Zuyd Security Beleid – Identity & Access Management

Zuyd Hogeschool

Versie 1.0

Vastgesteld door het CvB
op 16-01-2024

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

Documentatie

Er is gebruik gemaakt van de onderstaande informatie

Naam	Auteur	Status
Informatiebeveiligingsbeleid Zuyd Hogeschool versie 2023	CISO Zuyd Hogeschool	Definitief
Normenkader Informatiebeveiliging versie 2.0 (SURF)	Alf Moens	Definitief

Goedkeuringen

Dit document is goedgekeurd door:

Naam	Uitgiftedatum	Versie
CvB	16-01-2024	1.0

2. Management Summary

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 gebruikers het volgende:

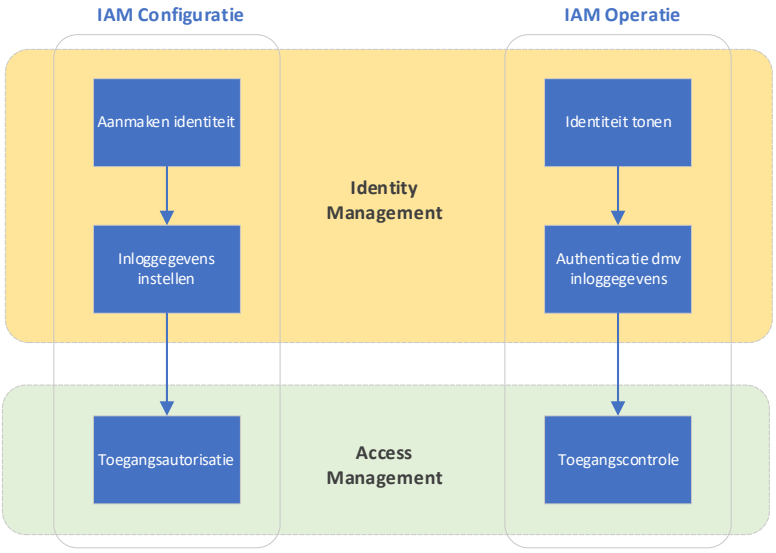
- gebruikersaccounts volgen een start-mutatie-stop proces vanuit het HR systeem of het studentvolgsysteem;
- er zijn aparte accounts voor reguliere kantoorwerkzaamheden en beheeractiviteiten;
- beheeraccounts worden buiten het start-mutatie-stop proces om aangemaakt;
- veiligheidseisen worden gesteld aan het gebruik van accounts, 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 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;
- systeemeigenaren die toegangsrechten mogen toekennen zijn vastgelegd in een toestemmingsprocedure;
- indien de functie/rol die een medewerker toegewezen krijgt niet eenduidig van de functietitel is af te leiden, worden extra rechten toegekend en onderbouwd vastgelegd op basis van het 4-ogen principe: de teamleider vraagt de rechten aan en de functioneel beheerder kent deze daadwerkelijk toe;
- de systeemeigenaar doet jaarlijks een review van verstrekte autorisaties aan gebruikers en (functioneel) beheerders 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 heeft tot bepaalde informatie. IAM houdt vertrouwelijke informatie zoals klantgegevens, persoonlijk identificeerbare informatie en intellectueel eigendom weg van ongeautoriseerde toegang.

Het IAM beleid beschrijft welke vormen van **authenticatie**[1] en **autorisatie**[2] worden gebruikt om de identiteit van gebruikers te verifiëren voordat deze toegang krijgen tot het systeem (Identity Management), welke autorisatieregels worden gebruikt om te bepalen welke gebruikers toegang hebben tot welke delen van het systeem (Access Management), hoe het systeem wordt gemonitord om ongeautoriseerde toegang te detecteren, hoe vaak de toegangscontrolemaatregelen worden geëvalueerd om te zorgen dat deze nog steeds effectief zijn en voldoen aan de bedrijfs- en informatiebeveiligingseisen, en hoe gebruikers worden getraind in het gebruik van het toegangscontrolesysteem en de risico's van ongeautoriseerde toegang begrijpen, en welke maatregelen worden genomen om ongeautoriseerde toegang te voorkomen.



Figuur 1: Identity & Access Management

3.2. Relatie tot andere beleidsstukken

Dit beleid is gekoppeld aan de uitgangspunten in het SURF Audit Toetsingskader[1].
"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, SM.02, OR.02) maar dient met name als een uitwerking van de beheersdoelstellingen NBA ID: ID.01, ID.02, ID.03, ID.04, ID.05 in het domein ***Identity & Access Management***.

[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.

3.3. Relatie tot overige documenten

Naast dit beleidsdocument zijn de volgende stukken relevant

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

3.4. Doel

Het doel van het Identity & Access management beleid is het beheer van gebruikersidentiteiten en toegangsprivileges van Zuyd te automatiseren en te stroomlijnen en daarbij zorg te dragen voor correcte authenticatie van en autorisatie voor gebruikers en daarbij dus ongeautoriseerde toegang te voorkomen. Dit omvat de juiste rechten en toegang tot de Zuyd ICT-Infrastructuur in alle stadia van de levenscyclus van de identiteit in het start-mutatie-stop proces. Dit om risico's inzake integriteit en vertrouwelijkheid te beperken.

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 en beheeraccounts.

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 werkzaamheden uit te voeren;
- Beheeraccounts, voor (functioneel) beheerders, ook wel superuser-, priviliged- of root-accounts genoemd, hebben uitgebreide privileges om besturingssystemen, applicaties en platforms te beheren;
- Standaard accounts zijn vaak vooraf geïnstalleerd en de gebruikersnamen en wachtwoorden kunnen algemeen bekend zijn, wat kan leiden tot een achterdeur.

3.6. Beleid

Bij het verlenen van toegang (authenticatie + autorisatie) aan gebruikers tot de Zuyd ICT-Infrastructuur gelden de volgende security richtlijnen met betrekking tot Identity & Access management:

1. Voor logische toegang tot de Zuyd ICT-Infrastructuur wordt gebruik gemaakt van identity & access management voor alle gebruikers (medewerkers/studenten/beheerders). (Control: NBA ID SM.02)
2. Elke gebruiker krijgt zijn eigen unieke gebruikersaccount (username en wachtwoord). (Control: NBA ID SM.02)
3. Gebruikersaccounts worden aangemaakt en beheerd door FB-ICT in een centraal bronsysteem (IAM). (Control: NBA ID SM.02)
4. Alle acties die met een verstrekt account worden uitgevoerd vallen onder de verantwoordelijkheid van diegene aan wie het account verstrekt is; (Control: NBA ID HR.01)
5. 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; (Control: NBA ID ID.02)

b) Initiële wachtwoorden worden geautomatiseerd gegenereerd en zijn uniek per account; (Control: NBA ID ID.01)
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; (Control: NBA ID SM.02)
d) Complexe wachtwoorden gebruiken:
    i. een combinatie van drie van de volgende vier karakters => cijfers, hoofd- en kleine letters en speciale tekens;
    ii. of het combineren van woorden of gezegden in een willekeurige mix. (Control: NBA ID SM.02)
e) Wachtwoorden die zijn gemaakt voor gebruik met MFA authenticatie moeten minimaal 8 tekens lang zijn; (Control: NBA ID SM.02)
f) Wachtwoorden die zijn gemaakt voor gebruik zonder MFA authenticatie moeten minimaal 14 tekens lang zijn; (Control: NBA ID SM.02)
g) Wachtwoorden zijn alleen onbeperkt geldig bij gebruik van MFA en worden minimaal jaarlijks vervangen;
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; (Control: NBA ID SM.02)
i) Er is een selfservice portal voor gebruikersaccounts om wachtwoorden, wanneer MFA actief is, te herstellen en resetten; (Control: NBA ID SM.02)
j) Indien een gebruiker een MFA reset wenst, dient deze zich in persoon te melden bij de balie van de servicedesk en zich daar te identificeren; (Control: NBA ID SM.02)
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); (Control: NBA ID SM.02)
l) Accounts van gebruikers op lang buitengewoon verlof, zoals bekend bij HR, worden disabled. (Control: NBA ID ID.02)
m) Gebruikersaccount:
    i. Hergebruik van aangemaakte wachtwoorden voor persoonlijke accounts is niet toegestaan; (Control: NBA ID SM.02)
    ii. 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; (Control: NBA ID SM.02)
    iii. Alle standaard nieuw ingestelde wachtwoorden voor de gebruiker moeten bij de eerste aanmelding worden gewijzigd door de gebruiker; (Control: NBA ID SM.02)
    iv. Gebruik van Phishing-bestendige MFA authenticatie om toegang te krijgen tot de Zuyd ICT-Infrastructuur is verplicht; (Control: NBA ID SM.02)
    v. Gebruik van Phishing-bestendige MFA authenticatie om toegang te krijgen tot extern gerichte applicaties is verplicht; (Control: NBA ID SM.02)
    vi. Gebruik van Phishing-bestendige MFA authenticatie om toegang te krijgen tot applicaties die worden gehost door een externe serviceprovider, indien ondersteund, is verplicht; (Control: NBA ID SM.02)
    vii. Inactief stellen van gebruikersaccounts:
        a. Medewerkers: bij einde dienstverband binnen 1 werkdag; (Control: NBA ID ID.02)
        b. Studenten: 30 dagen na uitschrijving opleiding. (Control: NBA ID ID.02)
    viii. Verwijderen van gebruikersaccounts:
        a. Medewerkers: bij einde dienstverband binnen 120 dagen verwijderen; (Control: NBA ID ID.02)
        b. Studenten: 90 dagen na uitschrijving opleiding. (Control: NBA ID ID.02)

n) Beheeraccounts:
    i. Elk beheeraccount voor Zuyd medewerkers is terug te leiden tot één specifieke persoon; (Control: NBA ID ID.03)
    ii. Er worden geen algemene beheeraccounts gebruikt, tenzij er technische beperkingen zijn inzake het gebruik van een systeem of applicatie, hierbij is een aanspreekpunt vereist per algemeen (service) account; (Control: NBA ID ID.03)
    iii. Gebruikers met een gebruikersaccount gebruiken alleen het beheeraccount voor beheer werkzaamheden; (Control: NBA ID ID.03)
    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; (Control: NBA ID SM.02)
    v. Bij een beheeraccount zijn wachtwoorden 180 dagen geldig bij gebruik zonder MFA;
    vi. Na einde dienstverband wordt het beheeraccount binnen 1 werkdag (Control: NBA ID ID.02):
        a. voorzien van een nieuw password;
        b. disabled.
    vii. Disabled beheeraccounts zijn maximaal 2 weken toegestaan en worden daarna verwijderd. (Control: NBA ID ID.02)
o) Serviceaccounts:
    i. Gebruik van (Group) Managed Service accounts waar de applicatie dit ondersteund; (Control: NBA ID ID.02)
    ii. interactief aanmelden met een serviceaccount is niet toegestaan; (Control: NBA ID ID.02)
    iii. Het wachtwoord van het serviceaccount is op een veilige plek opgeslagen. (Control: NBA ID ID.02)
p) Standaardaccounts:
    i. Voordat een systeem gebruikt voor Zuyd worden de naamgeving en het wachtwoord van het standaardaccount aangepast. (Control: NBA ID ID.02)

ii. Access Management (Toegangsautorisatie):

a) Rollen en verantwoordelijkheden zijn gescheiden 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) toebehoren.
c) Autorisatieregels worden gebruikt om te bepalen welke gebruikers toegang hebben tot welke delen van het systeem; (Control: NBA ID ID.01)
d) Autorisaties worden gedaan op basis van rollen, groepen of individuele gebruikers; (Control: NBA ID ID.01)
e) Voor alle accounts geldt dat toegang is ingericht volgens het least privilige principe; (Control: NBA ID ID.02)
f) Ongepaste of inactieve gebruikersrechten worden tijdig uitgeschakeld. (Control: NBA ID ID.02)
g) Gebruikersaccounts:
    i. De systeemeigenaar stelt de toegangsrechten d.m.v. een autorisatiematrix vast (welke gebruikers verkrijgen welke toegang op basis van de rol); (Control: NBA ID ID.02)
    ii. Autorisaties van rollen en data van applicaties op basis van een opgestelde autorisatiematrix per applicatie; (Control: NBA ID ID.02)
    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; (Control: NBA ID ID.02)
    iv. Toegang tot rollen en data in de applicatie moet op basis van de opgestelde autorisatiematrix worden ingericht; (Control: NBA ID ID.02)

v. Indien de rol die een medewerker toegewezen krijgt niet eenduidig van de functietitel is af te leiden, worden extra rechten toegekend en onderbouwd vastgelegd op basis van het 4-ogen principe: de teamleider vraagt de rechten aan en de functioneel beheerder kent deze daadwerkelijk toe; (Control: NBA ID ID.02)

h) Beheeraccounts:
   i. Systeemeigenaar draagt zorg voor een actuele lijst met beheeraccounts en uitgedeelde beheerrollen; (Control: NBA ID ID.02)
   ii. Beperk het aantal beheerders en verdeel de toegang in verschillende beheerrollen; (Control: NBA ID ID.01, NBA ID ID.02, NBA ID.03, NBA ID OR.02)
   iii. Beperk het aantal beheerrollen tot de minimaal indeling voor het (veilig) kunnen uitvoeren van de beheeractiviteiten; (Control: NBA ID ID.03)
   iv. Autorisaties voor beheeraccounts op aanvraag van beheerder wanneer deze nodig zijn (just in time access); (Control: NBA ID ID.02, NBA ID ID.02)
   v. Beheeraccounts worden alleen gebruikt voor het beheer waarvoor zij bedoeld zijn en hebben daarbij geen autorisatie voor andere toepassingen (just in time access + just enough access); (Control: NBA ID ID.03)
   vi. Een noodprocedure is vastgesteld om in geval van nood toegang tot accounts met super-user rechten te beheren. (Control: NBA ID ID.04)

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); (Control: NBA ID SM.02)
d. Het voeden van het IAM systeem gebeurt automatisch vanuit het studentvolgsysteem als bronsysteem voor studenten; (Control: NBA ID SM.02)
e. Het IAM systeem maakt accounts aan in de benodigde identiteitssystemen zoals AD en Entra ID; (Control: NBA ID SM.02)
f. Als een account in het bronsysteem wordt geblokkeerd wordt dit automatisch ook in alle gekoppelde systemen geblokkeerd. (Control: NBA ID SM.02)

6. Periodieke review:
   a. De loggingsinformatie van het gebruik van beheeraccounts (priviliged accounts) wordt minimaal eenmaal per kwartaal middels het vier-ogen principe beoordeeld door de systeemeigenaar. (Control: NBA ID ID.03)
   b. Eens per jaar dienen systeemeigenaren op basis van de autorisatiematrix alle geautoriseerde gebruikersaccounts en hun rol te controleren:
      i. of het account terecht nog geldig is; (Control: NBA ID ID.05)
      ii. of het account de juiste systeemrol heeft. (Control: NBA ID ID.05)
   c. Eens per jaar dienen systeemeigenaren op basis van de autorisatiematrix alle geautoriseerde beheeraccounts en hun rol te controleren:
      i. of het account terecht nog geldig is; (Control: NBA ID ID.05)
      ii. of het account de juiste systeemrol heeft. (Control: NBA ID ID.05)
   d. Van de benoemde punten bij periodiek uitgevoerde review (controle/beoordeling) wordt een verslag door de systeemeigenaar gemaakt en teruggekoppeld aan het management. (Control: NBA ID ID.05)
7. Identity Lifecycle Management is geborgd via een Start-Mutatie-Stop proces.
   a. Eigenaar van het Start-Mutatie-Stop proces is HR.
   b. Het Start-Mutatie-Stop proces omvat de volgende stappen:
      i. *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; (Control: NBA ID HR.03, NBA ID ID.01)

ii. *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; (Control: NBA ID HR.04, NBA ID ID.05))
iii. *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. (Control: NBA ID HR.04, NBA ID ID.05)

8. 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. Alleen 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 is gescheiden van salaristoekenning;
        ii. Inkoop en facturatie;
        iii. Eigen ontwikkelde IT systemen waarbij de maker geen toegang heeft tot de productieomgeving.
9. Logbestanden van gebeurtenissen van accounts: worden gemaakt, bewaard en regelmatig beoordeeld door de systeemeigenaar. (Control: NBA ID SM.04)
10. De gebruikte systemen moeten in staat zijn de loggingen van accounts door te sturen naar het Zuyd SIEM/SOC. (Control: NBA ID SM.04)
11. De systeemeigenaar draagt er zorg voor dat de activiteiten van beheeraccounts worden vastgelegd (minimaal 180 dagen bewaard) en de logbestanden worden beschermd, (Control: NBA ID SM.04)
12. Systeemeigenaren die toegangsrechten toekennen zijn vastgelegd in een toestemmingsprocedure. (Control: NBA ID: SM.02)
13. De systeemeigenaar zorgt ervoor dat er procedures zijn voor gebruikersbeheer en gebruikersauthenticatie gedefinieerd, gedocumenteerd en gecommuniceerd. (Control: NBA ID: SM.02)
14. De systeemeigenaar zorgt ervoor dat er periodieke controles van autorisaties plaatsvinden, en dat dit gedocumenteerd en gecommuniceerd is in een procedure. (Control: NBA ID: SM.02)
15. 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. (Control: NBA ID: SM.07)

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