TOOLS4EVER

Whitepaper V1.0 / 20 02 2024

Normenkader IBP FO en de rol van Identity Management

Inhoudsopgave

Inleiding 1
Hoe is het normenkader samengesteld? 2
Hoe word ik compliant? 3
Identity Management en het normenkader 5
Gestructureerd account en rechtenbeheer 5
Gestroomlijnde beheerprocessen 6
Access management 7
Auditeerbaarheid van het IAM 7
Betrouwbaar Identity Management met hoge beschikbaarheid ... 8
Meer weten? 8

Inleiding

Het basis en voortgezet onderwijs maakt steeds meer gebruik van digitale toepassingen. Zowel voor het onderwijs zelf, de onderlinge samenwerking en uiteraard de administratie. Dat betekent dat steeds meer persoonlijke gegevens van minderjarige leerlingen worden verzameld, opgeslagen en verwerkt. Een kwetsbare groep en daarom moeten we binnen dit zogeheten Funderend Onderwijs die leerling gegevens extra zorgvuldig verwerken en beveiligen. Ook de leerkrachten en ondersteunende medewerkers moeten volledig veilig en met voldoende privacy hun werk kunnen doen.

Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs

Het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hebben hiervoor de krachten gebundeld in het programma Digitaal Veilig Onderwijs. Doel is een onderwijssector waarin iedere leerling veilig digitaal kan leren en waar medewerkers digitaal veilig kunnen werken. Als onderdeel hiervan heeft men in 2023 het Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs (IBP FO) vastgesteld. Deze set normen helpt schoolbestuurders, schoolleiders en de betrokken professionals bij het versterken van hun informatiebeveiliging en privacy:

- **Informatiebeveiliging** omvat alles dat nodig is om de vertrouwelijkheid, integriteit en beschikbaarheid van alle informatie binnen een onderwijsinstelling te garanderen. Dat kan om persoonlijke gegevens gaan, maar ook om andere belangrijke gegevens zoals financiële informatie.
- **Privacy** richt zich specifiek op persoonlijke gegevens maar omvat meer dan alleen de beveiliging ervan. Het gaat bijvoorbeeld ook om wie die gegevens mag inzien en waarvoor ze gebruikt mogen worden. En of medewerkers, leerlingen of ouders hierover zijn geïnformeerd en toestemming is gevraagd.

Over deze whitepaper

In deze whitepaper gaan we in op de rol van Identity en Access Management (IAM) bij het implementeren van dit nieuwe normenkader binnen scholen. De eerste gepubliceerde versie in april 2023 omvat alleen de normen op het gebied van informatiebeveiliging; de privacy normen zijn nog in ontwikkeling. Dat is geen probleem voor de whitepaper. IAM is weliswaar relevant voor de privacybescherming maar doet dat met name door de informatiebeveiliging te verbeteren.

De whitepaper schetst eerst kort hoe het normenkader IBP FO is ontwikkeld. Vervolgens beschrijven we globaal de structuur en inhoud ervan. Aan de hand hiervan zoomen we in op Identity en Access Management en tonen we hoe IAM een rol speelt bij het compliant worden en blijven met het normenkader.

Hoe is het normenkader samengesteld?

Branche specifieke beveiligingsnormen zijn vaak gebaseerd op algemene normen die men vervolgens verfijnt voor de betreffende branche. Zo zijn de BIO (Baseline Informatiebeveiliging Overheid) en de NEN 751x (informatiebeveiliging voor de zorg) allebei een verfijning van de internationale ISO 27001 standaard. En de DNB (De Nederlandse Bank) hanteert best practices voor de financiële sector die naast ISO 27001 ook richtlijnen gebruiken uit onder andere Cobit en het NIST Cybersecurity Framework.

NBA Volwassenheidsmodel als uitgangspunt

Voor het normenkader Funderend Onderwijs is een iets andere aanpak gekozen. Net als het hoger onderwijs en middelbaar beroepsonderwijs gebruikt men het NBA Volwassenheidsmodel voor informatiebeveiliging. De NBA (Nederlandse Beroepsorganisatie van Accountants) ontwikkelde voor accountants en auditors een checklist om de informatiebeveiligingsmaatregelen van organisaties te beoordelen en onderling te vergelijken. Omdat verschillende organisaties verschillende standaarden kunnen gebruiken, zocht men een generieke checklist. Men heeft daarvoor 69 normen gedefinieerd – geclusterd in 15 domeinen - die allemaal zijn te herleiden tot onderwerpen in ISO 27001, BIO, DNB, NIST en Cobit. Een voorbeeld van zo'n NBA norm is:

> *There is a succession planning and staff backup for key/critical individuals and/or departments*

Voor ieder van die 69 NBA normen geeft de checklist vervolgens ook criteria om te beoordelen op wel volwassenheidsniveau deze norm in een organisatie is geïmplementeerd. Men hanteert daarvoor 5 niveaus, van 'Initial' (niets of nog in de kinderschoenen) tot 'Continuous Improvement' (best of class).

Van NBA model naar het normenkader IBP FO

Het normenkader heeft dit NBA model rechtstreeks overgenomen. Per norm is daarbij een minimaal gewenst volwassenheidsniveau vastgesteld, vaak op niveau 3 ('Defined'). Per norm zijn ook voorbeeldmaatregelen toegevoegd. Als een school die maatregelen invoert, voldoet men automatisch aan de norm.

Het originele NBA model is wat formeel beschreven en Engelstalig. Voor het normenkader IBP FO zijn de normen en het gewenste minimumniveau zoveel mogelijk letterlijk vertaald naar het Nederlands. Deze Nederlandse vertaling maakt de normenset toegankelijker binnen het onderwijs. Nadeel van de letterlijke vertaling is dat alles nog steeds wat formeel is opgeschreven, maar zo zijn de normen wel consistent met het NBA model en goed te onderhouden.

Hoe word ik compliant?

Het normenkader bevat 69 normen, geclusterd in 15 domeinen. Per domein wordt kort samengevat welke onderwerpen in dit domein worden behandeld. Ook is omschreven wie binnen de organisatie verantwoordelijk is voor dit domein en er zijn ondersteunende handreikingen, templates of andere hulpmiddelen beschikbaar (of gepland).

Normen

Iedere norm is in detail uitgewerkt, te beginnen met een definitie en een korte toelichting. Ook is het toetsingskader omschreven. Dat beschrijft het gewenste minimumniveau om aan de norm te voldoen. Een hoger niveau mag uiteraard en hangt vooral af van de risicobeoordeling in je eigen organisatie. Je vindt bij iedere norm ook concrete voorbeeldmaatregelen. Die zijn niet verplicht maar in het algemeen geldt dat als je de voorbeeldmaatregelen implementeert je automatisch voldoet aan het toetsingskader. Hieronder vind je de inhoud van een van de 69 normen.

Uit de eerste ervaringen van scholen blijkt dat sommige voorgestelde maatregelen nog wat pragmatischer mogen. Ook zijn nog niet alle hulpmiddelen beschikbaar. Er volgen dus ongetwijfeld nog aanpassingen en aanvullingen. Op dit moment is het normenkader ook nog niet verplicht, maar de verwachting is dat scholen vanaf 2027 compliant moeten zijn.

Prioriteit en groeipad

Achter in het normenkader vind je ook een tabel met prioriteiten. Het is namelijk niet realistisch om alle normen vanaf dag één te willen implementeren. Je kunt beginnen met 15 van de 69 normen om ‘de basis op orde’ te krijgen. Die hebben ook nog betrekking op een beperkt aantal domeinen. Vervolgens vind je in het normenkader een overzicht welke normen je kunt implementeren om achtereenvolgens de hoge beveiligingsrisico’s (24 normen) en medium beveiligingsrisico’s (19 normen) af te dekken. Met de resterende 11 normen kun je je informatiebeveiliging verder gaan optimaliseren en professionaliseren. De tabel is overigens alleen een suggestie. Je eigen roadmap hangt uiteraard af van jouw eigen risico analyse en prioriteiten.

Domeinen van het normenkader IBP FO. De blauw gemarkeerde domeinen bevatten normen die nodig zijn om de basis op orde te krijgen

Identity Management en het normenkader

Voor een goede informatiebeveiliging is het beheer van gebruikersaccounts en hun toegangsrechten erg belangrijk. Niet voor niets is er een separaat domein (nummer 10) met normen rondom Identity en Access Management. Dat bevat een aantal IAM-specifieke normen en zoomt daarbij ook in op specialistische onderwerpen als super-user beheer en procedures voor noodtoegang.

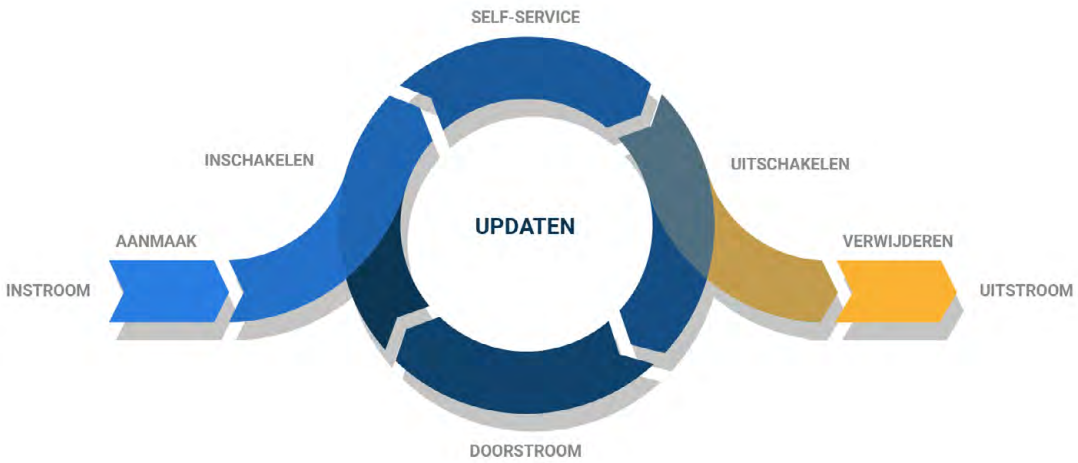
Let daarbij wel op. Dat specifieke domein is niet voldoende als je een compleet beeld wil van de benodigde IAM functionaliteit voor een onderwijsinstelling. In de lijst met normen die nodig zijn om de basis op orde te krijgen vind je bijvoorbeeld eis 9.3 (beveiligingseisen voor datamanagement). Om die eis in te vullen is een goed functionerend IAM platform al een belangrijk hulpmiddel. Ook andere domeinen bevatten normen waarvoor je een modern identity en access management nodig hebt. Check dus het hele normenkader als je de impact op je IAM omgeving in kaart wilt brengen.

In de hoofdstukken hierna illustreren we een aantal aandachtspunten voor het opzetten van een toekomstgericht IAM dat compliant is met het normenkader. We schetsen steeds eerst een samenvatting van de eisen in het normenkader. Vervolgens illustreren we aan de hand van onze eigen HelloID IAM oplossing hoe dit in de praktijk kan worden ingevuld.

Gestructureerd account en rechtenbeheer

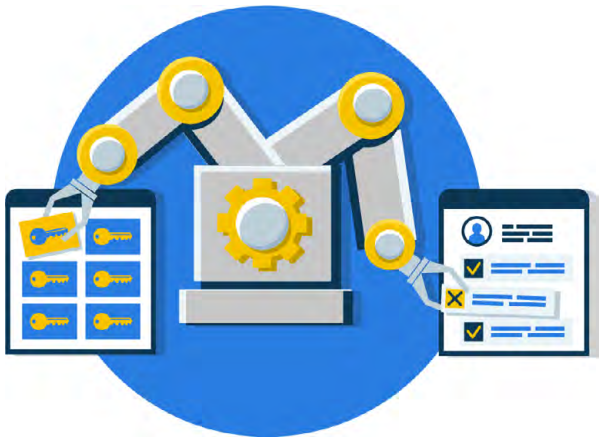
Toegangsrechten moeten worden toegekend op basis van transparante regels die het management bijvoorbeeld in de vorm van een autorisatiematrix vaststelt. Iemand mag alleen toegang krijgen tot applicaties en data die hij of zij nodig heeft om diens rol(len) in te vullen. Je mag dus alleen toegang krijgen op een need-to-know basis. Ook het rechtenbeheer voor IT administrators en andere super-users moeten onderdeel zijn van zo'n gestructureerde beheer aanpak. Het betreft bovendien niet alleen de logische toegangsrechten. Ook de fysieke toegang tot gebouwen, IT-kritische omgevingen of datacenters moet beperkt blijven tot geautoriseerd personeel.

Belangrijk daarbij is dat functiescheiding is geborgd, zodat opdracht gevende, uitvoerende en controlerende taken nooit door een en dezelfde persoon kunnen worden uitgevoerd. En tenslotte moeten de uitgegeven toegangsrechten voortdurend up-to-date zijn. Krijgt een medewerker een nieuwe functie? Dan moet het toegangsbeheer deze wijziging automatisch ook vertalen naar aangepaste toegangsrechten. En bij beëindiging van een dienstverband moeten accounts en toegangsrechten tijdig worden geblokkeerd.



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 bronsystemen zoals het HR-systeem en het Leerling Administratie Systeem (LAS). Dankzij een rechtstreekse koppeling tussen deze bronsystemen en HelloID ontvangt de nieuwe gebruiker bij instroom direct een gebruikersaccount met daaraan gekoppeld de faciliteiten en rechten die passen bij diens rol(len). Ook tijdens het verdere dienstverband of schoolcarrière houden we dit steeds actueel. Verandert iemands rol – of gaat een leerling naar een andere klas of onderwijsniveau - dan past HelloID direct de toegangsrechten aan. En verlaat iemand de organisatie, dan zorgt HelloID dat automatisch het account wordt geblokkeerd en de vertrekkende gebruiker geen toegang meer heeft. Stapeling van rechten en datalekken via accounts die per ongeluk toegankelijk blijven zijn niet langer mogelijk. Ook toegangspasjes en de daaraan gekoppelde fysieke toegangsrechten kunnen vanuit HelloID automatisch worden beheerd.

Gestroomlijnde beheerprocessen



Account en rechtenbeheer leunt dus op duidelijke beleidsregels, heldere processen en het minimaliseren van individueel en ongecontroleerd maatwerk. Zoals beschreven moeten de identity management processen zoveel mogelijk worden geautomatiseerd en gebaseerd zijn op iemands rol(len) in de organisatie. Tegelijkertijd zijn er altijd uitzonderingen mogelijk. Een leerkracht kan een specifieke applicatie nodig hebben voor zijn of haar lessen, zieke medewerkers moeten tijdelijk worden vervangen door flexkrachten of er is een projectleider nodig voor een bijzonder project. En dan zijn er ook nog noodprocedures om bijvoorbeeld toegang te krijgen tot superuser accounts bij calamiteiten. Alle processen moeten hiervoor zijn voorbereid zodat ze correct en veilig worden afgehandeld, met alle noodzakelijke controlestappen en op een manier dat alles traceerbaar is.

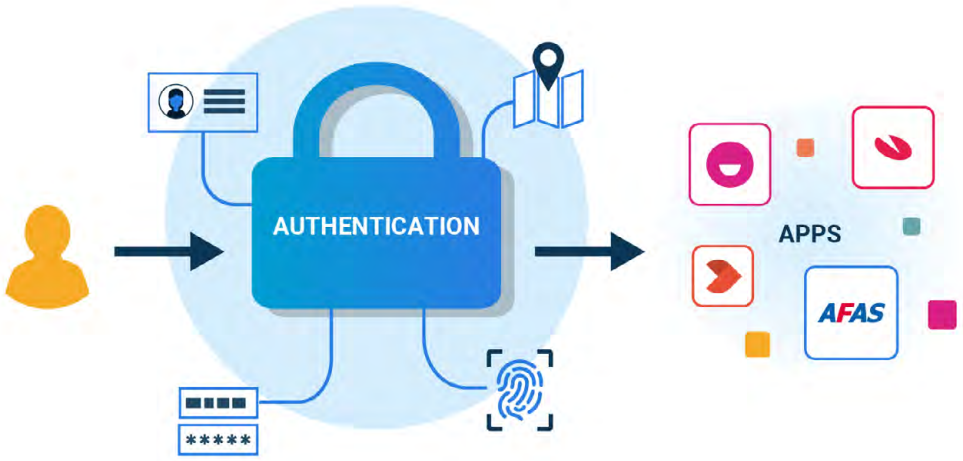
HelloID biedt die gewenste combinatie van standaardisatie en uitzonderingen:

- **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 of leerling krijgt. Vanaf de automatische onboarding bij indiensttreding tot en met de vertrekprocedure als iemand de school verlaat.
- Daarnaast voorziet HelloID in **uitzonderingen**. Voor specifiekere en lastig te automatiseren rechten kun je (self)service processen ontwerpen. Gebruikers kunnen hiermee zelf online toegang vragen tot applicaties of folders waarbij automatisch de juiste goedkeuringsstappen worden doorlopen. Na goedkeuring zorgt het geautomatiseerde proces voor de verdere activering zonder risicovolle uitzonderingen of vergissingen. Ook voor allerlei andere bijzondere processen – van noodprocedure tot gastaccounts – kun je zo geautomatiseerde processen implementeren waarbij altijd een strikte scheiding kan worden ingesteld tussen het aanvragen, toekennen en (de)activeren van accounts en toegangsrechten.

Geautomatiseerde configuratieregels zorgen dat de diensten- en datacatalogus automatisch up-to-date blijft. Een nieuwe applicatie of folder worden zo direct zichtbaar in de catalogus. Op ieder moment kan het systeem een overzicht geven van welke medewerkers en leerlingen actief zijn en welke licenties, applicaties, folders, et cetera zij in gebruik hebben.

Access management

Alle gebruikers - intern, extern en tijdelijk - en hun digitale activiteiten moeten uniek identificeerbaar zijn. Dat betekent dat groepsaccounts niet zijn toegestaan en identificatie, authenticatie en autorisatie van individuele gebruikers moet worden afgedwongen. Ook moet het gebruik van Two Factor Authentication (2FA) wordt ondersteund voor niet vertrouwde omgevingen en kritische systemen.



HelloID beschikt desgewenst over eigen Identity Provider functionaliteit maar vaak integreren we voor de primaire authenticatie met Active Directory, Entra ID en andere Identity Providers zoals Google, Salesforce, SAML en OpenID. Ook ondersteunt het platform extra beveiligingsopties zoals Two Factor Authentication (2FA). HelloID herkent bovendien 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. Om toegangsbeveiliging veilig én gebruiksvriendelijk te houden, ondersteunt HelloID 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.

Auditeerbaarheid van het IAM

Bij alle hiervoor genoemde processen is de registratie en rapportage essentieel. Als onderwijsinstelling moet je kunnen aantonen dat de verschillende processen volgens de relevante wet- en regelgeving worden uitgevoerd. Je moet de status van je rechtenbeheer op ieder moment kunnen reproduceren en bij een beveiligingsincident zoals een datalek snel kunnen traceren welke gebruikers welke handelingen hebben uitgevoerd. Ook moet alle informatie beschikbaar zijn om het toegangsbeleid en de uitgegeven accounts en toegangsrechten periodiek te beoordelen.

Als cloud based oplossing 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 auditeerbaar 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, wie 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.

Betrouwbaar Identity Management met hoge beschikbaarheid

De vorige hoofdstukken gingen over de rol die Identity en Access Management speelt bij het inrichten van je informatiebeveiliging. Tegelijkertijd is een IAM applicatie ook één van de binnen scholen gebruikte IT systemen. Hiervoor biedt het normenkader specifieke eisen die je bijvoorbeeld terugvindt in deze domeinen: Systeemontwikkeling, Datamanagement, Security Management, IT-Operatie en Ketenbeheer. Het is dus belangrijk om je IAM oplossing ook aan de hand van deze normen te beoordelen.

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. Compliance aan de strenge security-eisen is dan ook gewaarborgd. De dienstverlening heeft bovendien een zeer hoge beschikbaarheid dankzij de ingebouwde redundantie.

Als IDaaS (Identity as a Service) provider is het met name belangrijk dat wij een goede invulling geven aan domein 15 (ketenbeheer). Het gaat immers niet alleen om de kwaliteit van het platform, maar ook om de ondersteunende dienstverlening. In dat kader beschikt Tools4ever over een SOC 2 Type II auditverklaring. Zo'n Service Organization Controls audit is vooral gericht op dienstverlenende organisaties en een SOC 2-verklaring bevestigt naar klanten dat de kwaliteit van de dienstverlening is beoordeeld door een onafhankelijke deskundige. Deze beoordeling omvat het toezicht op de organisatie, programma's voor leveranciersbeheer, gedegen softwareontwikkeling, interne corporate governance en risicobeheerprocessen. Hiermee vormt de SOC 2 audit een belangrijke aanvulling op onze ISO 27001-certificatie.

Meer weten?

Identity Management vormt vandaag de dag een centrale rol binnen je IT beveiliging. Medewerkers en leerlingen 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 een informatiebeveiligingssysteem dat compliant is met het normenkader IBP FO.

Meer weten over de rol die Identity Management kan spelen bij de IBP FO compliance binnen je school of onderwijsinstelling? En hoe je de IT omgeving veilig kunt houden zonder in te leveren op gebruiksvriendelijkheid? We vertellen je hier graag meer over. Bijvoorbeeld aan de hand van onze reference list IBP FO – HelloID. In deze lijst behandelen we alle IBP FO normen met per norm een toelichting of – en zo ja, hoe – HelloID hieraan een bijdrage kan leveren.

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