.7.1 Voorafgaand aan het dienstverband

A.7.1.1	Screening	Screening van kandidaten valt buiten de scope van HelloID. Wel kunnen specifieke criteria (bijv. de aanwezigheid van een Verklaring omtrent Gedrag) 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 accounts of rechten aan medewerkers hiermee rekening te houden.
A.7.1.2	Arbeidsvoorwaarden	Contractuele afspraken in arbeidsvoorwaarden vallen buiten de scope van HelloID. Wel kunnen specifieke afspraken ook nog apart digitaal worden herbevestigd en 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 accounts of rechten aan medewerkers hiermee rekening te houden.

A.7.2 Tijdens het dienstverband

A.7.2.1	Directieverantwoordelijkheden	Dankzij het gestructureerde identity management binnen HelloID met duidelijke rollen en bijbehorende rechten, wordt het toepassen van de beleidsregels en procedures afgedwongen.
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Dankzij het gestructureerde identity management binnen HelloID met duidelijke rollen en bijbehorende rechten, werken gebruikers automatisch en intuïtief veilig volgens de regels. Hiermee kan trainingsbehoefte worden beperkt. Uiteraard kunnen trainingsafspraken en -resultaten ook nog apart digitaal worden herbevestigd en 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 accounts of rechten aan medewerkers hiermee rekening te houden.
A.7.2.3	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.7.3 Beëindiging en wijziging van dienstverband

A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Wijziging van een dienstverband resulteert vaak in een andere rol met andere verplichtingen en rechten. Deze wijzigingen worden in het HR systeem verwerkt en leiden dankzij de koppeling met HelloID automatisch tot wijzigingen van rollen en toegangsrechten voor de betreffende gebruiker. Bij het einde van het arbeidsverband worden verplichtingen voor de ex-medewerker (zoals geheimhouding) gestimuleerd omdat ook automatisch toegangsrechten worden beëindigd.

A.8 Beheer van bedrijfsmiddelen

A.8.1 Verantwoordelijkheden voor bedrijfsmiddelen

A.8.1.1	Inventariseren van bedrijfsmiddelen	HelloID onderhoudt automatisch een registratie van digitale bedrijfsmiddelen (zoals applicaties en shares) waar medewerkers toegang toe hebben. Daarnaast helpt HelloID de processen te automatiseren voor de uitgifte van fysieke devices als laptops en mobiele telefoons.
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Via de autorisatiematrix wordt per gebruiker diens rol gedocumenteerd en geïmplementeerd, met de bijpassende toegangsrechten voor applicaties en data. Uiteraard kunnen de afspraken met betrekking tot het gebruik van bedrijfsmiddelen ook nog apart digitaal worden herbevestigd en 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 accounts of rechten aan medewerkers hiermee rekening te houden.

A.8.2 Informatieclassificatie

A.8.2.3	Behandelen van bedrijfsmiddelen	In het geval van optioneel aanvraagbare bedrijfsmiddelen met verschillende classificatieniveaus (Beschikbaarheid, Integriteit, Vertrouwelijkheid) kunnen verschillende vormen van authenticatie (MFA) en bijpassende workflows worden ingezet.

A.9 Toegangsbeveiliging

A.9.1 Bedrijfseisen voor toegangsbeveiliging

A.9.1.2	Toegang tot netwerken en netwerkdiensten	Via provisioning krijgt elke medewerker een eigen persoonlijk account. Via een autorisatiematrix is het mogelijk om op basis van iemands rol exact vast te leggen welke netwerkdiensten de gebruiker in het kader van zijn werkzaamheden mag gebruiken. Bij het bepalen van de toegangsrechten kan HelloID ook rekening houden met contextuele factoren, zoals het gebruik van een mobiel device en of dit een geauthentiseerd of on-geauthentiseerd apparaat (Bring Your Own Device) betreft.

A.9.2 Beheer van toegangsrechten van gebruikers

A.9.2.1	Registratie en uitschrijving van gebruikers	Dankzij de provisioning functionaliteit kan het verstrekken van gebruikersaccounts worden gesynchroniseerd met de registratie van bijvoorbeeld medewerkers binnen het HR systeem. Daarnaast kunnen er aparte registratieprocedures worden toegevoegd (bijvoorbeeld voor gastaccounts). HelloID voorkomt het gebruik van groepsaccounts en draagt bij aan een sluitende formele administratie van gebruikersidentificaties.

A.9.2.2	Gebruikers toegang verlenen	Door binnen de organisatie te werken met vastgestelde rollen en mandaten en daar met HelloID op aan te sluiten, kunnen we medewerkers op ieder moment de rechten geven die specifiek horen bij de betreffende rol(len) van een medewerker. A.9.2.3 beschrijft hoe we met uitzonderingssituaties omgaan, waaronder speciale rechten.
A.9.2.3	Beheren van speciale toegangsrechten	Voor het toewijzen van speciale rechten (dus bovenop algemene rolbased rechten, waaronder meer privileged rechten), kunnen individuele rechten worden toegekend. De processen hiervoor kunnen klantspecifiek worden geconfigureerd, inclusief goedkeuringsprocedures (door een of meerdere functionarissen) en een regelmatige beoordeling hiervan.
A.9.2.4	Beheer van geheime authenticatieinformatie van gebruikers	HelloID verzorgt bij de instroom een geautomatiseerde en veilige procedure voor de initiële uitgifte van geheime authenticatie-informatie (organisatieafhankelijk naar het privé email adres of juist de manager). Authenticatieinformatie wordt dan verder 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 Azure AD. Verder gebruik van authenticatie-informatie voor andere gebruikte applicaties kan worden beperkt met single sign-on. Daarbij wordt gebruik gemaakt van tokens tussen de IdP en service provider.
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	HelloID biedt hiervoor heldere overzichten van gebruikers en de toegekende rechten. Deze kunnen automatisch periodiek naar managers en/of resource owners worden verstuurd ter controle.
A.9.2.6	Toegangsrechten intrekken of aanpassen	Door de geautomatiseerde provisioning en het rol based access management worden rechten automatisch ingetrokken of aangepast als iemands rol en bijbehorende rechten wijzigen. Ook worden rechten automatisch ingetrokken bij de beëindiging van het dienstverband.
A.9.3	**Gebruikersverantwoordelijkheden**	
A.9.3.1	Geheime authenticatie-informatie gebruiken	HelloID draagt hieraan bij door automatisch het correcte gedrag van authenticatie informatie af te dwingen en onveilige workarounds te voorkomen. Bovendien kunnen afhankelijk van de gebruikerscontext (netwerk, device etc.) gevraagd worden om een extra (multifactor) authenticatie. Organisaties kunnen zelf deze eisen configureren.
A.9.4	**Toegangsbeveiliging van systeem en toepassing**	
A.9.4.1	Beperking toegang tot informatie	De geautomatiseerde uitgifte en beheer van accounts en bijbehorende rechten (rol based) binnen HelloID borgen het 'least-privilege' principe. Daarbij heeft iemand altijd alleen toegang tot functionaliteit en data die noodzakelijk is voor de uitvoering van diens rol.

A.9.4.2	Beveiligde inlogprocedures	HelloID borgt dat mensen altijd gebruik moeten maken van de vereiste inlogprocedures, zo nodig aangevuld met een tweede factor verificatie. Daarnaast kunnen er aparte registratieprocedures worden toegevoegd voor speciale gebruikersgroepen zoals gasten of leveranciers.
A.9.4.3	Systeem voor wachtwoordbeheer	Dit is veelal onderdeel van de toegepaste Identity Provider (IdP). In het geval HelloID als IdP wordt ingezet, kunnen de beheerprocessen zodanig worden ingeregeld dat men voldoet aan het binnen de organisatie vastgestelde wachtwoordbeleid (met richtlijnen over bijvoorbeeld de wachtwoordlengte en complexiteit, geldigheidsduur ban het wachtwoord etc.).

A.11 Fysieke beveiliging en beveiliging van de omgeving

A.11.1 Beveiligde gebieden

A.11.1.2	Fysieke toegangsbeveiliging	Als onderdeel van de provisioning van gebruikersaccounts, rollen en toegangsrechten, kan HelloID ook worden gekoppeld aan fysieke toegangsbeveiligingssystemen waarin is vastgelegd tot welke fysieke beveiligingszones gebruikers toegang hebben.

A.12 Beveiliging bedrijfsvoering

A.12.1 Bedieningsprocedures en verantwoordelijkheden

A.12.1.2	Wijzigingsbeheer	Rol en rechtenwijzigingen worden automatisch doorgevoerd volgens een vastgesteld proces. Daarbij monitoren we proactief op (onverwacht) hoge aantallen wijzigingen. In dat geval wordt een beoordeling en akkoord van een beheerder gevraagd (de tresholds zijn instelbaar). Hiermee wordt voorkomen dat bijvoorbeeld een organisatiewijziging grote security risico's oplevert.

A.12.4 Verslaglegging en monitoren

A.12.4.1	Gebeurtenissen registreren	Logging en rapportages zijn basiscomponenten van elk beveiligingsbeleid. Omdat Identity Management in veel processen een rol speelt, is het cruciaal dat alle IdM activiteiten worden gelogd. HelloID verzorgt dit en geeft in de vorm van een 'audit trail' inzicht in het gebruik van de HelloID-omgeving. Alle binnen en door HelloID uitgevoerde acties worden opgeslagen in Elastic reporting functionaliteit met uitgebreide rapportage mogelijkheden. De opgeslagen informatie is toereikend om incidenten te herleiden tot individuele gebruikers, het gebruikte apparaat, het datum en tijdstip en het resultaat van de handeling. Dit omvat onder andere: Provisioning: per systeem en gebruiker alle acties omtrent het creëren, enablen, updaten, verplaatsen, disablen, het verwijderen van accounts, en het toekennen en intrekken van permissies. Service Automation met alle (self) service acties omtrent aanvragen, workflows, goedkeuringen, formulierdata en configuratiewijzigingen. Access Management met alle succesvolle en mislukte aanmeldingen, de geografische locatie van de gebruiker, gebruikte apparaten, geïnitieerde wachtwoord resets,

		toegangspogingen voor applicaties en mislukte toegangspogingen als gevolg van het toegangsbeleid. Uiteraard kan HelloID de rapportages en logs ook delen met SIEM en/of SOC faciliteiten van de klant.

A.16 Beheer van informatiebeveiligingsincidenten

A.16.1 Beheer van informatiebeveiligingsincidenten en - verbeteringen

A.16.1.7	Verzamelen van bewijsmateraal	Alle toegangspogingen worden geregistreerd binnen het HelloID Identity Management platform. Ook bevat het platform op ieder moment een overzicht van toegangsrechten per gebruiker. Naast de rol gebaseerde rechten kan het systeem alle uitzonderingen (wie vroeg specifieke toegangsrechten aan en wie gaf goedkeuring) traceren. Alle geregistreerde gegevens kunnen worden opgeslagen en/of gedeeld met andere klantsystemen, conform het beveiligingsbeleid van de klant.

A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

A.17.1 Informatiebeveiligingscontinuïteit

A.17.1.2	Informatiebeveiligingscontinuïteit implementeren	Met HelloID worden alle afgesproken processen en procedures omtrent toegang en autorisatie (semi)-geautomatiseerd afgedwongen.

A.18 Naleving

A.18.1 Naleving van wettelijke en contractuele eisen

A.18.1.3	Beschermen van registraties	M.b.t. de registraties zorgt HelloID met een centraal en geautomatiseerde Identity Management dat alles registraties binnen dat domein gegarendeerd worden uitgevoerd.
A.18.1.4	Privacy en bescherming van persoonsgegevens	Door een rol-based Identity Management kan de organisatie aantonen dat medewerkers alleen op een 'need-to-know' toegang krijgen op persoonsgegevens. Ook worden alle toegangsverzoeken gelogd ten behoeve van onderzoeken bij incidenten