Afbeelding met Lettertype, tekst, schermopname, Graphics

Automatisch gegenereerde beschrijving

Identiteits- en toegangsbeheer- beleid

Voorbeelddocument

Versie: juni 2025

Afbeelding met Kleurrijkheid, Graphics, blauw, patroon

Automatisch gegenereerde beschrijving

**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je bij het maken van een eigen identiteits- en toegangsbeheerbeleid. Elke school en elk schoolbestuur is anders. Pas het beleid daarom aan, zodat het past bij jouw situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je het beleid definitief maakt.
* Dit beleid gaat ervan uit dat taken, rollen en functies die nodig zijn om het beleid uit te voeren bij de juiste personen zijn belegd. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* Geel gearceerde teksten moet je vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.

Afbeelding met biljartbal, symbool, cirkel

Automatisch gegenereerde beschrijving

Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///C:/Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een e-mail naar [*ibp@kennisnet.nl*](mailto:ibp@kennisnet.nl)*.*

**Documentgeschiedenis**

***Toelichting***

* *Vul in wie het beleid vaststelt.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld. |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties>. |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

**Inhoudsopgave**

[1 Inleiding 5](#_Toc201586594)

[1.1 Doelstelling 5](#_Toc201586595)

[1.2 Reikwijdte 5](#_Toc201586596)

[2 Identiteitsbeheer 6](#_Toc201586597)

[2.1 Type identiteiten 6](#_Toc201586598)

[2.2 Instroom, doorstroom en uitstroom 7](#_Toc201586599)

[2.2.1 Registratie van personen 7](#_Toc201586600)

[2.2.2 Accountbeheer 8](#_Toc201586601)

[2.3 Authenticatie 9](#_Toc201586602)

[2.3.1 Wachtwoorden 9](#_Toc201586603)

[2.3.2 Single sign on 9](#_Toc201586604)

[2.3.3 Tweefactorauthenticatie 9](#_Toc201586605)

[3 Toegangsbeheer 10](#_Toc201586606)

[3.1 Toekennen en intrekken van rollen en rechten 10](#_Toc201586607)

[3.1.1 Role-based access control (RBAC) 10](#_Toc201586608)

[3.1.2 Losse rollen en rechten 11](#_Toc201586609)

[3.1.3 Autorisatiematrix 12](#_Toc201586610)

[3.2 Superusers en beheeraccounts 12](#_Toc201586611)

[4. Monitoring 13](#_Toc201586612)

[4.1 Periodieke controle van toegangsrechten 13](#_Toc201586613)

[4.2 Rapportage 13](#_Toc201586614)

[4.3 Beleidsherziening 14](#_Toc201586615)

# Inleiding

Dit is een beleid voor identity- en accessmanagement (IAM). We noemen dat ook wel identiteits- en toegangsbeheer. Het beschrijft hoe het schoolbestuur omgaat met het beheer van digitale identiteiten en toegangsrechten binnen de organisatie. IAM is een essentieel onderdeel van de informatiebeveiliging van je organisatie. Het zorgt voor grip op wie toegang heeft tot welke systemen en gegevens. Bovendien is een zorgvuldig IAM-proces noodzakelijk om te voldoen aan wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). Dit beleid vormt een belangrijke basis voor een veilige, beheersbare en toekomstbestendige digitale omgeving binnen <vul naam schoolbestuur in>.

## Doelstelling

***Toelichting***

* *Pas onderstaande doelstellingen aan, zodat ze passen bij jouw organisatie. Bepaal of je wilt voldoen aan een concreet volwassenheidsniveau en neem dit op in de doelstelling.*

Het doel van dit IAM-beleid is het waarborgen van veilige en efficiënte toegang tot digitale middelen, systemen en gegevens binnen alle onder dit bestuur vallende onderwijsinstellingen. Hiermee willen we het volgende bereiken:

1. **Bescherming van leerlingen, medewerkers en externe partijen** door middel van passende maatregelen.
2. **Centralisatie en standaardisatie van toegangsbeheer**, zodat gebruikers op het juiste moment en met de juiste rechten toegang hebben tot de juiste informatie.
3. **Vergroting van digitale weerbaarheid** door misbruik van accounts, datalekken en onbevoegde toegang tot systemen en data te voorkomen.
4. **Optimalisatie van beheer** door het creëren van een efficiënte aanpak voor het aanmaken, wijzigen en intrekken van accounts en de bijbehorende rollen en rechten.

Met dit beleid wordt een stevige basis gelegd voor een toekomstbestendige, veilige en gebruikersvriendelijke digitale leer- en werkomgeving.

## Reikwijdte

***Toelichting***

* *Pas onderstaande reikwijdte aan, zodat die past bij jouw organisatie. Bepaal hoe je omgaat met accounts en toegangsrechten van systemen die worden beheerd door leveranciers.*

Dit beleid is van toepassing op alle leerlingen, docenten, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van <vul naam schoolbestuur in>.

Het beleid heeft betrekking op het beheren van alle soorten accounts, rollen en rechten die toegang geven tot systemen die worden beheerd door <vul naam schoolbestuur in> of leveranciers van <vul naam schoolbestuur in>.

# Identiteitsbeheer

## Type identiteiten

***Toelichting***

* *Het is mogelijk dat er meer of minder type identiteiten worden onderscheiden binnen de bestaande IAM-processen van jouw organisatie. Pas onderstaande identiteiten daarom aan, zodat ze passen bij jouw situatie.*

We verlenen alleen toegang tot digitale voorzieningen aan personen die correct zijn geregistreerd en die toegang nodig hebben voor het uitvoeren van hun werk, voor het geven of volgen van onderwijs of vanwege een andere geldige reden. Binnen dit beleid worden de volgende categorieën gebruikers onderscheiden:

1. Medewerkers  
Personen die in loondienst zijn bij de school of het bestuur. Het gaat hierbij om:

* Onderwijzend personeel (leerkrachten, docenten)
* Ondersteunend personeel (administratie, conciërges, intern begeleiders, beleidsadviseurs etc.)
* Schoolleiding en bestuur

2. Tijdelijke krachten en inhuur  
Personen die tijdelijk werkzaamheden verrichten, maar niet in loondienst zijn.

3. Leerlingen  
Personen die zijn ingeschreven bij een van de scholen die onder dit schoolbestuur vallen en onderwijs volgen.

4. Ouders/verzorgers  
Ouders of wettelijk vertegenwoordigers van leerlingen, die beperkt toegang kunnen krijgen tot ouderportalen of communicatiesystemen (zoals leerlingvolgsystemen).

5. Gasten  
Personen die op uitnodiging van de school tijdelijk toegang krijgen tot bepaalde voorzieningen.

6. Externen  
Personen van externe organisaties– zoals leveranciers of samenwerkingspartners – die toegang nodig hebben tot specifieke onderdelen van het netwerk of bepaalde applicaties, onder voorbehoud van duidelijke afspraken over gebruik en beveiliging.

## Instroom, doorstroom en uitstroom

Hier beschrijven we de instroom, doorstroom en uitstroom van identiteiten en de bijbehorende accounts.

### Registratie van personen

***Toelichting***

* *Beschrijf waar, hoe en wie de registratie van personen vastlegt, zodat op basis van deze registratie de juiste accounts, rollen en rechten kunnen worden aangemaakt.*
* *Beschrijf per type identiteit hoe de registratie van een nieuw persoon leidt tot het aanmaken van de juiste accounts.*

De registratie van personen wordt vastgelegd in de bronsystemen voor de verschillende identiteiten. Per type identiteit is beschreven waar deze is vastgelegd en op welke manier er een signaal richting beheerders wordt verstuurd voor het aanmaken, wijzigen en intrekken van accounts.

1. Medewerkers

<*Voorbeeldbeschrijving*>  
<Personeel in loondienst wordt geregistreerd in het bronsysteem voor medewerkers. Hierbij wordt het volgende vastgelegd:

* Functie
* Datum indiensttreding
* Einddatum van de arbeidsovereenkomst.

Bij het registreren van de nieuwe medewerker in het bronsysteem, wordt er een ticket aangemaakt voor de beheerders. Zo kunnen zij de juiste accounts aanmaken binnen de verschillende systemen. Bij het wijzigen van de functie of bij beëindiging dienstverband wordt er een ticket aangemaakt voor het deactiveren van de accounts.>   
  
<Let op: dit is een voorbeeld. Het is mogelijk om het aanmaken van accounts te automatiseren binnen verschillende systemen op basis van brondata uit het systeem voor medewerkers. Pas deze beschrijving daarom aan, zodat deze past bij jouw situatie.>

2. Tijdelijke krachten en inhuur

<Beschrijf hoe de registratie van tijdelijke krachten en inhuur leidt tot het registreren van de juiste functie en het aanmaken van de juiste accounts.>

3. Leerlingen

<Beschrijf hoe de registratie van leerlingen leidt tot het registreren van de juiste functie en het aanmaken van de juiste accounts.>

4. Ouders/verzorgers

<Beschrijf hoe de registratie van ouders/verzorgers leidt tot het registreren van de juiste functie en het aanmaken van de juiste accounts.>

5. Gasten

<Beschrijf hoe de registratie van gasten leidt tot het registreren van de juiste functie en het aanmaken van de juiste accounts.>

6. Externen

<Beschrijf hoe de registratie van externen leidt tot het registreren van de juiste functie en het aanmaken van de juiste accounts.>

Voor een verdere uitwerking van het registreren van personen wordt verwezen naar het proces logische toegang.

### Accountbeheer

***Toelichting***

* *Het kan zijn dat binnen de organisatie alle accounts handmatig worden aangemaakt op basis van hr-brondata of het leerlingadministratiesysteem. Het kan ook zijn dat deze accounts automatisch worden aangemaakt. Beschrijf in deze paragraaf op welke manier dit binnen jouw organisatie gebeurt.*
* *Bepaal hoelang een account wordt gedeactiveerd voordat het wordt verwijderd.*

Op basis van de registratie in een van de bronsystemen wordt door <beschrijf hier hoe beheerders accounts aanmaken. Handmatig of geautomatiseerd>. Er wordt voor het aanmaken van accounts binnen de verschillende systemen zo veel mogelijk gebruikgemaakt van een unieke gebruikersnaam.

Tijdelijke krachten  
Accounts voor tijdelijke krachten – zoals invallers of stagiairs – worden aangemaakt met een einddatum, waarop het account automatisch inactief wordt.

Beheeraccounts (superusers)  
Voor het aanmaken van beheeraccounts (superusers) wordt waar mogelijk gebruikgemaakt van persoonlijke accounts. Deze persoonlijke accounts worden aangemaakt naast het reguliere account van de medewerker. Is het niet mogelijk om een persoonlijk beheeraccount aan te maken? Dan worden er extra beveiligingsmaatregelen genomen, zoals het afdwingen van multifactor-authenticatie (MFA) en het inrichten van logging. Er is extra toezicht op het aanmaken van beheeraccounts.

Break glass accounts  
Daarnaast zijn er <vul aantal in> break glass accounts. Deze accounts kunnen worden gebruikt in een noodsituatie, waarbij reguliere beheeraccounts niet toegankelijk zijn en het reguliere proces voor aanvragen van nieuwe accounts niet volledig kan worden gevolgd. Toegang tot deze accounts kan als volgt worden verkregen:

* De gegevens zijn gedocumenteerd en geborgd in de fysieke kluis die in beheer is van het schoolbestuur.
* De gegevens zijn gedocumenteerd in een digitale wachtwoordkluis, strikt toegankelijk voor bevoegde personen.

De break glass accounts kunnen worden geactiveerd binnen de beheeromgeving na het doorlopen van een noodprocedure.

Op basis van de beëindiging of wijziging van de registratie in een van de bronsystemen, deactiveren de beheerders de accounts. Gedeactiveerde accounts worden na <vul in> jaar verwijderd binnen de systemen. Voor een verdere uitwerking van het aanmaken van accounts wordt verwezen naar het proces logische toegang.

## Authenticatie

### Wachtwoorden

***Toelichting***

* *Beschrijf hoe de gebruiker het initiële wachtwoord ontvangt na het aanmaken van een account binnen een van de systemen.*
* *Beschrijf bij punt 2 of de organisatie een wachtwoordkluis aanraadt, zodat kan worden omgegaan met verschillende wachtwoorden voor de verschillende systemen.*

We hanteren waar mogelijk de volgende vereisten voor het beheer van wachtwoorden:

* <vul de minimale vereisten in voor wachtwoordsterkte. Denk aan de hoeveelheid tekens, gebruik van speciale tekens, veel voorkomende combinaties als 12345.>

1. Medewerkers maken gebruik van unieke wachtwoorden voor de verschillende systemen.
2. Het initieel verstrekte wachtwoord wordt verplicht gewijzigd na de eerste login.
3. Wachtwoorden van beheeraccounts worden minimaal elke 6 maanden gewijzigd.

* Wachtwoorden vanbreak glass accounts worden na elk gebruik gewijzigd en <beschrijf waar de wachtwoorden worden opgeslagen of bewaard>.
* <Vul aan>.

### Single sign on

***Toelichting***

* *Beschrijf voor welk deel van de systemen single sign on wordt gebruikt. Microsoft cloud-systemen maken bijvoorbeeld gebruik van Microsoft Entra ID als centrale identity provider en veel leermiddelen gebruiken Entree Federatie voor single sign on toegang.*

Bij toegang naar applicaties wordt bij voorkeur gebruikgemaakt van single sign on. Daarbij loggen gebruikers in met de centrale identiteit. De applicatie leidt de gebruiker eerst langs de identity provider waar de gebruiker inlogt. Daarna wordt de gebruiker voorzien van de juiste attributen – ten behoeve van autorisatie – en teruggestuurd naar de applicatie.

### Tweefactorauthenticatie

***Toelichting***

* *Bepaal voor welke systemen en gebruikers het afdwingen van tweefactorauthenticatie nodig is.*
* *Het ROSA-certificeringsschema bevat tweefactormaatregelen voor verschillende classificatieniveaus. Binnen het deelproject security baselines kan er per classificatieniveau een tweefactoreis worden opgenomen.*
* *Het kan zijn dat er onderscheid wordt gemaakt in tweefactorauthenticatie binnen en buiten het schoolnetwerk of voor verschillende gebruikersgroepen (leerlingen versus medewerkers). Is dit van toepassing op jouw situatie? Beschrijf dat dan hier.*

Op basis van de classificatie van de applicatie <voeg hier een verwijzing naar het classificatieproces toe> wordt tweefactorauthenticatie afgedwongen voor beheeraccounts en reguliere accounts.

# Toegangsbeheer

## Toekennen en intrekken van rollen en rechten

Hier beschrijven we het toekennen en intrekken van rollen en rechten van de accounts.

### Role-based access control (RBAC)

***Toelichting***

* *Beschrijf de verantwoordelijkheid van hr in het toekennen en bijhouden van de juiste functies en het versturen van de juiste signalen naar de beheerders van Active Directory en de applicaties bij een wijziging.*
* *Beschrijf wie er verantwoordelijk is voor het updaten en aanpassen van de centrale rollen en wie er verantwoordelijk is voor het toekennen en intrekken van deze centrale rollen.*
* *Zorg dat duidelijk is welke verschillende functies er binnen de organisatie aanwezig zijn. Op basis van deze functies– denk aan de functie docent, conciërge of security officer– kunnen er centrale rollen worden bepaald. Binnen de centrale identity provider (Active Directory) kunnen de verschillende securitygroepen als centrale rollen worden gebruikt.*
* *Bepaal zelf welk aantal centrale en applicatierollen werkbaar is voor jouw organisatie. Het beperken van de hoeveelheid rollen zorgt voor een goede beheersbaarheid. Het toevoegen van meer variatie zorgt voor een fijnmazigere toegang.*

Functies

Elke nieuwe gebruiker krijgt een functie toegewezen die wordt vastgelegd in het hr-bronsysteem. Zie 2.2.1. Een nieuwe leerling krijgt automatisch de functie van leerling, tenzij het nodig is daar onderscheid in te maken.

Afbeelding met tekst, schermopname, Lettertype, lijn

Door AI gegenereerde inhoud is mogelijk onjuist.

Centrale rollen

Elke functie wordt gekoppeld aan een van de centrale rollen. Deze rollen worden in de Active Directory als security groups aangemaakt.

* De centrale rollen worden ontwikkeld en beheerd door <vul functietitel in>.
* De centrale rol wordt door de beheerder van de Active Directory toegekend of ingetrokken na <beschrijf hier hoe het signaal van het aanmaken, wijzigen of beëindigen van een dienstverband– en daarmee de bijbehorende functie– terechtkomt bij de beheerders van de Active Directory, zodat centrale rollen tijdig worden ingetrokken>.

Applicatierollen

De rollen binnen de verschillende applicaties zijn zo veel mogelijk gelijk aan de centrale rollen van onze organisatie. Elke rol binnen een applicatie is gekoppeld aan een centrale rol. Op basis van de centrale rol maken de beheerders van de applicaties de juiste applicatierollen aan.

* De koppeling tussen de centrale rol en de corresponderende applicatierollen wordt ontwikkeld en beheerd door <geef aan of de systeemeigenaar of de beheerder in opdracht van de systeemeigenaar dit doet>.
* Na een wijziging van de centrale rol worden applicatierollen ingetrokken door <geef aan of de systeemeigenaar of de beheerder in opdracht van de systeemeigenaar dit doet>. <Beschrijf hier hoe het signaal van het toekennen of intrekken van een centrale rol terechtkomt bij de beheerders van de applicaties, zodat rollen en individuele rechten worden ingetrokken>.

Voor een verdere uitwerking van het toekennen van centrale rollen en applicatierollen wordt verwezen naar het proces logische toegang.

### Losse rollen en rechten

Het toekennen van losse rollen of individuele rechten wordt zo veel mogelijk beperkt.

De directe leidinggevende is verantwoordelijk voor alle individueel toegekende rollen en rechten die niet vallen binnen de centrale rol van gebruikers. De leidinggevende beslist over het toekennen en intrekken hiervan.

### Autorisatiematrix

***Toelichting***

* *Bepaal of je als organisatie een administratie van uitgegeven rollen en rechten wilt bijhouden (IST-matrix). Hou je geen IST-matrix bij? Verwijder dan de tekst hieronder die daar betrekking op heeft.*
* *Hou binnen de SOLL-matrix de koppeling tussen functies en centrale rollen en de koppeling tussen centrale rollen en de verschillende applicatierollen bij.*

We maken onderheid tussen een matrix waarin de huidige rollen en rechten worden bijgehouden (IST-matrix) en een matrix waarin de rollen en rechten worden bijgehouden zoals ze moeten worden toegekend volgens de functie van de gebruiker (SOLL-matrix).

**IST**

Alle superuser-, beheer- en service-accounts worden bijgehouden in een IST-matrix. In deze matrix wordt minimaal vastgelegd welke gebruikers toegang hebben tot accounts en wanneer de toegang van en tot deze accounts voor het laatst is beoordeeld.

**SOLL**

In de SOLL-matrix is vastgelegd welke centrale rol een gebruiker krijgt op basis van de functie. Vervolgens is er voor elke applicatie vastgelegd welke applicatierol een gebruiker krijgt op basis van de centrale rol. Sharepointgroepen of mailboxen worden net als applicatierollen vastgelegd in de SOLL-matrix en gekoppeld aan de centrale rol. De SOLL-matrix is niet bedoeld om de huidige rechten en rollen van medewerkers bij te houden. Dit gebeurt in de IST-matrix.

## Superusers en beheeraccounts

Voor iedere applicatie is het noodzakelijk om superusers en beheeraccounts aan te maken. Deze specifieke accounts hebben een grote hoeveelheid rechten in de applicatie om de werking van de applicatie te kunnen borgen. Voor supersusers en beheeraccounts gelden de volgende extra eisen:

* Beheeraccounts en superuser-accounts worden strikt gescheiden van persoonlijke gebruikersaccounts. Medewerkers gebruiken hun persoonlijke accounts voor reguliere werkzaamheden en aparte beheeraccounts voor beheertaken.
* Beheeraccounts worden uitsluitend gebruikt voor beheertaken.
* Superusers en beheeraccounts worden expliciet geregistreerd in een autorisatiematrix. Deze "IST-matrix" geeft een actueel overzicht van alle bestaande beheeraccounts en hun rechten.
* Multifactor-authenticatie (MFA) is verplicht voor alle superusers en beheeraccounts, ongeacht de locatie of het apparaat waarmee wordt ingelogd.
* Alle activiteiten die worden uitgevoerd met beheeraccounts en superuseraccounts worden gelogd.
* Service-accounts worden onderscheiden van beheeraccounts.
* Wachtwoorden van service-accounts worden regelmatig gewijzigd en automatisch geroteerd als dat mogelijk is.
* Periodieke review van alle superusers, beheeraccounts en service-accounts is verplicht. Minimaal elk kwartaal wordt gecontroleerd of toegang van deze accounts nog legitiem en noodzakelijk is.
* Gebruik van gedeelde beheeraccounts is verboden, tenzij technisch onvermijdelijk.
* Aanvragen voor beheeraccounts en superuserrechten verlopen via het <naam IAM-proces>, inclusief goedkeuring door leidinggevende.
* <Vul aan>.

# 4. Monitoring

## 4.1 Periodieke controle van toegangsrechten

***Toelichting***

* *Beschrijf wie verantwoordelijk is voor de periodieke controle van de koppeling tussen centrale rollen en applicatierollen.*
* *Beschrijf wie verantwoordelijk is voor de periodieke controle van alle extra toegangsrechten die zijn toegekend buiten de reguliere rollenstructuur.*
* De **systeemeigenaar** is verantwoordelijk voor het <bepaal frequentie> controleren of de juiste applicatierollen aan de juiste centrale rollen zijn gekoppeld.
* De **lijnmanagers** zijn verantwoordelijk voor het <bepaal frequentie> controleren van alle extra toegangsrechten die zijn toegekend buiten de reguliere rollenstructuur.

De verdere uitwerking van de periodieke controle van toegangsrechten staat in het proces logische toegang.

## 4.2 Rapportage

***Toelichting***

* *Het schoolbestuur kan het monitoren van en het rapporteren over de toepassing van het beleid delegeren. Bijvoorbeeld aan de IBP’er. Wanneer de IBP’er ook veel van de eerstelijnstaken uitvoert binnen dit beleid, is het aan te raden om deze taak niet te delegeren.*

<vul naam schoolbestuur in> heeft de verantwoordelijkheid om het IAM-beleid formeel goed te keuren en te monitoren of de organisatie het IAM-beleid toepast. Periodiek <bepaal de frequentie> wordt hierover gerapporteerd in <bepaal waar deze rapportage wordt vastgelegd.

## 4.3 Beleidsherziening

Het IBP-beleid wordt door <vul naam schoolbestuur in> eenmaal per <invullen herzieningstermijn> getoetst en indien nodig herzien. Bij een wijziging van het IBP-beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt mogelijk een beleidswijziging.