****

**IAM**

Security Nederland

**Versiebeheer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Datum** | **Auteur** | **Omschrijving** |
| 0.1 | Concept | 5-9-2023 | **Niels Dutij**  Ludo Cuijpers  Leo Jaarsma  Henk Links  Sebastiaan van Trigt | Basisdocument |
|  |  |  |  |  |

**Vastgesteld door Security Nederland:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| 1.0 |  |  | College van Bestuur |

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en MBO Raad geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.



Creative commons

MBO Raad 4.0 Nederland

(CC BY 4.0) **Copyright**

De gebruiker mag:

Het werk kopiëren, verspreiden en doorgeven

Remixen – afgeleide werken maken

Onder de volgende voorwaarde:

Naamsvermelding – De gebruiker dient bij het werk de naam van MBO Raad te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

Inhoudsopgave

[Beleid voor Identity acces management (IAM) 3](#_Toc144978233)

[**Inleiding** 3](#_Toc144978234)

[1.Uitgifte van beheer van identiteiten 3](#_Toc144978235)

[**We onderhouden één Identiteit en beheren deze ook.** 3](#_Toc144978236)

[**We onderhouden één account** 3](#_Toc144978237)

[**Context bepaalt autorisatie** 3](#_Toc144978238)

[**Need-to-know, need-to-use, time-to-know** 3](#_Toc144978239)

[**Functie-scheiding** 4](#_Toc144978240)

[**Uitgifte van rollen en rechten** 4](#_Toc144978241)

[2. Principes voor authenticatie 5](#_Toc144978242)

[**Proportionaliteit** 5](#_Toc144978243)

[**Beveiligde inlogprocedure en Multi-factorauthenticatie** 5](#_Toc144978244)

[**Wachtwoordbeheer** 6](#_Toc144978245)

[**Inrichten van de applicatie en het beheer van de applicatie** 7](#_Toc144978246)

[**Systeem-eigenaar** 7](#_Toc144978247)

[**Proces-eigenaren:** 7](#_Toc144978248)

[**Periodieke** **controle** 7](#_Toc144978249)

[3. Borging van het IAM Beleid 8](#_Toc144978250)

[**Omgaan met uitzonderingen** 8](#_Toc144978251)

[**Consolidatie** 8](#_Toc144978252)

[**Breaking glas procedure** 8](#_Toc144978253)

[1. Bijlage 1: Rollen en rechten 10](#_Toc144978254)

[**1.1.1** **Voorbeeld hbo instelling (rollen binnen Osiris)** 11](#_Toc144978255)

[2. Bijlage 2: Autorisatiematrix Osiris 13](#_Toc144978256)

**Beleid voor Identity acces management (IAM)**

**Inleiding**

Een goed proces rondom IAM is essentieel om zicht te houden op uitgegeven rollen en rechten, maar ook op de inrichting van systemen. Om te kunnen voldoen aan wet- en regelgeving is het cruciaal om een goed zicht op deze onderdelen te behouden.

**1.Uitgifte van beheer van identiteiten**

**We onderhouden één Identiteit en beheren deze ook.**

Iedere natuurlijke persoon (student, medewerker, andere betrokkenen) heeft één identiteit. Het HR-systeem (medewerkers) of de deelnemersregistratie (studenten en relaties) geldt als bronsysteem.

Het aangewezen bronsysteem van een identiteit geldt als bron voor de levenscyclus. Zodra de persoon niet meer actief is bij de onderwijsinstelling wordt zijn/haar identiteit gedeactiveerd (incl. alle autorisaties). De bewaartermijn van (gedeactiveerde) identiteiten, accounts en autorisaties wordt bepaald door de proces-eigenaar. Een bewaartermijn van drie maanden wordt vaak als passend gezien.

**We onderhouden één account**

Een medewerker en een student (identiteit) beschikt over één account voor onze ICT-infrastructuur. Een uitzondering wordt gemaakt voor test-, beheer- en service-accounts, die echter wel te herleiden zijn naar een natuurlijk persoon of specifiek systeem.

Accounts voor applicaties worden zoveel mogelijk geautomatiseerd aangemaakt en verwijderd. Voor applicaties geldt dat accounts direct gedeactiveerd worden wanneer de medewerker uit dienst treedt of als de student/andere betrokkene geen toegang meer nodig heeft.

Er worden geen ‘algemene’ accounts gebruikt, die niet gekoppeld zijn aan een persoon. Als er toch sprake is van een algemene account, dan is hiervan altijd een eigenaar die verantwoordelijk is voor het correcte gebruik.   
  
Een account wordt enkel toegekend aan medewerkers of andere personen met een contractuele relatie , zoals een arbeidsovereenkomst of een detacheringsovereenkomst. Voor studenten geldt dat zij een account krijgen, indien zij zijn ingeschreven bij de onderwijsinstelling. Er worden geen accounts toegekend aan externe partijen zonder contractuele relatie. Een leerplichtambtenaar of andere externe partij zal daarom geen account krijgen van de onderwijsinstelling.

**Context bepaalt autorisatie**

De context van een identiteit bepaalt in eerste instantie de autorisatie. Voorbeelden zijn iemands functie en organisatieonderdeel, op basis waarvan basale autorisaties (account uitgifte en autorisaties binnen applicaties) worden toegekend. Naarmate er meer eigenschappen bekend worden (voor strikt organisatorische doeleinden), wordt het verlenen en muteren van autorisaties verder verfijnd en geautomatiseerd.

**Need-to-know, need-to-use, time-to-know**

Personen krijgen alleen toegang tot functionaliteiten en informatie voor zover dit strikt noodzakelijk is voor het uitvoeren van de aan hen opgedragen werkzaamheden. In de praktijk mogen autorisaties geen belemmering vormen in het kunnen uitvoeren van een functie of procesrol, maar zijn ook geen vanzelfsprekendheid.

Personen krijgen niet langer dan strikt noodzakelijk toegang tot functionaliteiten en informatie voor het uitvoeren van de aan hen opgedragen werkzaamheden, in overeenstemming met hun rol. Autorisaties komen te vervallen bij het wijzigen van functie. Als dit niet automatisch kan, dan dient een kernsysteem hier een beheerproces voor in te richten.

Alle formele rollen worden vastgelegd in een autorisatie-matrix door de functioneel beheerder. In de praktijk is er een autorisatiematrix per applicatie waarin wordt vastgelegd wie (rol en/of context van de identiteit) wat mag (rol/autorisatie). De autorisatiestructuur van een kernsysteem sluit aan bij de goedgekeurde procesbeschrijvingen.

**Functie-scheiding**

Dit geldt zowel voor het beheer van de autorisaties als het gebruik ervan.

* De aanvrager van autorisaties en de uitgever ervan zijn verschillende functionarissen (vier ogen principe).
* De samenstelling van rollen/rechten combinaties en de toekenning van autorisaties is dusdanig dat er sprake is van passende functiescheiding voor de eindgebruiker. HRM dient een functie-scheiding conflictmatrix op te stellen om conflicterende functies te scheiden.
* Rollen en rechten dienen periodiek gecontroleerd te worden.

**Uitgifte van rollen en rechten**

Rollen en rechten worden enkel uitgegeven na aanvraag of goedkeuring door de leidinggevende. Dit proces wordt vastgelegd, bijvoorbeeld in het meldingensysteem van de onderwijsinstelling. De functioneel beheerder toetst of de aangevraagde rollen en rechten voldoen aan de vastgestelde autorisatiematrix van de applicatie en de beleidsuitgangspunten van dit IAM-beleid en de functie-scheiding conflictmatrix.

Daarnaast krijgen medewerkers tijdens hun loopbaan diverse rollen- en rechten toegewezen. Deze rollen en rechten van medewerkers dienen ieder half jaar gecontroleerd te worden op actualiteit. De leidinggevende is verantwoordelijk voor het controleren voor de uitgegeven rollen en rechten, de applicatie-eigenaar faciliteert het controleren van de rollen en rechten door bijvoorbeeld het genereren van overzichten van uitgegeven rollen en rechten. De applicatie-eigenaar is gerechtigd uitgegeven rollen in te trekken als rollen/rechten niet afdoende gecontroleerd worden door de leidinggevende.

**Super-Users en admin-accounts**  
Voor iedere applicatie is het noodzakelijk om super-users en admin-accounts aan te maken. Deze specifieke rollen hebben een grote hoeveelheid rechten in de applicatie om de werking van de applicatie te kunnen borgen.   
  
Voor supers-users en admin-accounts gelden de volgende extra eisen:

* Super-users en admin-accounts worden zoveel mogelijk beperkt, maar in iedere applicatie zijn er ten minste twee super-users/admins om de continuiteit te waarborgen.
* Iedere aanvraag of wijziging van een super-user/admin-account dient aangevraagd te worden via het meldingensysteem, waarbij de leidinggevende goedkeuring dient te geven.
* De aanvraag dient aanvullend ook goedgekeurd te worden door zowel een huidige super-user/admin van de desbetreffende applicatie en door de systeem-eigenaar.
* De speciale toegangsrechten van ieder systeem en elke toepassing (inclusief beheeraccounts van netwerkapparatuur etc.) en de gebruikers aan wie ze moeten worden toegewezen moeten worden geïdentificeerd en geregistreerd.
* Speciale toegangsrechten worden alleen op basis van “need-to-know” en “need-to-use” toegekend.
* Speciale rechten worden nooit toegekend aan een standaard gebruikersaccount voor dagelijkse werkzaamheden (mail, tekstverwerking, spreadsheet, etc.).
* Activiteiten van accounts met speciale rechten worden gelogd.

**2. Principes voor authenticatie**

**Proportionaliteit**

Hoe gevoeliger de gegevens zijn hoe meer we ons ervan willen overtuigen dat de persoon werkelijk is wie hij zegt dat hij is. Voor gegevens met een hoge vertrouwelijkheid (bijvoorbeeld bijzondere persoonsgegevens) wordt altijd gebruik gemaakt van multi-factorauthenticatie.

Voor applicaties in het huidige applicatielandschap die geen meervoudige authenticatie ondersteunen maar dat wel nodig hebben wordt een alternatief gezocht of er worden aanvullende maatregelen getroffen om een gewenst beveiligingsniveau te bereiken.  
  
**Classificatie**  
Onze instelling hanteert het ROSA classificatiemodel en de uitkomsten van de classificatie worden openomen in het dataregister. Het ROSA Classificatiemodel bevat tevens de maatregelen die passen bij de gehanteerde classificatie. Proces-eigenaren stellen de classificatie vast voor de gegevens die vallen binnen hun proces.  
  
Onze instelling classificeert de data in het dataregister, waarbij de uitkomsten worden gebruikt voor de beoordeling van applicaties, het toekennen van rollen en rechten en het vaststellen van de autorisatiematrix.   
  
Bij een Hoge Vertrouwelijkheid van gegevens (hiervan is altijd sprake bij het gebruik van BSN, Zorg- en begeleidingsinformatie en beeldmateriaal) geldt aanvullend op het ROSA Classificatiemodel het volgende:

* Multi-factorauthenticatie dient te worden afgedwongen voor alle gebruikers.
* Documenten of andersoortige gegevens met een vertrouwelijkheid Hoog zoveel mogelijk in de applicatie te blijven. Bij uitwisseling van gegevens geldt dat hiervoor SURF Filesender gebruikt dient te worden of een andere beveiligde mail-oplossing.

**Gebruiker is de bron**Het wachtwoord is verbonden aan de gebruiker zelf. De instelling slaat deze alleen op in het inlogsysteem en deelt deze nooit met derde partijen.

**Single sign-on: 1x inloggen**Personen loggen niet apart in op onderdelen van de ICT-infrastructuur van de onderwijsinstelling, maar maken zoveel mogelijk gebruik van signle sign-on. Indien dit voor een specifieke applicatie niet mogelijk blijkt, dan dient hierover afstemming plaats te vinden met de systeem-eigenaar en de proces-eigenaar.  
  
Indien er geen gebruik wordt gemaakt van de SSO, dient de leverancier in ieder geval een wachtwoord-beleid te ondersteunen dat passend is. Het NCSC (<https://www.ncsc.nl/onderwerpen/authenticatie>) is hiervoor het uitgangspunt. Gebruikers dienen een ander wachtwoord te gebruiken dan hun standaard-wachtwoord bij het instellingsaccount.

**Beheer van de ICT infrastructuur**Authenticatie voor het beheer en services in de ICT infrastructuur vereist strikte beveiligingsmaatregelen. Deze worden continue geactualiseerd conform de standaarden voor beveiliging van de ICT infrastructuur.

**Beveiligde inlogprocedure en Multi-factorauthenticatie**

Alle netwerken en systemen van de onderwijsinstelling zijn slechts toegankelijk via een beveiligde inlogprocedure. Dit betekent dat gebruikersnaam en wachtwoord altijd via een beveiligde verbinding worden verstuurd, zodat onderscheppen door middel van “sniffing” erg moeilijk dan wel zelfs onmogelijk is.

Daarnaast geldt de verplichting om MFA te gebruiken bij systemen die persoonsgegevens verwerken met de vertrouwelijkheid classificatie Hoog.

De inlogprocedure omvat de volgende maatregelen:

* Een algemene waarschuwing tonen dat de computer alleen toegankelijk is voor bevoegde gebruikers.
* Het tonen van de laatste ingelogde gebruikersnaam is niet toegestaan.
* Tijdens de inlogprocedure geen hulpboodschappen weergeven waarmee onbevoegde gebruikers hun doel kunnen bereiken.
* De inloginformatie pas na invoer van alle gegevens valideren. Indien zich een fout voor- doet, behoort het systeem niet aan te geven welk deel van de gegevens juist of onjuist is.
* Bescherming bieden tegen inlogpogingen die met grove middelen worden uitgevoerd (Brute Force Attack).
* Niet-succesvolle en succesvolle inlogpogingen worden geregistreerd in een logbestand (NB: Niet de wachtwoorden), bewaartermijn 6 maanden.
* Bij een poging tot of een succesvolle schending van de inlogbeheersmaatregelen wordt een informatiebeveiligingsincident geïnitieerd.
* Een wachtwoord dat wordt ingevoerd wordt niet leesbaar weergegeven.
* Inactieve sessies van toepassingen worden na een bepaalde tijd van inactiviteit van de gebruiker beëindigd.

**Wachtwoordbeheer**

Bij het wachtwoord beheer dienen onderstaande eisen te worden gehanteerd. De eisen aan een dergelijk systeem worden ook gesteld aan individuele systemen en toepassingen, voor zover er geen gebruik wordt gemaakt van SSO.

* De keuze voor sterke wachtwoorden wordt afgedwongen, de gewenste complexiteit wordt ingesteld.
* Gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen binnen de gestelde complexiteitseisen.
* Gebruikers worden gedwongen hun initiële wachtwoord bij het eerste inloggen te wijzigen.
* Periodieke wijziging van het wachtwoord wordt afgedwongen.
* Voorkomt dat wachtwoorden opnieuw worden gebruikt door een wachtwoordhistorie bij te houden.
* Wachtwoorden worden niet leesbaar op het scherm getoond als ze worden ingevoerd.
* Wachtwoordbestanden worden apart van systeemgegevens van toepassingen opgeslagen.
* Wachtwoorden worden versleuteld opgeslagen en verstuurd.

Alle applicaties en toepassingen binnen de onderwijsinstelling worden zodanig ingericht dat, voor zover technisch mogelijk, aan de bovenstaande eisen wordt voldaan.

**Inrichten van de applicatie en het beheer van de applicatie**

Tijdens het inrichten van het systeem wordt bepaald welke onderdelen geconfigureerd moeten worden. De volgende rollen zijn hiervan van belang:

**Systeem-eigenaar**

De systeemeigenaar is eigenaar van alle componenten in het ICT netwerk. Het functioneel beheer en de scholing van de medewerkers in de applicaties valt niet onder de verantwoording van de systeemeigenaar. Het functioneel beheer valt onder de applicatie-eigenaar van de desbetreffende applicatie. De systeem-eigenaar faciliteert het technische proces, maar is niet verantwoordelijk voor de inhoud of het beheer van een applicatie.

**Applicatie-eigenaar**  
De applicatie-eigenaar is de eigenaar van de desbetreffende applicatie die hem/haar is toegewezen. De applicatie-eigenaar is verantwoordelijk voor:

* Inrichten van de applicatie conform de eisen van het IBP-beleid (waaronder de eis van inrichting op basis van need-to-know in ieder geval valt);
* Het vaststellen van een autorisatiematrix en een passende toegangsverleningsprocedure;
* In samenspraak met de proces-eigenaar de rollen en rechten van medewerkers vaststelt;
* Het toezien op leveranciersmanagement, waaronder het jaarlijks beoordelen van de verwerkersovereenkomst en beveiligingsaspecten, ondersteund door de afdeling Inkoop;
* Het periodiek laten uitvoeren van een data protection impact assessment, indien dit noodzakelijk is conform wetgeving;
* Het , in samenspraak met de proces-eigenaar, tijdig laten verwijderen van persoonsgegevens conform het Documentair Structuurplan van de MBO-raad.

**Proces-eigenaren:**

De proces-eigenaren worden door het College van Bestuur benoemd. De proceseigenaar zal in overleg met de applicatie-eigenaren de processen laten inrichten, doorgaans met behulp van applicaties waarvan hij de functionaliteit mee heeft bepaald.

De proces-eigenaar is daardoor ook verantwoordelijk voor bijvoorbeeld de inrichting van het systeem op basis van de principes uit dit beleid. Dit betekent bijvoorbeeld concreet dat de proces-eigenaar verantwoordelijk is voor het vaststellen van rollen en rechten en de toetsing op need-to-know en dataminimalisatie binnen zijn proces en de bijbehorende applicaties.

**Functioneel beheerder:**  
Bundelt de rechten in een systeem tot een systeemrol en volgt procedures conform het inrichting- of beheerdocument voor die applicatie. De rechten op functionaliteiten en specifieke data worden vastgelegd in de autorisatiematrix. Op verzoek van leidinggevenden worden deze rollen aan specifieke medewerkers toegekend.  
De functioneel beheerder van een applicatie zorgt voor actuele autorisatiematrix, waarin is opgenomen welke rollen en rechten er zijn binnen de desbetreffende applicatie.

**Periodieke** **controle**

De leidinggevende is verantwoordelijk voor de uitgifte van rollen en rechten van haar medewerkers. De leidinggevende dient periodiek (eens per zes maanden) te controleren of de uitgegeven rollen/rechten nog actueel zijn, de systeem-eigenaar faciliteert hiervoor een proces.

**3. Borging van het IAM Beleid**

**Omgaan met uitzonderingen**

Applicatie-eigenaren moeten expliciet toestemming verlenen bij ondergenoemde autorisatie-aanvragen:

* Toekennen van rechten die breder zijn dan behorende bij de procesrol of functiebeschrijving.
* Toekennen van rechten die afwijken van het ontwerp van het proces of de applicatie.
* Aanbrengen van mutaties in de autorisatiematrices, in zoverre deze niet door de leverancier aangepast worden bij nieuwe versies van de applicatie.

De functioneel beheerder:

* Contacteert de applicatie-eigenaar.
* Legt deze goed- of afkeuring vast (voor controle en verantwoording).
* Voert de autorisatie door in de applicatie (voor zover dit niet geautomatiseerd plaatsvindt).

**Consolidatie**

Autorisaties zonder verantwoording (verleend buiten de autorisatie matrices en zonder fiat van leidinggevende) worden ingetrokken.

**Breaking glas procedure**

Wachtwoorden van super-Users en admin-accounts kunnen op 2 manieren worden opgeslagen en in geval van nood gebruikt worden:

1. Verzegelde enveloppen met wachtwoorden liggen in een kluis en zijn alleen door een leidinggevende te openen.
2. Leidinggevende1 heeft een encrypte USB stick in zijn bezit maar het wachtwoord is niet in zijn/haar bezit. Leidinggevende2 kan in geval van nood dit wachtwoord aan hem/haar doorgeven waarna leidinggevende1 de wachtwoorden kan doorgeven aan de vervanger.
3. **Bijlage 1: Rollen en rechten**

**Inleiding**

Begin januari 2020 (red. HAS green academy) werd een nieuw autorisatiebeleid en autorisatiemodel voor Osiris geïntroduceerd, met de volgende doelstellingen:

* Iedere medewerker kan in Osiris alleen doen wat nodig en toegestaan is vanuit zijn of haar functie en/of taken binnen de mbo instelling.
* Iedere medewerker heeft alleen toegang tot die gegevens in Osiris die relevant, nodig en toegestaan zijn (mede gelet op wet‐ & regelgeving, bijvoorbeeld AVG) voor zijn of haar functie en/of taken binnen de mbo instelling.
* De autorisaties worden opgeschoond. De meeste oude rollen worden inactief gezet.
* De rollen worden toegewezen aan bepaalde personen, zoals privacygevoelig werk (bv Zorg). Hiervoor zijn eisen en beperkingen opgesteld, waarop wordt gecontroleerd bij toekenning van deze rollen.
* De nieuwe autorisatierollen sluiten aan op de werkprocessen van de hbo instelling.

**Introductie tot het autorisatiemodel Osiris**

Het autorisatiemodel is als volgt opgebouwd:

Autorisatierollen:

* Functierol, bv. docent: voor iedere functie binnen de hbo instelling worden uniforme autorisatierechten gedefinieerd, die voor iedere gebruiker met de desbetreffende functie nodig en toegestaan zijn.
* Taakrol, bv. Studieadviseur: soms hebben functionarissen aanvullende taken. Per taakrol zijn aanvullende autorisatierechten nodig en toegestaan. Deze worden aan iedere gebruiker met de desbetreffende taakrol toegekend.
* Als een gebruiker meerdere functie‐ en/of taakrollen krijgt toegekend, worden de autorisatierechten ‘gestapeld’.
* Autorisatie gebeurt op het niveau van organisatie‐eenheid waarvoor de medewerker werkzaam is. (locatie, opleiding, team)

Als een medewerker meerdere autorisatierollen en/of meerdere organisatie‐eenheden toegekend krijgt, worden deze in Osiris gestapeld:

* De rechten van alle autorisatierollen te samen worden aan de medewerker toegekend.

Bij het toekennen van rollen aan medewerkers kunnen soms eisen en/of beperkingen gelden:

* Goedkeuringseis: de toekenning van een autorisatierol na goedkeuring door een leidinggevende, bijv. leidinggevende of HR.
* Beperking, bv. maximering van het aantal medewerkers met de rol per organisatie‐eenheid.
* Deskundigheidseis: toekenning van een autorisatierol pas nadat bv. een training is afgerond.
  + 1. **Voorbeeld hbo instelling (rollen binnen Osiris)**

**Uitwerking/toelichting autorisaties en AVG**

OSIRIS maakt gebruik van standaard profielen. Er zijn keuzes gemaakt welke activiteiten (rollen en rechten) bij welk profiel horen in overleg met afgevaardigden uit de opleidingen. Het is niet wenselijk om persoonlijke profielen te maken met een eigen palet aan rollen en rechten door de hoge beheerslasten en foutgevoeligheid die dit met zich meebrengt (AVG, veiligheid resultaten etc.). Persoonlijke profielen zijn ook ongewenst met het oog op het feit dat de hbo instelling processen wil harmoniseren. Volgens AVG mag je datgene zien wat je voor je werk nodig hebt.

**Uitgangspunten profielen**

* Iedere docent die een student in een les heeft zou toegang moeten hebben tot diens totale cijferlijst, zodat er, wanneer nodig, begeleiding op maat kan worden gegeven. Cijfers en studiepunten zijn iets anders dan andere persoonlijke gegevens, omdat ze gaan over de directe relatie tussen de student en de opleiding, waar de desbetreffende docent ook deel van uitmaakt.
* De hbo instelling heeft meerdere soorten coaches: De coach die de student vanaf de aanvang van de opleiding persoonlijk coacht, de stagecoach, een projectbegeleider, de inhoudelijke coach bij een specialiserende minor, de project(bege)leider in een BO. Al deze medewerkers hebben inzicht nodig in studieresultaten en moeten kunnen opzoeken hoe een student presteerde bij eerdere verslagen, schriftelijke toetsen, en/of projecten en als daar aanleiding toe is kan de docent ook bij beoordelingsformulieren om de onderbouwing van een bepaald (opvallend) cijfer te achterhalen.
* Een modulecoördinator moet inschattingen kunnen maken in hoeveel studenten er in zijn module terecht komen, zodat die daarop kan plannen. Met name bij een grote opleiding maakt dit nogal uit. Daarbij moeten zij in bepaalde gevallen kunnen inschatten of iemand toelaatbaar is tot de module (latere jaren, al vanaf TB2, want als iemand in TB1 niet voldoende studiepunten haalt komt die niet in het 2e jaar). Jaarcoördinatoren (die hebben we bij TB, maar niet bij alle opleidingen, dus dat is geen gedefinieerde rol) moeten hetzelfde kunnen doen in deze situatie.
* Een opleiding zou in OSIRIS niet zo gesplitst moeten worden in modules Het leren en begeleiden van een student is een continu proces dat door vele collega’s in samenwerking met elkaar moet gebeuren. Alle docenten moeten zich een beeld kunnen vormen van de groep als geheel (mijn toets is slecht gemaakt, hoe zat dat hiervoor), en van een individuele student (deze student kwam op mij zo en zo over in mijn projectgroep, hoe heeft ie het hiervoor gedaan?). En dit wordt nog belangrijker met het flexibel en adaptief onderwijs. Je hebt het echt nodig om een totaalplaatje van de prestaties een student te vormen, en daar zijn de beoordelingen een onderdeel van.

**Voorbeelden van aanvullende verzoeken in het kader van de autorisatie:**

1. Modulecoördinator: Inzicht in alle resultaten van alle studenten, inclusief die van andere modules. Inzicht in de historie van resultaten van de module, ook als er een andere modulecoördinator was.
2. Stagecoördinator: Inzicht in resultaten van alle studenten voorgaande jaren.
3. Secretariaat: inzicht in de contactgegevens van de studenten van andere opleidingen binnen het cluster.
4. Cluster “Innovatie”: inzicht in de resultaten, contactgegevens en nieuwe aanmeldingen van alle studenten van alle opleidingen.
5. Coach: inzicht in de contactgegevens van coachstudenten.
6. Manager (niet zelf gevraagd, maar aanvraag via secretariaat): inzicht in alle resultaten van de opleiding.
7. Extra rol receptie: er is vraag naar een rol waarbij de contactgegevens van studenten kunnen worden ingezien en fotolijsten kunnen worden gegenereerd.

**Profielen**

De indeling van de profielen.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Profiel** |  | **Inzage van studenten** | | | | | | **Genereren lijsten** | | | **Aanpassen** | |
|  | **Naam en opleiding** | **Voertaal** | **NAW en telefoonnr.**  **(M.3.1.1)** | **Geboortedatum**  **Plaats**  **Nationaliteit**  **(M.3.1.1)** | **Info eerdere onderwijs instelling**  **(M.3.1.1)** | **Resultaten**  **(M.3.1.7)** | **Voorzieningen** | **Foto-**  **lijst**  **groep**  **klas**  **(M.3.0.1)** | **Resultaten-lijst** | **Rapportages** | **Resultaten**  **(M6.2)** | **Cursus-informatie** |
| **Secretariaat** | Ja  de hbo instelling | NL of ENG | Ja  Opleiding | Nee | Nee | Ja  Opleiding | Nee | Ja | Nee | Nee | Nee | Nee |
| **Studieadviseur** | Ja  de hbo instelling | NL of ENG | Ja  Opleiding | Ja | Ja | Ja  Opleiding | Ja | Ja | Ja | Ja | Nee | Nee |
| **Studie plus** | Ja  de hbo instelling | NL of ENG | Alleen naam en geslacht en telefoonnr. | Nee | Ja | Ja  Opleidingen | Ja | Nee | Nee | Nee | Nee | Nee |
| **Coach** | Ja  de hbo instelling | NL of ENG | Ja (geen adresgegevens) | Nee | Ja | Ja  Coach-student | Nee | Ja  Coach-student | Ja  Coach-student | Nee | Nee | Nee |
| **Docent** | Ja  de hbo instelling | NL of ENG | Alleen naam en geslacht | Nee | Nee | Ja  Module | Nee | Ja | Nee | Nee | Nee | Nee |
| **Examinator** | Ja  de hbo instelling | NL of ENG | Alleen naam en geslacht | Nee | Nee | Ja  Module | Nee | Ja | Nee | Nee | Ja | Nee |
| **Module-coördinator** | Ja  de hbo instelling | NL of ENG | Alleen naam en geslacht | Nee | Nee | Ja  Module | Nee | Ja | Ja  Module | Nee | Ja | Ja |
| **Examencommissie** | Ja  de hbo instelling | NL of ENG | Alleen naam | Nee | Nee | Ja  Opleiding | Nee | Nee | Ja  Opleiding | Nee | Vrijstelling | Nee |
| **Cursusinvoer** | Ja  de hbo instelling | NL of ENG | Nee | Nee | Nee | Nee | Nee | Nee | Nee | Nee | Nee | Ja |
| **International Office** | Ja  de hbo instelling | NL of ENG | Ja | Ja | Ja | Ja | Nee | Ja | Ja | Ja | Nee | Nee |
| **Management** | Ja  de hbo instelling | NL of ENG | Nee | Nee | Nee | Nee | Nee | Nee | Nee | Nee | Nee | Nee |
| **Financieel** | Ja  de hbo instelling | NL of ENG | Ja | Ja | Nee | Nee | Nee | Nee | Nee | Ja | Nee | Nee |
| **Studentzaken** | Ja  de hbo instelling | NL of ENG | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja |
| **Beheerder** | Ja  de hbo instelling | NL of ENG | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja |

Het profiel Receptie is nog niet uitgewerkt.

1. **Bijlage 2: Autorisatiematrix Osiris**

Naam leidinggevende: <naam1>

Organisatorische eenheid: <aanduiding1)

Datum: 22 juni 2022

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Naam  medewerker | Personeelsnummer | Secretariaat | Studieadviseur | Studie plus | Coach | Docent | Examinator | Module-coördinator | Examencommissie | Cursusinvoer | International Office | Management | Financieel | Studentzaken | Beheerder | Uitzondringen |
| Naam1 | P1 | **X** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Naam2 | P2 |  |  |  |  |  |  |  |  |  |  | **X** |  |  |  |  |
| Naam3 | P3 |  |  |  |  | **X** |  |  |  |  |  |  |  |  |  |  |
| Naam4 | P4 |  |  |  |  | X |  | **X** | **X** |  |  |  |  |  |  |  |
| Naam5 | P5 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| Naam6 | P6 |  |  |  |  | X |  |  | **X** |  |  |  |  |  |  |  |
| Naam7 | P7 |  |  |  |  | X |  |  | **X** | **X** | **X** |  |  |  |  |  |

Naam leidinggevende: <naam1>

Organisatorische eenheid: <aanduiding1)

Naam functioneel beheerder: <beheerder1)

Datum: 7 september 2022

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Naam  medewerker | Personeelsnummer | Secretariaat | Studieadviseur | Studie plus | Coach | Docent | Examinator | Module-coördinator | Examencommissie | Cursusinvoer | International Office | Management | Financieel | Studentzaken | Beheerder | Uitzondringen |
| Naam1 | P1 | **X** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Naam2 | P2 |  |  |  |  |  |  |  |  |  |  | **X** |  |  |  |  |
| Naam3 | P3 |  |  |  |  | **X** | **X** |  |  |  |  |  |  |  |  |  |
| Naam4 | P4 |  |  |  |  | X |  | **X** | **X** |  |  |  |  |  |  |  |
| Naam5 | P5 |  |  |  |  | X |  |  |  |  |  |  |  |  |  |  |
| Naam6 | P6 |  |  |  |  | X |  |  | **X** |  | **X** |  |  |  |  |  |
| Naam7 | P7 |  |  |  |  | X |  |  | **X** | **X** | **X** |  |  |  |  |  |