# Zuyd Security Beleid – Remote Beheer door Externe Partijen

Versie 1.2

Vastgesteld door het CvB op 11-02-2025

# Inhoudsopgave

# 1. Documentenbeheer

**Revisiehistorie**

| Revisiedatum | Samenvatting veranderingen | Door | Versie |
|---|---|---|---|
| 20-09-2022 | Draft versie | D. Heynen | 0.1 |
| 02-12-2022 | Reviewed ISO | D. Heynen | 0.8 |
| 05-12-2022 | Reviewed CISO, opmerkingen verwerkt | D. Heynen | 0.85 |
| 26-01-2023 | Verwerking review opmerkingen FB-ICT, Juridische afdeling, FG&PO. | D. Heynen | 0.9 |
| 06-09-2023 | Concept versie voor CvB met alle opmerkingen verwerkt. | D. Heynen | 0.95 |
| 26-09-2023 | Vastgesteld door CvB. | R. Sterken | 1.0 |
| 26-11-2024 | Minor Update, template Zuyd, url koppelingen, tekstuele aanpassing. | D. Heynen | 1.1 |
| 11-02-2025 | 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 |
| Privacy & Security Risicomanagement | CISO Zuyd Hogeschool | Definitief |

**Jaarlijkse vaststelling**

Dit document is vastgesteld door:

| Naam | Uitgiftedatum | Versie |
|---|---|---|
| CvB | 11 februari 2025 | 1.2 |

# 2. Management Summary

Remote beheer, waarbij een organisatie delen van haar automatisering op afstand laat beheren door externe partijen, brengt specifieke risico's met zich mee voor de informatiebeveiliging. Deze risico's ontstaan doordat het beheer deels buiten de beheersbare bedrijfsomgeving plaatsvindt, waardoor de organisatie minder invloed heeft op de beveiliging van externe werkstations en werkplekken. Deze werkplekken kunnen als springplank gebruikt worden. Bovendien kan deze extra toegang gebruikt worden voor een aanval.

Dit beleid streeft ernaar de informatiebeveiliging te waarborgen bij remote beheer, met focus op het beschermen van Zuyd data en systemen tegen ongeautoriseerde toegang en potentiële beveiligingsincidenten.

Scope:

- De scope van het beleid betreft alle Zuyd systemen in beheer bij FB-ICT van Zuyd Hogeschool, waar contractueel is vastgelegd dat door de externe partijen remote beheer kan worden uitgevoerd.

Kernpunten:

- Veiligheid: Toegang van externe partijen aan Zuyd systemen dient te worden uitgevoerd met een door Zuyd verstrekt remote account. Dit remote account is standaard uitgeschakeld.

- Verantwoordelijkheid: Minimaal jaarlijks dient er door de systeemeigenaar opnieuw verantwoording te worden gegeven voor de noodzaak van de benodigde remote accounts van externe partijen.

- Autorisatie: Er dient registratie door FB-ICT van het verstrekte Zuyd remote account inclusief autorisaties & betreffende systemen en actuele toegangsstatus plaats te vinden.

# 3. Zuyd Security Beleid – Remote beheer door Externe Partijen

## 3.1. Inleiding

Men spreekt van remote beheer als een organisatie delen van haar automatisering op afstand beheert of laat beheren door een externe partij. Remote beheer brengt, net als telewerken in het algemeen, andersoortige bedreigingen met zich mee, omdat het voor een deel buiten de beheersbare bedrijfsomgeving plaatsvindt. Dat laatste betekent dat een organisatie mogelijk minder invloed heeft op de beveiliging van (niet vertrouwde) werkstations en (externe) werkplekken van beheerders van externe partijen.

Verder is de impact van incidenten relatief groot. Zo worden er potentieel veel gebruikers getroffen als externe partijen in geval van storingen geen beheer op afstand kunnen uitvoeren. Bovendien kan misbruik van accounts van de externe partijen veel schade veroorzaken, omdat deze remote accounts doorgaans ruime bevoegdheden hebben op Zuyd systemen en daarbij behorende Zuyd data. Zo zou bijvoorbeeld malware op een Zuyd server geplaatst kunnen worden.

## 3.2. Relatie tot SURF CMM Toetsingskader

Dit beleid is gekoppeld aan de uitgangspunten in het SURF Audit Normenkader. 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 heeft sterke raakvlakken met meerdere beheers doelstellingen uit dit kader (te weten: NBA ID: ID.01, NBA ID: ID.02, NBA ID: ID.03, NBA ID: ID.05, NBA ID: OR.01, NBA ID: OR.02, NBA ID: SM.02, NBA ID: SM.04, NBA ID: SM.06, NBA ID: SM.08) maar dient met name als een uitwerking van de beheers doelstelling **NBA ID:ID.03** 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.
- Privacybeleid Zuyd Hogeschool
  - Het document dat het privacybeleid van Zuyd beschrijft.

## 3.4. Doel

Dit beleid is opgesteld om risico's bij het uitvoeren van remote beheer door externe partijen zo klein mogelijk te maken en daarmee invloeden op de informatiebeveiliging zoals op de beschikbaarheid (dataverlies), integriteit (ongewenste mutaties van Zuyd systemen) en vertrouwelijkheid (verlies data voorkomen) bij het gebruik van remote accounts te voorkomen en/of te beperken.

## 3.5. Scope

De scope van het beleid betreft alle Zuyd systemen in beheer bij FB-ICT van Zuyd Hogeschool, waar contractueel is vastgelegd dat door de externe partijen remote beheer kan worden uitgevoerd.

## 3.6. Beleid

Bij het beheren door externe partijen van Zuyd systemen middels remote accounts dienen buiten de Zuyd baseline richtlijnen ook de volgende richtlijnen te worden toegepast:

1. Toegang van externe partijen aan Zuyd systemen dient te worden uitgevoerd met een door Zuyd verstrekt remote account. (Control: NBA ID ID.02)
2. Uitgangspunt is dat Zuyd één niet persoonsgebonden remote account aanreikt per bedrijf. In overleg met Zuyd kunnen maximaal vijf remote accounts per externe partij worden uitgereikt. (Control: NBA ID OR.02)
3. De volgende technische maatregelen dienen ingericht te zijn voor remote beheer door externe partijen:
    a. Het Just-in-Time principe wordt toegepast d.w.z. standaard is het remote account van externe partijen disabled; (Control: SURF SB.13.005, NBA ID ID.03)
    b. Het gebruik van multi-factor authenticatie (MFA) en/of een door Zuyd geleverd token is de standaard bij elke remote account aanmeldpoging van een externe partij; (Control: NBA ID ID.01);
    c. Als het bij punt 3b benoemde niet mogelijk is dan wordt door Zuyd Hogeschool met de externe partij gekeken naar een andere (tijdelijke) oplossing;
    d. In alle gevallen is de externe partij verantwoordelijk voor goed huisvaderschap bij het op afstand uitvoeren van werkzaamheden op Zuyd systemen; (Control: NBA ID OR.01)
    e. Wanneer remote ondersteuning op Zuyd systemen noodzakelijk is door een externe partij, dan dient de levensduur van de verbinding te worden beperkt tot de tijd (Just in Time Access) die nodig is om deze ondersteuning uit te voeren; (Control: NBA ID ID.03)
    f. Het wachtwoord van een Zuyd remote account van een externe partij dient 3-maandelijks gewijzigd te worden en heeft een lengte van minimaal 15 karakters; (Control: SURF SB.13.005, NBA ID ID.03)
    g. Een Zuyd remote account van een externe partij heeft een verloopdatum ingesteld van maximaal 365 dagen; (Control: NBA ID ID.05)
    h. Toegang van externe partij remote accounts dient beperkt te blijven (Just Enough Access) tot de Zuyd systemen waar de externe partij ondersteuning op moet kunnen verlenen; (Control: NBA ID ID.02)
    i. Computers die de externe partij gebruikt voor remote beheer, die op afstand zijn verbonden met het bedrijfsnetwerk van Zuyd, mogen niet tegelijkertijd verbonden zijn met een ander netwerk, met uitzondering van persoonlijke netwerken die onder de volledige controle van de gebruiker staan; (Control: NBA ID SM.08)
    j. Uitgevoerde werkzaamheden van elk remote account van de externe partij dient automatisch vastgelegd te worden door middel van logging; (Control: NBA ID SM.04)
    k. Real time monitoren en managen van beveiligingsgebeurtenissen van aan de extern verstrekte Zuyd remote accounts van externe partijen verloopt via het Zuyd SIEM/SOC; (Control: NBA ID SM.04)
    l. Het is verplicht dat computers van externe partijen die zijn verbonden met Zuyd interne netwerken via externe toegangstechnologieën, de meest up-to-date operating system en antivirussoftware gebruiken; (Control: NBA ID SM.06)
    m. Het wordt aanbevolen dat computers van externe partijen die zijn verbonden met Zuyd interne netwerken via externe toegangstechnologieën, een host-firewall geïnstalleerd hebben die compatibel is met het gebruikte remote toegangssysteem. (Control: NBA ID SM.08)

4. Het gebruik van remote accounts is enkel toegestaan wanneer er een systeem- of bedrijfsbeperking is die het gebruik van een afzonderlijk/individueel account verhindert. Deze gevallen moeten worden beoordeeld en gedocumenteerd door FB-ICT en de eigenaar van de dienst/product/applicatie moet akkoord geven.

5. Elk remote account dient te zijn voorzien van contactgegevens van de externe partij (contactpersoon en/of naam van de medewerker). (Control: NBA ID SM.02)

6. Er dient registratie door FB-ICT van het verstrekte Zuyd remote account inclusief autorisaties & betreffende systemen en actuele toegangsstatus plaats te vinden. (Control: NBA ID SM.02)

7. Minimaal jaarlijks dient er door de systeemeigenaar opnieuw verantwoording te worden gegeven voor de noodzaak van de benodigde remote accounts van externe partijen. (Control: NBA ID ID.05, SM.02)

8. FB-ICT zorgt dat procedures aanwezig zijn voor de systeemeigenaar om voor de externe partij de (initiële) toegang, wijzigingen en beëindiging van de remote accounts aan te vragen binnen Zuyd Hogeschool. (Control: NBA ID OR.01)

9. FB-ICT zorgt dat procedures aanwezig zijn om tijdelijke toegang van de externe partijen remote accounts te beheren binnen Zuyd Hogeschool. (Control: NBA ID OR.01)

10. Externe partijen die niet-standaard externe toegangsoplossingen willen implementeren op het productienetwerk van Zuyd, moeten vooraf toestemming krijgen van de CISO van Zuyd Hogeschool. (Control: NBA ID ID.03)

11. Rechten en plichten van de externe partijen die remote beheer uitvoeren worden van tevoren vastgesteld in een overeenkomst van Zuyd Hogeschool. (Control: NBA ID ID.03)

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