Zuyd Security Beleid – Identity & Access Management

Versie 1.2

Vastgesteld door het CvB op 21-10-2025

Inhoudsopgave

1. Documentenbeheer 3
2. Managementsamenvatting 4
3. Zuyd Security Beleid – Identity & Access Management 5
3.1. Inleiding 5
3.2. Relatie tot SURF CMM Toetsingskader 6
3.3. Relatie tot overige documenten 6
3.4. Doel 6
3.5. Scope 6
3.6. Beleid 7

1. Documentenbeheer

Revisiehistorie

Revisiedatum	Samenvatting veranderingen	Door	Versie
10-07-2023	Draft versie	D. Heynen	0.1
25-09-2023	Verdere uitwerking/verdieping	D. Heynen	0.4
06-10-2023	Review (C)ISO's	D. Heynen	0.5
27-11-2023	Verwerking review opmerkingen IM, FB&ICT, Juridische afdeling, FG & PO.	D. Heynen	0.96
16-01-2024	Identity & Access Management beleid vastgesteld door CvB.	R. Sterken	1.0
09-09-2025	Minor Update, template Zuyd, url koppelingen, tekstuele aanpassing.	D. Heynen	1.1
21-10-2025	Vastgesteld door CvB	R. Sterken	1.2

Documentatie

Er is gebruik gemaakt van de onderstaande informatie

Naam	Auteur	Status
Informatiebeveiligingsbeleid Zuyd Hogeschool	CISO Zuyd Hogeschool	Definitief
Normenkader Informatiebeveiliging versie 2.0	SURF	Definitief
SURF Security Baseline voor onderwijs en onderzoek	SURF	Definitief
Baseline Informatiebeveiliging Zuyd Hogeschool	CISO Zuyd Hogeschool	Definitief
Cyberveilig woordenboek	Cyberveilig Nederland	Definitief

Jaarlijkse vaststelling

Dit document is vastgesteld door:

Naam	Uitgiftedatum	Versie
CvB	21 oktober 2025	1.2

2. Managementsamenvatting

Identity & Access management is een belangrijk onderdeel van informatiebeveiliging binnen Zuyd en speelt een essentiële rol bij het beschermen van Zuyd ICT-Infrastructuur tegen ongeautoriseerde toegang. Het doel van het Identity & Access management beleid is risico's te beperken door het beheer van accounts (gebruikersidentiteiten) en toegangsrechten van Zuyd te automatiseren en te stroomlijnen, en daarbij zorg te dragen voor correcte authenticatie en autorisatie van gebruikers en beheerders met als doel ongeautoriseerde toegang te voorkomen.

In grote lijn betekent dit bij het gebruik van de Zuyd ICT-Infrastructuur voor Zuyd medewerkers (waaronder extern/inhuur) en studenten het volgende:

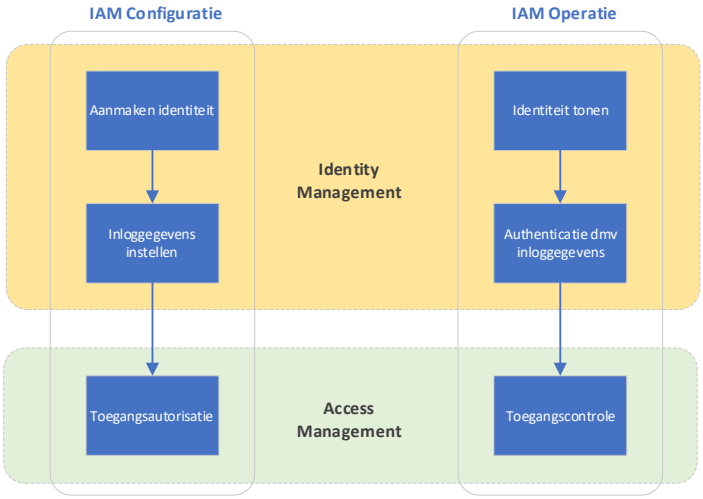
- We kennen beheer- en gebruikersaccounts;
- Gebruikersaccounts volgen een start-mutatie-stop proces vanuit het HR systeem of het studentvolgsysteem;
- Elke beheerder heeft gescheiden accounts voor beheer en kantoorwerkzaamheden. Zij mogen geen kantoorwerkzaamheden via het beheeraccount uitvoeren
- Beheeraccounts worden buiten het start-mutatie-stop proces en het studentvolgsysteem om aangemaakt;
- Aan het gebruik van accounts worden veiligheidseisen gesteld, denk hierbij aan phishing bestendige MFA;
- Gebruikersaccounts voor medewerkers worden na uitdiensttreding binnen 1 dag disabled en voor 120 dagen behouden;
- Gebruikersaccounts voor studenten blijven na uitschrijving opleiding 30 dagen toegankelijk en worden aansluitend voor 90 dagen behouden;
- Toegang wordt door de systeemeigenaar verleend op basis van een autorisatiematrix, hierin staan toegangsrechten van zowel gebruikers op basis van functie/rol als van (functioneel) beheerders;
- Er is een toestemmingsprocedure voor de systeemeigenaar die toegangsrechten toekent.;
- Indien de functie/rol die een medewerker toegewezen krijgt niet eenduidig van de functietitel is af te leiden, worden extra rechten toegekend, rechten ontnomen en onderbouwd vastgelegd op basis van het 4-ogen principe: de teamleider/opleidingsmanager vraagt de rechten aan en de functioneel beheerder kent deze daadwerkelijk toe;
- De systeemeigenaar doet jaarlijks een review van de aan gebruikers en (functioneel) beheerders verstrekte autorisaties en legt dit vast.

3. Zuyd Security Beleid – Identity & Access Management

3.1. Inleiding

Identity & Access management (IAM) is een belangrijk onderdeel van informatiebeveiliging binnen Zuyd en speelt een essentiële rol bij het beschermen van Zuyd ICT-Infrastructuur tegen ongeautoriseerde toegang. Hierbij gaat het niet over de fysieke toegangscontrole van Zuyd.

IAM (zie Figuur 1) helpt te beschermen tegen diefstal, corruptie of exfiltratie van gegevens door ervoor te zorgen dat alleen Zuyd gebruikers van wie de identiteit is geverifieerd, toegang hebben tot bepaalde informatie. IAM houdt vertrouwelijke informatie zoals studentgegevens, persoonlijk identificeerbare informatie en intellectueel eigendom weg van ongeautoriseerde toegang.



Figuur 1: Identity & Access Management

Het IAM-beleid beschrijft:

- Welke vormen van **authenticatie**[1] en **autorisatie**[2] worden toegepast.
- Hoe identiteiten van gebruikers worden gecontroleerd (Identity Management).
- Welke autorisatieregels bepalen wie toegang heeft tot welke systemen (Access Management).
- Hoe systemen worden gecontroleerd op ongeautoriseerde toegang.
- Hoe vaak toegangscontrolemaatregelen worden geëvalueerd.
- Hoe wordt vastgesteld of toegangscontrole nog effectief en passend is.
- Hoe gebruikers worden getraind in het gebruik van toegangscontrole.
- Hoe gebruikers leren over risico's van ongeautoriseerde toegang.
- Welke maatregelen worden genomen om ongeautoriseerde toegang te voorkomen.

[1] Authenticatie is het proces waarbij wordt gecontroleerd of een gebruiker, computer of applicatie daadwerkelijk is wie hij beweert te zijn.
[2] Autorisatie is het proces van het verlenen van toestemming aan een gebruiker om bepaalde acties uit te voeren of toegang te krijgen tot bepaalde bronnen, op basis van de identiteit van de gebruiker en de toegangsrechten die aan die identiteit zijn gekoppeld.

3.2. Relatie tot SURF CMM Toetsingskader

Dit beleid is gekoppeld aan de uitgangspunten in het SURF Audit Toetsingskader[1]. SURF schrijft: "De meest geaccepteerde internationale standaard op het gebied van informatiebeveiliging is ISO27002:2013. Wij hebben ons normenkader hierop gebaseerd". Uit deze ISO-norm zijn de onderdelen geselecteerd die een onderwijsinstelling in ieder geval geregeld moet hebben.

Het beleid heeft sterke raakvlakken met meerdere beheersdoelstellingen uit dit kader (te weten: NBA ID: ID.01, ID.02, ID.03, ID.04, ID.05, HR.04, OR.02, SM.02, SM.03 en SM.04) maar dient met name als een uitwerking van de beheersdoelstellingen NBA ID: ID.01, ID.02, ID.03, ID.04 en ID.05 in het domein ***Identity & Access Management***.

3.3. Relatie tot overige documenten

Naast dit beleidsdocument zijn de volgende stukken relevant

- Informatiebeveiligingsbeleid Zuyd (IBB)
  - Het document dat het informatiebeveiligingsbeleid van Zuyd beschrijft.
- Baseline Informatiebeveiliging Zuyd
  - Het document dat het informatiebeveiligingsbeleid van Zuyd beschrijft.
- CIS Controls Account and Credential Management Policy
  - Het document van CIS dat CIS Controls omtrent IAM beschrijft.
- Privacybeleid Zuyd Hogeschool
  - Het document dat het privacybeleid van Zuyd beschrijft.

3.4. Doel

Het doel van het Identity & Access Management beleid is het automatiseren en overzichtelijk organiseren van gebruikersaccounts en toegangsrechten binnen Zuyd. Hierbij wordt zeker gesteld dat gebruikers correct worden geauthentiseerd (controle identiteit) en geautoriseerd (toegang verlenen), zodat ongeautoriseerde toegang tot systemen en informatie wordt voorkomen.

Dit betekent concreet dat gebruikers enkel de toegangsrechten krijgen die zij nodig hebben. Dit geldt gedurende de hele levenscyclus van een account (start, mutatie, stop). Hiermee worden risico's voor de integriteit en vertrouwelijkheid van informatie beperkt.

3.5. Scope

De beleidsuitgangspunten in dit document hebben betrekking op de geauthentiseerde en geautoriseerde toegang tot de Zuyd ICT-Infrastructuur. De toegang tot Zuyd ICT-infrastructuren verloopt via gebruikersaccounts, beheeraccounts, serviceaccounts en standaardaccounts.

Het betreft daarbij de volgende account types:

- Gebruikersaccounts zijn accounts met de benodigde standaard rechten voor Zuyd medewerkers en studenten die worden gebruikt om hun dagelijkse werkzaamheden uit te voeren;
- Beheeraccounts, ook wel superuser-, privileged- of root-accounts genoemd) met uitgebreide rechten, bedoeld voor systeem;
- Serviceaccounts zijn accounts die door een applicatiesoftware of -service wordt gebruikt om te communiceren met andere applicaties of het besturingssysteem;
- Standaardaccounts die vooraf geïnstalleerd worden geleverd op systemen of software. Omdat gebruikersnamen en wachtwoorden hiervan algemeen bekend kunnen zijn, vormen ze een potentieel beveiligingsrisico (bijvoorbeeld achterdeuren).

3.6. Beleid

Bij het verlenen van toegang (authenticatie + autorisatie) aan gebruikers tot de Zuyd ICT-Infrastructuur dienen buiten de richtlijnen zoals vastgelegd in het document Baseline Informatiebeveiliging ook de volgende richtlijnen met betrekking tot Identity & Access management te worden toegepast:

1. Voor logische toegang tot de Zuyd ICT-Infrastructuur wordt gebruik gemaakt van identity & access management voor alle gebruikers (medewerkers/studenten/beheerders).
2. Elke gebruiker krijgt zijn eigen unieke gebruikersaccount (username en wachtwoord).
3. Er zijn aparte accounts voor reguliere kantoorwerkzaamheden en beheeractiviteiten.
4. Gebruikersaccounts volgen een start-mutatie-stop proces vanuit het HR systeem of het studentvolgsysteem.
5. Beheeraccounts worden buiten het start-mutatie-stop proces om aangemaakt.
6. Gebruikersaccounts worden aangemaakt en beheerd door FB-ICT in een centraal bronsysteem (IAM).
7. Alle acties die met een verstrekt account worden uitgevoerd vallen onder de verantwoordelijkheid van diegene aan wie het account verstrekt is.
8. De volgende technische maatregelen dienen ingericht te zijn op de systemen (dat geldt zowel voor Zuyd ICT-Infrastructuur als SaaS oplossingen) die worden gebruikt door Zuyd:

i. Identity Management (Accounts):

a) Voor alle accounts geldt dat wanneer dit kan deze ingericht zijn met phishing bestendige MFA.
b) Initiële wachtwoorden worden geautomatiseerd gegenereerd en zijn uniek per account.
c) Wachtwoorden worden altijd versleuteld opgeslagen met behulp van een coderingsalgoritme dat ervoor zorgt dat het wachtwoord zelf niet opnieuw kan worden gegenereerd op basis van het opgeslagen gecodeerde wachtwoord.
d) Complexe wachtwoorden zijn verplicht:
    i. een combinatie van drie van de volgende vier soorten karakters => cijfers, hoofd- en kleine letters en speciale tekens;
    ii. of het combineren van woorden of gezegden in een willekeurige mix.
e) Wachtwoorden voor gebruikersaccounts die zijn gemaakt voor gebruik met MFA authenticatie moeten minimaal 8 tekens lang zijn, voor overige accounts minimaal 15 tekens lang.
f) Wachtwoorden die zijn gemaakt voor gebruik zonder MFA authenticatie moeten minimaal 15 tekens lang zijn.
g) Wachtwoorden moeten minimaal jaarlijks vervangen worden, tenzij MFA gebruikt is.
h) In het geval dat een account / wachtwoord combinatie niet geldig is, wordt een bericht gegenereerd dat de combinatie niet geldig is. Er wordt niet aangegeven of het account, het wachtwoord of beide onbekend zijn voor het systeem.
i) Er is een selfservice portal voor gebruikersaccounts om wachtwoorden, te herstellen en resetten.
j) Indien een gebruiker een MFA reset wenst, dient deze zich in persoon of via controle op stand te melden bij de servicedesk en zich daar te identificeren.
k) Er kan niet rechtstreeks ingelogd worden op de applicaties waarvoor accounts geautoriseerd zijn. De authenticatie verloopt altijd via Surfconext of Entra ID (uitzondering zijn lokale accounts voor noodsituaties).
l) Accounts van gebruikers op lang buitengewoon verlof, zoals bekend bij HR, worden disabled.
m) Accounts/wachtwoorden zijn strikt persoonlijk en mogen niet worden gedeeld of geopenbaard. Alle acties die met een verstrekt account worden uitgevoerd vallen onder de verantwoordelijkheid van diegene aan wie het account verstrekt is.

n) Gebruikersaccount:
    i. Wachtwoorden voor persoonlijke accounts worden alleen door account eigenaar gekozen.
    ii. Alle standaard nieuw ingestelde wachtwoorden voor de gebruiker moeten bij de eerste aanmelding worden gewijzigd door de gebruiker.
    iii. Gebruik van Phishing-bestendige MFA authenticatie om toegang te krijgen tot de Zuyd ICT-Infrastructuur is verplicht.
    iv. Gebruik van Phishing-bestendige MFA authenticatie om toegang te krijgen tot extern gerichte applicaties is verplicht.
    v. Gebruik van Phishing-bestendige MFA authenticatie om toegang te krijgen tot applicaties die worden gehost door een externe serviceprovider, indien ondersteund, is verplicht.
    vi. Inactief stellen van gebruikersaccounts:
        a. Medewerkers: bij einde dienstverband binnen 1 werkdag;
        b. Studenten: 30 dagen na uitschrijving opleiding.
    viii. Verwijderen van gebruikersaccounts:
        a. Medewerkers: bij einde dienstverband binnen 120 dagen verwijderen;
        b. Studenten: 90 dagen na uitschrijving opleiding.
o) Beheeraccounts:
    i. Elk beheeraccount voor Zuyd medewerkers is terug te leiden tot één specifieke persoon.
    ii. Er worden geen algemene beheeraccounts gebruikt, tenzij er technische beperkingen zijn inzake het gebruik van een systeem of applicatie, hierbij is de registratie en een aanspreekpunt vereist per algemeen (service) account.
    iii. Gebruikers met een gebruikersaccount gebruiken het beheeraccount uitsluitend voor beheer werkzaamheden.
    iv. Phishing-bestendige MFA authenticatie is vereist voor alle beheeraccounts op alle bedrijfsmiddelen, ongeacht of deze on-site worden beheerd of via een externe provider.
    v. Bij een beheeraccount waarop geen MFA van toepassing is zijn wachtwoorden 90 dagen geldig.
    vi. Na einde dienstverband wordt het beheeraccount binnen 1 werkdag voorzien van een nieuw password en disabled.
    vii. Disabled beheeraccounts worden maximaal 2 weken bewaard en daarna verwijderd.
p) Serviceaccounts:
    i. Gebruik van (Group) Managed Service accounts waar de applicatie dit ondersteunt.
    ii. Interactief aanmelden met een serviceaccount is niet toegestaan.
    iii. Het wachtwoord van het serviceaccount is op een veilige plek opgeslagen.
    iv. Zodra het service account niet meer nodig is wordt het disabled. Binnen 45 dagen wordt het account verwijderd.
q) Standaardaccounts:
    i. Voor de ingebruikname van een Zuyd systeem worden de naamgeving en het wachtwoord van het standaardaccount aangepast.

ii. Access Management (Toegangsautorisatie):

a) Om verantwoordelijkheden te scheiden worden rollen gebruikt om de kans te verkleinen dat individuele personen kritieke processen in gevaar brengen.
b) Medewerkers voeren alleen geautoriseerde taken uit die bij hun respectievelijke rollen en functie(s) behoren.
c) Autorisatieregels worden gebruikt om te bepalen welke gebruikers toegang hebben tot welke delen van het systeem.

d) Autorisaties worden gedaan op basis van rollen, groepen of individuele gebruikers.
e) Voor alle accounts geldt dat toegang is ingericht volgens het least privilige principe.
f) Rechten die de gebruiker niet meer nodig heeft vanuit zijn functie worden tijdig ingetrokken.
g) Gebruikersaccounts:
    i. Toegangsrechten zijn ingesteld d.m.v. een autorisatiematrix (welke gebruikers verkrijgen welke toegang op basis van de rol).
    ii. Autorisaties van rollen en data van applicaties op basis van een opgestelde autorisatiematrix per applicatie.
    iii. De autorisatiematrix bevat de onderkende rollen uitgezet tegen de dataelementen of groepen van dataelementen en er wordt voor elk van die elementen aangegeven of de rol lees, schrijf, wijzigings- of verwijderrechten heeft of geen rechten heeft.
    iv. Toegang tot rollen en data in de applicatie moet op basis van de opgestelde autorisatiematrix worden ingericht.
    v. Indien de rol die een medewerker toegewezen krijgt niet eenduidig van de functietitel is af te leiden, worden extra rechten toegekend, rechten ontnomen en onderbouwd vastgelegd op basis van het 4-ogen principe: de teamleider/opleidingsmanager vraagt de rechten aan en de functioneel beheerder kent deze daadwerkelijk toe.
h) Beheeraccounts:
    i. Er is een actuele lijst met beheeraccounts en uitgedeelde beheerrollen.
    ii. Beperk het aantal beheerders en verdeel de toegang in verschillende beheerrollen.
    iii. Beperk het aantal beheerrollen tot een minimum voor het (veilig) kunnen uitvoeren van de beheeractiviteiten.
    iv. Autorisaties voor beheeraccounts via tijdelijke, verhoogde privileges om toegang te krijgen tot kritieke systemen en applicaties (just in time access).
    v. Beheeraccounts worden alleen gebruikt voor het beheer waarvoor zij bedoeld zijn en hebben daarbij geen autorisatie voor andere toepassingen (just enough access).
    vi. Een noodprocedure is vastgesteld voortoegang tot accounts met super-user rechten in het geval van nood.

iii. Bronsysteem:

a. Bronsysteem voor gebruikersaccounts van medewerkers is het HR systeem.
b. Bronsysteem voor gebruikersaccounts van studenten is het studentenvolgsysteem.
c. Het voeden van het IAM systeem gebeurt automatisch vanuit het HR systeem voor medewerkers als bronsysteem op basis van de functie(s) (need to know / need to access).
d. Het voeden van het IAM systeem gebeurt automatisch vanuit het studentvolgsysteem als bronsysteem voor studenten.
e. Het IAM systeem maakt accounts aan in de benodigde identiteitssystemen zoals AD en Entra ID.
f. Als een account in het bronsysteem wordt geblokkeerd wordt dit automatisch ook in alle gekoppelde systemen geblokkeerd.

9. Periodieke review:
    a. De loggingsinformatie van het gebruik van beheeraccounts (priviliged accounts) wordt minimaal eenmaal per kwartaal middels het vier-ogen principe beoordeeld.
    b. Eens per jaar dienen systeemeigenaren op basis van de autorisatiematrix van alle geautoriseerde **gebruikersaccounts** en hun rol te controleren:
        i. of het account terecht nog toegewezen is;
        ii. of het account de juiste systeemrol heeft.
    c. Eens per jaar dienen systeemeigenaren op basis van de autorisatiematrix van alle geautoriseerde **beheeraccounts** en hun rol te controleren:
        i. of het beheeraccount terecht nog toegewezen is;
        ii. of het beheeraccount de juiste systeemrol heeft.

d. Van de benoemde punten bij periodiek uitgevoerde review (controle/beoordeling) wordt een verslag door de systeemeigenaar gemaakt en teruggekoppeld aan het management.

10. Identity Lifecycle Management (ILM)
    a. ILM voor medewerkers is geborgd via een Start-Mutatie-Stop proces.
        I. Eigenaar van het Start-Mutatie-Stop proces is HR.
        II. Het Start-Mutatie-Stop proces omvat de volgende stappen:
            a. *Start* (Onboarding): Bij het onboarding proces wordt een nieuwe identiteit aangemaakt en moet ervoor gezorgd worden dat de juiste toegangsrechten (autorisaties) worden verleend op basis van de functie en verantwoordelijkheden van de gebruiker. Dit omvat het instellen van de juiste autorisatieregels en het toewijzen van de benodigde privileges;
            b. *Mutatie* (Wijzigingen): Gedurende de levenscyclus van een identiteit kunnen er wijzigingen optreden, zoals een verandering van functie of verantwoordelijkheden. Er moet worden zorggedragen dat de toegangsrechten worden bijgewerkt en aangepast op basis van deze wijzigingen, zodat gebruikers alleen toegang hebben tot de benodigde informatie en systemen;
            c. *Stop* (Beëindiging): Wanneer een gebruiker de organisatie verlaat, moet ervoor gezorgd worden dat de toegangsrechten en privileges van de gebruiker (autorisaties) direct worden ingetrokken en alle identiteiten worden gedeactiveerd en verwijdert. Dit voorkomt dat voormalige gebruikers nog steeds toegang hebben tot systemen en gegevens.
    b. ILM voor studenten is geborgd via aanmelding/afmelding DUO proces.
11. Functiescheiding:
    a. moet voorkomen dat slechts één persoon ongecontroleerd transacties of verplichtingen kan aangaan, autoriseren, verwerken en afwikkelen en toegang heeft tot activa.
    b. Functiescheiding gebeurt op basis van een risico assessment. Op zijn minst voor processen waarin het risico op fraude of het maken van onbedoelde fouten onaanvaardbaar is, wordt functiescheiding doorgevoerd. Dit betreft ten minste:
        i. HR, salarisverwerking;
        ii. Inkoop en facturatie;
        iii. Eigen ontwikkelde IT systemen.
12. Logbestanden van securitygebeurtenissen van accounts: worden gemaakt, bewaard en periodiek beoordeeld door de systeemeigenaar.
13. De gebruikte systemen moeten in staat zijn de loggingen van accounts door te sturen naar het Zuyd SIEM/SOC.
14. De systeemeigenaar werkt met een toestemmingsprocedure om toegangsrechten toe te kennen.
15. De systeemeigenaar zorgt ervoor dat er procedures voor gebruikersbeheer en gebruikersauthenticatie zijn gedefinieerd, gedocumenteerd en gecommuniceerd.
16. De systeemeigenaar zorgt ervoor dat er periodieke controles van autorisaties plaatsvinden, en dat deze gedocumenteerd en gecommuniceerd worden.
17. Er zijn procedures voor het reageren op beveiligingsincidenten en inbreuken waarbij gebruikers betrokken zijn, inclusief protocollen voor het melden en onderzoeken van incidenten en voor het nemen van passende corrigerende maatregelen.

De CISO en ISO's van Zuyd houden toezicht op het volgen van dit beleid. Afwijkingen dienen via de CISO/ISO aangevraagd te worden.