# Bijlage D – Voorwaarden IAM

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| **Functionaliteit IAM** | | | | |
| **1** | **Identiteiten-beheer** | **Centraal beheer identiteiten** | **De oplossing moet centraal beheer van identiteiten mogelijk maken, waarbij alle digitale identiteiten binnen de organisatie op één plek worden beheerd volgens de geldende processen van Stichting BOOR. Dit omvat de standaard functionaliteiten van Identity Management (IDM), zoals het beheer van de volledige levenscyclus van identiteiten: het aanmaken, bijwerken en verwijderen. De oplossing moet daarnaast integreren met de Identity provider (IDP) Entra-ID om efficiëntie, consistentie en veiligheid in identiteitsbeheer te waarborgen.**<br>**Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **Een centraal beheerde identiteit verbetert de beveiliging, efficiëntie en gebruikerservaring.** |
| 1.1 | | Meerdere Entra-ID tenants (IDP) per identiteit | Binnen BOOR zijn meerdere Entra-ID tenants (IDP). Het moet mogelijk zijn om aan één identiteit, afhankelijk van de autorisatie van de identiteit, meerdere Microsoft accounts te koppelen die in de afzonderlijke tenants gebruikt kunnen worden. | Ondersteunen huidige inrichting van de organisatie. |
| 1.2 | | Signalering en verwerking dubbele identiteiten | De oplossing moet unieke identiteiten toewijzen en daarom dubbele identiteiten kunnen signaleren op basis van vooraf gedefinieerde attributen, zoals e-mailadressen, personeelsnummers of andere unieke kenmerken. Hierbij moet de mogelijkheid bestaan om meerdere broninstanties handmatig en, bij voorkeur, automatisch te koppelen aan één unieke identiteit. Indien geen match gevonden wordt, moet de oplossing in staat zijn om automatisch een nieuwe identiteit aan te maken op basis van vooraf ingestelde naamgevingsconventies. | Dit proces draagt bij aan de consistentie en nauwkeurigheid van het identiteitsbeheer binnen de organisatie, terwijl het handmatig beheer tot een minimum wordt beperkt. |
| 1.3 | | Tijdelijke identiteiten | Het moet mogelijk zijn om in de IAM-oplossing tijdelijke identiteiten aan te maken, te wijzigen, te pauzeren, of te verwijderen, ook wanneer deze niet in de bronsystemen worden beheerd. De tijdelijke aard van deze identiteiten wordt gewaarborgd door een verplichte einddatum in te stellen bij het aanmaken, zodat ze automatisch verlopen en de toegang op het juiste moment wordt beëindigd. | Het creëren van tijdelijke identiteiten in de IAM-oplossing en niet direct in de bronsystemen biedt meer controle, veiligheid, flexibiliteit en compliance, terwijl het bronsysteem overzichtelijk en vrij van tijdelijke of irrelevante accounts, zoals (dag)gast- en testaccounts, blijft. |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| 1.4 | | (Tijdelijk) intrekken identiteit | De mogelijkheid voor een beheerder om handmatig identiteiten (tijdelijk) in te trekken en daarmee ook de accounts voor de (verschillende) identity providers (IDP) te deactiveren. | In situaties waarin er een direct beveiligingsrisico ontstaat, zoals bij verdachte activiteiten of bij een medewerker die met langdurig verlof gaat, moet een beheerder, snel, kunnen ingrijpen en tijdelijk de toegang tot systemen of gevoelige gegevens kunnen beperken. Dit biedt niet alleen controle bij urgente situaties, maar zorgt er ook voor dat het toegangsbeheer kan worden afgestemd op veranderende omstandigheden, zonder afhankelijk te zijn van geautomatiseerde processen. Hierdoor wordt de kans op ongeautoriseerde toegang geminimaliseerd en blijft de beveiliging van de organisatie op peil. |
| **2** | **Autorisatie-beheer** | **Centraal beheer autorisaties** | **De oplossing moet centraal beheer van autorisaties, volgens de geldende processen van Stichting BOOR, mogelijk maken, waarbij alle toegangsrechten binnen de organisatie efficiënt worden beheerd. Dit omvat standaard Access Management (AM)-functionaliteiten zoals het inrichten, beheren en handhaven van autorisatieregels, evenals het toekennen en intrekken van toegangsrechten. De oplossing automatiseert autorisatieprocessen door dynamisch toegangsrechten toe te wijzen of in te trekken op basis van rolwijzigingen of andere relevante criteria.**<br>**Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **Zorgdragen voor een robuust en flexibel autorisatiebeheer dat voldoet aan de behoeften van moderne organisaties op het gebied van beveiliging, compliance, en efficiëntie.** |
| 2.1 | | RBAC | Stichting Boor moet in staat zijn om rollen centraal te beheren, inclusief het instellen van een start- en einddatum, en automatisch toe te wijzen aan gebruikers op basis van hun functie, afdeling of positie in de organisatie. | De oplossing moet Rolgebaseerde Toegangscontrole (RBAC) ondersteunen, wat inhoudt dat gebruikers op basis van hun rol(-len) binnen de organisatie toegang krijgen tot systemen en applicaties. |
| 2.2 | | ABAC | Stichting BOOR moet in staat zijn om gedetailleerde toegangs- en beleidsregels, inclusief het instellen van een start- en einddatum, te definiëren op basis van gebruikersattributen, zoals rol, afdeling, locatie, of functie binnen de organisatie. Dit maakt het mogelijk om toegangsrechten fijnmazig en dynamisch te beheren, waarbij toegangsbeslissingen automatisch kunnen worden aangepast op basis van veranderende omstandigheden of attributen. | De oplossing moet Attribuutgebaseerde Toegangscontrole (ABAC) ondersteunen, waarbij toegang wordt toegekend op basis van attributen van de gebruiker, zoals school, groep of beveiligingsniveau. Door deze flexibiliteit kan de organisatie eenvoudig contextgevoelige toegang implementeren. Dit bevordert zowel de veiligheid als de efficiëntie van het toegangsbeheer, terwijl het nalevingsvereisten en beleidsregels van de organisatie ondersteunt. |
| 2.3 | | Hiërarchieën van rollen (persona) | De oplossing moet de mogelijkheid bieden om hiërarchieën van rollen, inclusief een start- en einddatum, te creëren, zodat hogere rollen automatisch de rechten krijgen van lagere rollen. | Bevorderen van consistentie en efficiëntie in het toegangsbeheer, doordat het beheer van toegangsrechten eenvoudiger wordt bij complexe organisatiestructuren. Door gebruik te maken van rolhiërarchieën kunnen rechten centraal worden beheerd en geüpdatet, waarbij |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| | | | | wijzigingen in lagere rollen automatisch worden doorgevoerd naar hogere rollen. Dit verkleint de kans op fouten, vermindert administratieve lasten en zorgt ervoor dat gebruikers snel de juiste rechten krijgen op basis van hun positie binnen de organisatie. |
| 2.4 | | Tijdelijk intrekken autorisaties | De oplossing moet beheerders in staat stellen om handmatig toegangsrechten in te trekken of te pauzeren op basis van individuele omstandigheden. | Voorkomen dat autorisaties onnodig lang toegewezen blijven, bijvoorbeeld in situaties zoals bij een medewerker die met sabbatical gaat of langdurig afwezig is. |
| 2.5 | | Delegeren / mandateren | De oplossing moet de mogelijkheid bieden om bepaalde bevoegdheden voor het beheren van toegangsrechten op een gecontroleerde en traceerbare manier (tijdelijk) over te dragen aan andere gebruikers of rollen binnen de organisatie. | Zorgdragen voor een flexibele en efficiënte verdeling van toegangsbeheer passend bij de verschillende schoolinrichtingen, terwijl de controle en verantwoording behouden blijft via audit logs en rapportages. |
| 2.6 | | Expliciete toegang | Identiteiten moeten tijdelijke rechten kunnen verkrijgen voor specifieke taken, applicaties of projecten. Hiervoor moet de oplossing autorisatie op aanvraag mogelijk maken, waarbij gebruikers tijdelijk rechten kunnen aanvragen die worden toegekend na goedkeuring die is gedefinieerd in een workflow. Expliciete toegang is altijd inclusief einddatum en opgaaf van reden. | De oplossing moet dynamische en fijnmazige toegangsmogelijkheden bieden, waarbij autorisaties flexibel kunnen worden aangepast op basis van veranderende omstandigheden of tijdelijke behoeften. |
| 2.7 | | Scheiding van taken (SOD) | De oplossing moet beleid ondersteunen dat scheiding van taken (Segregation of Duties, SoD) afdwingt door automatisch te controleren en te voorkomen dat conflicterende rollen, zoals het aanmaken én goedkeuren van betalingen, aan één enkele gebruiker worden toegewezen. | Dit voorkomt dat een gebruiker toegang krijgt tot systemen of gegevens die kunnen leiden tot belangenconflicten of frauderisico's, zoals het gelijktijdig kunnen aanmaken van facturen en het goedkeuren van betalingen. Door SoD-beleid te implementeren, wordt ervoor gezorgd dat kritieke functies altijd door meerdere personen worden uitgevoerd, wat de integriteit van bedrijfsprocessen en de naleving van interne en externe regelgeving waarborgt. |
| 2.8 | | Rapporteren verschil IST-SOLL | Bij wijziging van de inrichting van de autorisatiestructuur moet de IAM-oplossing de mogelijkheid bieden om de uitkomst te simuleren voordat de wijzigingen daadwerkelijk worden doorgevoerd. | De beheerders in staat stellen om te zien welke impact de wijzigingen zullen hebben op de toegangsrechten van gebruikers en systemen, zodat ongewenste gevolgen, zoals onterechte toegang of verlies van essentiële rechten, kunnen worden voorkomen. Het simuleren van autorisatiewijzigingen draagt bij aan een veiligere en gecontroleerde implementatie van veranderingen binnen het toegangsbeheer. |
| **3** | **Workflow-management** | **Centraal inrichten en beheren workflows** | **De oplossing moet Stichting BOOR de mogelijkheid bieden om workflows in te richten en te beheren, zodat processen zoals het toekennen, intrekken of aanpassen van toegangsrechten efficiënt kunnen worden geautomatiseerd. Beheerders moeten in staat zijn om op basis van vooraf gedefinieerde** | **Waarborgen van consistent en gestroomlijnd beheer van toegangsrechten en andere administratieve taken.** |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| | | | **regels en triggers workflows te configureren, bijvoorbeeld bij rolwijzigingen, nieuwe gebruikersregistraties of het verlopen van tijdelijke toegangsrechten. Daarnaast moet de oplossing mogelijkheden bieden voor het monitoren en optimaliseren van bestaande workflows om de efficiëntie te verbeteren en beveiligingsrisico's te minimaliseren.**<br>**Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | |
| 3.1 | | Minimale set aan workflows | Tijdens de initiële implementatie moeten minimaal de volgende workflows beschikbaar worden gemaakt:<br>- Onboarding nieuwe identiteit<br>- Doorstroom/uitbreiding rechten<br>- Offboarden identiteit<br>- Aanvraag expliciete toegang<br>- Attestatie | |
| 3.2 | | Integratie servicemanagement -systeem | De oplossing moet naadloos kunnen communiceren met Topdesk om toegangsbeheerprocessen te automatiseren en te stroomlijnen. Dit omvat het automatisch aanmaken van tickets in Topdesk op basis van triggers in de IAM-omgeving, zoals het aanmaken van nieuwe gebruikers, het aanvragen van toegangsrechten, of het intrekken van rechten bij functiewijzigingen of offboarding. De integratie moet ook mogelijk maken de status op tickets vanuit Topdesk worden gesynchroniseerd met de IAM-workflows, zodat autorisaties consistent en transparant worden beheerd. | De integratie met Topdesk maakt het mogelijk om autorisaties die handmatig geïmplementeerd moeten worden, zoals de uitgifte van tags, toch centraal op basis van RBAC en ABAC ingericht kunnen worden. |
| 3.3 | | Integratie mailvoorziening | De oplossing moet de mogelijkheid bieden tot het versturen van dynamische mailberichten gebaseerd op attributen als naam, rol, workflow, status. | Het mogelijk maken om binnen workflows berichten te versturen waarin gegevens opgenomen zijn zoals het soort wijziging, naam medewerker, naam leidinggevende.<br>Toepassingsvoorbeeld: Informeren leidinggevenden en eigenaren over wijzigingen.<br>Bijvoorbeeld: Beste <voornaam> <achternaam>, Uw aanvraag voor Visio is geaccepteerd en actief per <datum>. |
| 3.4 | | Ondersteuning meerdere goedkeurders | De oplossing moet ondersteunen dat aanvragen kunnen worden toegewezen aan meerdere goedkeurders indien nodig (bijv. een informatie eigenaar en manager). | De mogelijkheid om aanvragen toe te wijzen aan meerdere goedkeurders, zoals een informatie-eigenaar en een manager, is essentieel om te voldoen aan organisatie specifieke goedkeuringsprocessen en om een extra beveiligingslaag toe te voegen, zoals het vier-ogenprincipe. |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| **4** | **Auditing en Attestatie** | **Auditing** | **De oplossing moet volledige, accurate en niet aanpasbare auditlogs genereren die alle identiteit en toegang gerelateerde activiteiten vastleggen, zoals aanmaak, deactivatie en wijzigingen in identiteiten, rollen, toegangsrechten en goedkeuringsprocessen. Deze logs moeten eenvoudig toegankelijk zijn voor beheerders en auditors, met mogelijkheden om rapportages te genereren voor compliance, interne controles en forensisch onderzoek. Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **Het genereren van uitgebreide auditlogs is cruciaal voor transparantie, beveiliging en compliance, omdat het alle toegang gerelateerde activiteiten traceerbaar maakt. Deze logs ondersteunen beheerders bij het opsporen van ongeautoriseerde toegang en het uitvoeren van interne controles, terwijl ze voldoen aan wettelijke eisen zoals AVG. Eenvoudig toegankelijke logs en rapportagemogelijkheden zorgen daarnaast voor effectieve incidentrespons.** |
| 4.1 | | Autorisatie tot auditlogs | Alleen geautoriseerde beheerders mogen toegang hebben tot de auditlogs. Logs moeten beveiligd zijn tegen ongeoorloofde toegang. | Toegang tot auditlogs moet beperkt blijven tot geautoriseerde beheerders om de vertrouwelijkheid van gevoelige gegevens te waarborgen en het risico op ongeoorloofde toegang te minimaliseren. |
| 4.2 | | Bewaartermijnen auditlogs | Auditlogs worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze zijn verzameld en worden automatisch verwijderd na afloop van de bewaartermijnen die in overleg met Stichting BOOR zijn vastgesteld. | Het naleven van bewaartermijnen voor auditlogs en het automatische verwijderen ervan na deze periode is essentieel om te voldoen aan privacywetgeving en het risico op ongeoorloofde toegang tot verouderde gegevens te minimaliseren, terwijl het beleid in overeenstemming blijft met de afspraken van Stichting BOOR. |
| 4.3 | | Registratie workflow in auditlog | Alle toegangsaanvragen en goedkeuringsacties moeten worden gelogd voor auditdoeleinden, inclusief wie het verzoek heeft ingediend, wie het heeft goedgekeurd of afgewezen, eventuele opmerkingen of wijzigingen die zijn gemaakt, en of de toegangsaanvraag wel of niet toegewezen is. | Het loggen van alle toegangsaanvragen en goedkeuringsacties is cruciaal voor auditdoeleinden, omdat het zorgt voor volledige traceerbaarheid en verantwoordelijkheid binnen het toegangsbeheerproces. Door vast te leggen wie een verzoek heeft ingediend, wie het heeft goedgekeurd of afgewezen, en welke wijzigingen of opmerkingen zijn gemaakt, kunnen organisaties achteraf nauwkeurig controleren of toegangsbeslissingen volgens beleid en compliance-vereisten zijn genomen. |
| **5** | **Auditing en Attestatie** | **Attestatie** | **De oplossing ondersteunt periodieke controles (attestaties) om te bevestigen dat gebruikers nog steeds de juiste toegangsrechten hebben op basis van hun rol en verantwoordelijkheden. Beheerders, leidinggevenden en proces-/systeem-/informatie-eigenaren moeten in staat zijn om op geplande intervallen de toegangsrechten van gebruikers te herzien en goed te keuren of te herroepen, met een duidelijk en geautomatiseerd proces voor het verzamelen van goedkeuringen van leidinggevenden of andere belanghebbenden. Naast bovenstaande heeft Stichting BOOR de volgende aanvullende** | **Deze functie is essentieel voor naleving van beveiligings- en compliance-eisen, zoals het principe van least privilege, en zorgt ervoor dat toegangsrechten continu worden afgestemd op de actuele behoeften en risico's binnen de organisatie.** |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| | | | **requirements:** | |
| 5.1 | | | De oplossing heeft de mogelijkheid om door middel geautomatiseerde tools of scripts controles uit te voeren op autorisatieregels en toegekende autorisaties. Indien dit geen standaard functionaliteit is moet de oplossing de optie bieden om deze gegevens te exporteren, zodat diepgaande analyses buiten het systeem kunnen worden uitgevoerd. | Dit verhoogt de efficiëntie van het beheer en maakt het mogelijk om eenvoudig naleving van beleidsregels te controleren en te analyseren. |
| **6** | **Koppelingen** | **Integratie bron-/doelsystemen** | **De oplossing moet kunnen integreren met verschillende systemen die als bron en/of doel fungeren voor identiteits- en toegangsbeheer. De IAM-oplossing moet deze systemen naadloos kunnen koppelen en synchroniseren, zodat identiteiten en toegangsrechten consistent zijn in alle systemen. Daarnaast moeten wijzigingen in bron- of doelsystemen automatisch, volgens de bij Stichting BOOR geldende processen, worden doorgevoerd in het IAM-systeem om handmatige tussenkomst te minimaliseren en de efficiëntie te verhogen.<br>Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **Het integreren van de IAM-oplossing met verschillende bron- en doelsystemen is essentieel om ervoor te zorgen dat identiteiten en toegangsrechten consistent en actueel blijven in alle systemen. Door deze systemen naadloos te koppelen en te synchroniseren, wordt het risico op fouten of beveiligingslacunes door handmatige updates geminimaliseerd. Automatische doorvoering van wijzigingen in bron- en doelsystemen verhoogt de efficiëntie en maakt het mogelijk om toegangsbeheer in real-time te beheren, wat cruciaal is voor de beveiliging en naleving van compliance-eisen.** |
| 6.1 | | Bron-/doelsystemen | De oplossing moet tenminste koppeling(en) kunnen maken als bron- en doelsysteem met AFAS, Magister, ParnasSys, Somtoday, Presentis, Zermelo en Microsoft-modules zoals Entra, Exchange en Teams. Eventuele specifieke eisen per koppeling zijn apart opgenomen. | De genoemde bron-/doelsystemen fungeren als bron voor in-, door- en uitstroomprocessen en leveren aanvullende gegevens die als attributen aan identiteiten moeten worden toegevoegd. Daarnaast dienen deze systemen als doelsystemen voor de (de)provisioning van accounts en toegangsrechten. |
| 6.2 | | Real-time en batchsynchronisatie | De oplossing moet in staat zijn om zowel real-time als batchsynchronisaties uit te voeren, zodat gegevens bij voorkeur direct in de systemen worden bijgewerkt. Voor systemen die niet continu beschikbaar zijn voor real-time synchronisatie, worden updates op vaste tijdstippen uitgevoerd, zoals dagelijks of wekelijks. | Dit garandeert dat alle systemen up-to-date blijven, terwijl de flexibiliteit behouden blijft om aan te sluiten bij de beschikbaarheid en prestaties van verschillende systemen. |
| 6.3 | | Import- en exportfunctionaliteit | De oplossing moet goed gedocumenteerde API's bieden voor het importeren van identiteiten en attributen, en het exporteren van identiteiten en autorisaties, met ondersteuning voor RESTful API's en Webhooks. Deze API's moeten voldoen aan moderne beveiligings- en interoperabiliteitsstandaarden, zoals SCIM (System for Cross-domain Identity Management) en LDAP (Lightweight Directory Access Protocol), om een consistente en efficiënte uitwisseling van identiteitsgegevens te garanderen. | Dit maakt het mogelijk om andere systemen op een flexibele, schaalbare en veilige manier te integreren. Ondersteuning voor moderne standaarden zoals SCIM en LDAP zorgt ervoor dat provisioning-processen gestroomlijnd verlopen en systemen gemakkelijk met elkaar kunnen communiceren, terwijl de beveiliging en interoperabiliteit worden gewaarborgd. Dit maakt het mogelijk om gebruikersidentiteiten veilig en schaalbaar te beheren in complexe IT-omgevingen. |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| 6.4 | | Aansluiting onderwijs-uitwisselings-standaarden | De oplossing ondersteunt de laatste versies van de onderwijs-uitwisselingsstandaarden, zoals opgenomen in de FORA, ROSA en EDU-V. | Deze standaarden bevorderen een gestandaardiseerde en veilige uitwisseling van gegevens tussen verschillende systemen en instellingen, wat cruciaal is voor een efficiënte administratie en betere samenwerking binnen het onderwijs. Door deze standaarden te volgen, blijft de oplossing future-proof en in lijn met de wettelijke en operationele eisen van de sector, waardoor adoptie en integratie makkelijker worden. |
| **7** | **Koppelingen** | **Beheer en monitoring** | **De oplossing moet in staat zijn om de status en werking van de koppelingen continu te bewaken en te beheren. Dit omvat het monitoren van de synchronisatie tussen het IAM-systeem en de bron-/doelsystemen om ervoor te zorgen dat de provisioning van gegevens zoals accounts, rollen en toegangsrechten correct en consistent verloopt. Beheerders moeten inzicht krijgen in status van deze koppelingen, inclusief waarschuwingen bij storingen, synchronisatiefouten of andere afwijkingen.**<br>**Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **Het continu bewaken en beheren van de status en werking van de koppelingen is essentieel om de consistentie en juistheid van gegevens zoals accounts, rollen en toegangsrechten te waarborgen. Door het monitoren van de synchronisatie tussen het IAM-systeem en bron-/doelsystemen kunnen beheerders proactief reageren op eventuele storingen, synchronisatiefouten of afwijkingen, wat de betrouwbaarheid van de provisioning-processen verhoogt. Dit inzicht stelt beheerders in staat om snel in te grijpen en problemen op te lossen, wat cruciaal is voor het handhaven van de operationele continuïteit en het voldoen aan de beveiligings- en compliance-eisen van Stichting BOOR.** |
| 7.1 | | Handmatig stoppen, starten en pauzeren. | De oplossing moet mogelijkheden bieden voor het beheer van koppelingen, zoals het handmatig starten, tijdelijk pauzeren, en het opnieuw synchroniseren van de datastromen. | Dit stelt beheerders in staat om snel in te grijpen bij technische problemen, wijzigingen in bedrijfsprocessen of geplande onderhoudsactiviteiten, zonder de gehele integratie te verstoren. Hierdoor blijft de consistentie van gegevens gewaarborgd en kunnen eventuele fouten of verstoringen proactief worden aangepakt, wat de betrouwbaarheid en continuïteit van het toegangsbeheer verbetert. |
| 7.2 | | Data-interpretatie | De oplossing moet de mogelijkheid bieden om eenvoudige beleidsregels toe te voegen voor het interpreteren, transformeren en toewijzen van data tussen systemen. | Dit maakt het mogelijk om de datastromen flexibel aan te passen op basis van specifieke bedrijfsbehoeften, en zorgt ervoor dat toegangsrechten en identiteiten nauwkeurig en consistent worden beheerd. |
| 7.3 | | Automatic response | De oplossing moet in staat zijn om op basis van vooraf ingestelde drempelwaarden automatisch te reageren, bijvoorbeeld door de data-uitwisseling automatisch te pauzeren en/of een waarschuwing te sturen naar beheerders. | Dit zorgt voor snelle en proactieve actie bij het detecteren van afwijkingen of fouten, waardoor verdere problemen worden voorkomen en de integriteit van de gegevens behouden blijft. |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| **8** | **Koppelingen** | **Microsoft-tenant** | **De koppeling van de IAM-oplossing met de verschillende Microsoft-tenants moet een moderne cloudgebaseerde integratie bieden die identiteits- en toegangsbeheer volledig automatiseert en centraliseert. Deze integratie moet zorgen voor de naadloze uitwisseling van identiteiten en autorisaties tussen de systemen, zodat het IAM-systeem deze effectief kan beheren en synchroniseren.** | **Het bieden van een cloudgebaseerde integratie tussen de IAM-oplossing en meerdere Microsoft Entra-tenants is essentieel om identiteiten en toegangsrechten centraal en automatisch te beheren in een moderne, dynamische IT-omgeving. Door identiteiten en autorisaties naadloos tussen de systemen uit te wisselen, kan het IAM-systeem niet alleen effectief toezicht houden op toegangsrechten, maar ook de uitgebreide beveiligingsmogelijkheden van Microsoft Entra benutten, zoals SSO en MFA. Dit verhoogt zowel de beveiliging als de efficiëntie, terwijl het beheer van identiteiten en toegangsrechten sterk wordt vereenvoudigd in een cloud-first omgeving.** |
| 8.1 | | Multi-tenant | De oplossing moet meerdere tenants (zoals verschillende scholen of afdelingen) ondersteunen, waarbij elke tenant volledig gescheiden is qua gegevens en toegangsbeheer. Dit houdt in dat elke tenant zijn eigen gebruikers, rechten, beleidsregels en applicaties kan beheren zonder tussenkomst van andere tenants. | Dit stelt scholen in staat om hun gebruikers, rechten, beleidsregels en applicaties onafhankelijk te beheren, zonder risico op gegevensvermenging of ongeautoriseerde toegang tussen tenants. Deze scheiding is essentieel voor de veiligheid en privacy van gevoelige gegevens, zoals leerlinginformatie, en garandeert dat elke school of afdeling zijn eigen processen autonoom kan beheren, terwijl de IT-omgeving schaalbaar en beheersbaar blijft. |
| **9** | **Koppelingen** | **Microsoft Exchange** | **De IAM-oplossing moet automatisch e-mailaccounts kunnen aanmaken en bijwerken wanneer gerelateerde attributen, zoals voorkeursnaam, veranderen in het bronsysteem. Dit omvat het beheer van e-mailadressen en aliassen, waarbij wijzigingen in gebruikersinformatie of domeininstellingen direct worden doorgevoerd om ervoor te zorgen dat e-mailadressen consistent blijven en aansluiten op de geldende beleidsregels. De oplossing moet ook ondersteuning bieden voor het automatisch aanpassen van e-mailaliassen op basis van rolveranderingen of organisatorische wijzigingen, waardoor het e-mailbeheer efficiënt en foutloos blijft.**<br>**Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **Door wijzigingen zoals rolveranderingen of organisatorische updates automatisch door te voeren, blijft het e-mailbeheer up-to-date zonder handmatige tussenkomst, wat het risico op fouten aanzienlijk vermindert. Dit zorgt ervoor dat e-mailadressen en aliassen altijd correct zijn en aansluiten op de geldende beleidsregels, wat cruciaal is voor een gestroomlijnd communicatieproces en een veilige, foutloze werking van de IT-omgeving.** |
| 9.1 | | Maildomein/format per school | De oplossing moet het mogelijk maken om (per school) in te stellen welk domein en welk format er voor de mail gebruikt wordt. | Dit stelt scholen in staat om hun unieke domeinnamen en aliassen nauwkeurig te beheren, waardoor hun professionele en herkenbare identiteit in alle communicatie wordt gewaarborgd. Automatisering vermindert bovendien de kans op fouten en zorgt voor efficiënter beheer bij rolveranderingen of |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| | | | | organisatorische updates, zonder de schoolidentiteit in gevaar te brengen. |
| 9.2 | | Beheer op mailadressen | Beheerders moeten de mogelijkheid hebben om handmatig e-mailadressen, zowel primaire als secundaire, toe te voegen en te verwijderen. | Hiermee behouden beheerders de flexibiliteit om uitzonderingen te beheren en individuele aanpassingen door te voeren waar nodig, zonder afhankelijk te zijn van geautomatiseerde processen. |
| **10** | **Koppelingen** | **Micrsoft groups (oa. Teams)** | **De oplossing moet de mogelijkheid bieden om op basis van de organisatiestructuur uit de bronsystemen automatisch Microsoft (Teams-)groepen aan te maken en te beheren. Dit omvat het dynamisch toevoegen en verwijderen van gebruikers in op basis van wijzigingen in de structuur, zoals functiewisselingen, afdelings-/groepswijzigingen of nieuwe leerlingen/medewerkers. De IAM-oplossing moet ervoor zorgen dat Teams-groepen altijd up-to-date blijven, waarbij de juiste identiteiten automatisch toegang krijgen tot de relevante communicatiekanalen en samenwerkingsomgevingen.** | **Het automatisch aanmaken en beheren van Microsoft (Teams-)groepen stelt scholen in staat om de efficiëntie te verhogen door bijvoorbeeld jaarlijks groepen te creëren en te onderhouden voor de samenwerking tussen leerlingen en hun leerkrachten. Dit vermindert de handmatige inspanning voor het beheren van groepen en zorgt ervoor dat iedere leerling en leerkracht direct toegang heeft tot de juiste samenwerkingsomgevingen. Hierdoor kunnen scholen eenvoudig inspelen op veranderende klassen(indelingen) per schooljaar, wat bijdraagt aan een gestroomlijnd en effectief leerproces.** |
| **11** | **Self-service** | **Portaal** | **De oplossing moet een gebruiksvriendelijk portaal bieden waarmee gebruikers zelfstandig veelvoorkomende acties kunnen uitvoeren zonder tussenkomst van beheerders. Dit omvat functionaliteiten zoals het aanvragen of intrekken van toegangsrechten door identiteithouder, leidinggevende, mandaathouder of eigenaar, evenals het beheren en inzien van persoonlijke gegevens zoals contactinformatie en autorisaties. Het portaal moet naadloos integreren met het IAM-systeem en moet verzoeken automatisch doorsturen naar goedkeuringsworkflows indien nodig.**<br>**Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **Dit stelt identiteithouders, leidinggevenden, mandaathouders of eigenaren in staat om snel en direct toegang te beheren, zonder afhankelijk te zijn van handmatige tussenkomst van IT-beheerders. Het naadloos integreren van het portaal met het IAM-systeem en het automatisch doorsturen van verzoeken naar goedkeuringsworkflows zorgt voor een veilig, gestroomlijnd proces dat de operationele continuïteit bevordert en naleving van beveiligingsbeleid waarborgt.** |
| 11.1 | | | Gebruikers moeten in staat zijn om via het self-service portaal bepaalde toegangsfunctionaliteiten te delegeren. | Hierdoor kunnen verantwoordelijkheden eenvoudig worden overgedragen zonder tussenkomst van beheerders, bijvoorbeeld tijdens afwezigheid of in specifieke projecten, terwijl het beheer van toegangsrechten blijft voldoen aan interne controles. |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| **12** | **Beheer-module** | **Configureer-baarheid** | **De oplossing moet flexibel en eenvoudig kunnen worden aangepast aan de specifieke behoeften en beleidsregels van de organisatie, zonder dat hiervoor uitgebreide maatwerkontwikkeling nodig is.<br>Het gaat hier om standaard configuratiemogelijkheden zoals:<br>- Aanpassen beleidsregels<br>- Activatie/deactivatie identiteit en gekoppelde accounts<br>- Aanmaak/verwijderen accounts in tenant(s)<br>- Bewaartermijnen identiteiten<br>- Configureerbaarheid attributen als account, mailadres (apart van account), naam, etc.<br>Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **De configureerbaarheid van de oplossing verhoogt de wendbaarheid van de organisatie, maakt het mogelijk om snel in te spelen op nieuwe compliance-eisen, veranderingen in personeelsstructuren, of wijzigingen in bedrijfsprocessen.** |
| 12.1 | | Verlengde toegang bij doorstroom | De mogelijkheid om in te stellen wanneer een identiteit toegang mag hebben tot de nieuwe gegevens en hoe lang een medewerker toegang behoudt bij doorstroom binnen BOOR. | Ondersteunen overdracht tussen medewerkers. Voorbeeld medewerker mag twee maanden eerder bij documenten van zijn/haar nieuwe afdeling, voordat diegene daadwerkelijk doorstroomt. |
| 12.2 | | Configuratie account format | Binnen BOOR zijn meerdere IDP's voor het proces toegang verlenen. Het moet mogelijk zijn om per IDP/resource een accountformat in te stellen. | Aan kunnen sluiten bij het format van de organisatie. Bijvoorbeeld: ali.elsahin@stichtingboor.nl, gwe@wolfert.nl |
| 12.3 | | Einddatum expliciete toegang | In kunnen stellen wat de maximale termijn is van handmatig ingerichte autorisaties. | Autorisaties niet onnodig lang toegewezen zijn. |
| 12.4 | | Configuratie batch synchronisatie | De oplossing moet per koppeling de mogelijkheid bieden om te bepalen wanneer, hoe frequent en op welke tijdstippen data uit bronsystemen wordt opgehaald en identiteiten en autorisaties naar doelsystemen worden geprovisioned. Beheerders moeten flexibele instellingen kunnen configureren om de synchronisatieprocessen aan te passen op basis van de behoeften van elk systeem. | Dit zorgt voor optimaal beheer en planning van datastromen, voorkomt overbelasting van systemen, en garandeert dat de gegevens consistent en up-to-date blijven door nauwkeurige synchronisatie op de meest geschikte tijdstippen en frequenties. |
| 12.5 | | Hergebruik accountnamen en mailadressen | Accountnamen en e-mailadressen mogen gedurende een vooraf instelbare periode niet opnieuw worden gebruikt. Na het verstrijken van deze periode moeten ze beschikbaar komen voor hergebruik. | Het tijdelijk niet hergebruiken van accountnamen en e-mailadressen na deactivering voorkomt verwarring en mogelijke beveiligingsrisico's, zoals het per ongeluk toewijzen van een oud account aan een nieuwe gebruiker of het ontvangen van e-mails die bedoeld waren voor een vorige gebruiker. Door deze gegevens pas na een configureerbare periode opnieuw beschikbaar te maken, wordt de integriteit van de accounts gewaarborgd, terwijl hergebruik op de lange termijn zorgt voor efficiënt beheer van IT-resources. |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| **13** | **Beheer-module** | **Beheerschermen** | **De oplossing biedt intuïtieve en overzichtelijke beheerschermen. Aangevuld met dashboards voor overzichtelijke weergaven van de status van identiteiten, rollen, toegangsrechten, en beleidsregels, inclusief waarschuwingen en belangrijke acties die aandacht vereisen.<br>De schermen bieden zoek- en filterfunctionaliteit voor het snel zoeken naar gebruikers, rollen, of rechten en het toepassen van filters op basis van specifieke attributen, zoals afdelingen, rollen of toegangsniveaus, om eenvoudig inzicht te krijgen in identiteitgroepen.<br>Naast bovenstaande heeft Stichting BOOR de volgende aanvullende requirements:** | **De beheerschermen moeten ervoor zorgen dat het beheer van de IAM-oplossing efficiënt en transparant verloopt, terwijl de kans op fouten wordt geminimaliseerd en de naleving van beveiligings- en compliance-eisen wordt gegarandeerd.** |
| 13.1 | | Schermen bij gevraagde requirements | De oplossing biedt beheerschermen waarmee beheerders efficiënt de in deze voorwaarden vastgelegde requirements kunnen beheren en uitvoeren. | Het aanbieden van beheerschermen die beheerders in staat stellen de vastgelegde requirements efficiënt uit te voeren, is essentieel voor effectief beheer van de IAM-oplossing. |
| 13.2 | | Inzien identiteiten | De oplossing moet een overzicht bieden van alle actieve en inactieve identiteiten, inclusief hun attributen, rollen en toegangsrechten.<br>Beheerders moeten eenvoudig en helder inzicht krijgen in de actuele status en toegangsrechten van elke gebruiker, zodat zij snel en efficiënt beheeracties kunnen uitvoeren. | Dit geeft beheerders volledige zichtbaarheid in de toegangsrechten van elke gebruiker en hun herkomst, wat helpt bij het voorkomen van ongeautoriseerde toegang, het opsporen van anomalieën en het waarborgen van naleving van beveiligings- en compliance-eisen. |
| 13.3 | | Gedelegeerd beheer | De oplossing moet de mogelijkheid bieden om het beheer van identiteiten en toegangsrechten te delegeren aan verschillende beheerders. Deze beheerders moeten bevoegd zijn om dit beheer uit te voeren voor specifieke delen van de organisatie of doelapplicaties. Hierbij dient de oplossing te waarborgen dat toegang wordt verleend op basis van het ‘least privilege’-principe. | Hierdoor kunnen verantwoordelijkheden gedecentraliseerd worden zonder de controle over het algehele toegangsbeheer te verliezen en wordt gewaarborgd dat beheerders enkel toegang krijgen tot de benodigde rechten en functies die strikt noodzakelijk zijn voor hun specifieke taken binnen het beheerproces. |
| **Applicatie** | | | | |
| **14** | **Beveiliging en compliance** | **Aanvullende beveiligings-requirements** | **De oplossing moet aan de in de IBP-voorwaarden gestelde requirements voldoen. Onderstaand zijn een aantal van deze requirements specifiek gemaakt voor de IAM-oplossing.** | |
| 14.1 | | SSO | Het Self-Service portaal en de beheermodule moeten Single Sign-On (SSO) functionaliteit ondersteunen, zodat gebruikers met één set inloggegevens toegang krijgen tot de portal. SSO moet minimaal gekoppeld kunnen worden aan één Microsoft-tenant, met voorkeur voor ondersteuning van multi-tenant om het beheer van meerdere omgevingen te vereenvoudigen en de gebruikerservaring verder te verbeteren. | Het ondersteunen van Single Sign-On (SSO) in de Self-Service portal en beheermodule verhoogt zowel de gebruiksvriendelijkheid als de beveiliging, doordat gebruikers met één set inloggegevens toegang krijgen tot meerdere systemen zonder zich telkens opnieuw te hoeven aanmelden. |

| ID | Categorie | Verkorte naam | Requirement | Motivatie |
|---|---|---|---|---|
| 14.2 | | Encryptie | Alle gegevens moeten versleuteld worden opgeslagen en overgedragen, waarbij zowel data in rust als tijdens overdracht wordt beveiligd met sterke encryptiemethoden op basis van moderne beveiligings- en compliance-standaarden. Hierbij moet rekening worden gehouden met het type data, zodat de juiste versleutelingsniveaus en technieken worden toegepast, afhankelijk van de gevoeligheid van de informatie. | Dit is essentieel om de vertrouwelijkheid, integriteit en veiligheid van gevoelige informatie te waarborgen en te beschermen tegen ongeautoriseerde toegang of datalekken. Sterke encryptie voorkomt dat kwaadwillenden gegevens kunnen lezen of manipuleren, zelfs als zij toegang krijgen tot de gegevensopslag of tijdens de gegevensoverdracht. Dit voldoet tevens aan de eisen van moderne beveiligings- en compliance-standaarden. |

**Voor akkoord:**

Ondergetekende verklaart hierbij de inhoud van deze bijlage volledig te hebben gelezen en begrepen, en akkoord te gaan met alle hierin gestelde voorwaarden. Tijdens de implementatieperiode zullen deze requirements getoetst worden. Indien u niet voldoet aan de requirements, is dat reden tot ontbinding van de overeenkomst. In geval van ontbinding zullen de reeds gefactureerde kosten gecrediteerd worden.

Handtekening: _____ Datum / /

Naam en functie _____ Plaats _____

Als rechtsgeldig vertegenwoordiger van: _____