Zuyd Security Beleid – Backup

Versie 2.4

Vastgesteld door het CvB op 11-02-2025

Inhoudsopgave

1. Documentenbeheer

Revisiehistorie

Revisiedatum	Samenvatting veranderingen	Door	Versie
03-04-2020	Draft versie	Rob Geerts	0.1
08-09-2020	Definitieve versie	Rob Geerts	1.0
07-06-2021	Draft versie	Rob Geerts	2.0
28-09-2021	Vastgesteld door CvB.	R. Sterken	2.2
13-02-2025	Minor Update, template Zuyd, url koppelingen, tekstuele aanpassing.	D. Heynen	2.3
11-02-2025	Vastgesteld door CvB	R. Sterken	2.4

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
Enterprise Architectuur - Kroonjuwelen	IM	Definitief

Jaarlijkse vaststelling

Dit document is vastgesteld door:

Naam	Uitgiftedatum	Versie
CvB	11 februari 2025	2.4

2. Management Summary

Het beleid van Zuyd Hogeschool inzake backups is erop gericht om Zuyd data te beschermen en daarmee invloeden op de informatiebeveiliging zoals op de vertrouwelijkheid (dataverlies), integriteit (corruptie) of beschikbaarheid (ransomware) te voorkomen.

Een effectief backup beleid zorgt ervoor dat Zuyd snel kan herstellen van dataverlies, waardoor:

- Downtime wordt geminimaliseerd
- Bedrijfsprocessen kunnen worden voortgezet
- Financiële verliezen worden beperkt
- Naleving wet- en regelgeving (waaronder SURF CMM3 normenkader)

Scope:

- De scope van het beleid betreft alle Zuyd data op Zuyd systemen.
- De systeemeigenaar bepaalt of de Zuyd data van zijn systeem wordt geback-upt en wat er wordt geback-upt (incl. backup strategie).
- Als er wordt besloten géén back-up te maken wordt dit vastgelegd.
- Voor de zogenaamde kroonjuwelen van Zuyd bestaat een back-up-plicht vanuit het CvB.

De kernpunten zijn:

- Er wordt een back-up strategie wordt vastgesteld en deze wordt vastgelegd in een document.
- De bewaarperiode van de back-up, met inachtneming van relevante wet- en regelgeving, dan wel gedragscodes (Selectielijst hogescholen), dan wel het noodzakelijkheidscriterium is.
- Er technische documentatie aanwezig is voor zowel de back-up als de restore van informatie.
- Er een audit-trail wordt bijgehouden van minimaal:
    - de resultaten van back-up als de (test) restore activiteiten;
    - toegang tot de back-up data en uitgevoerde back-up en restore activiteiten;
    - de verblijfplaats van gebruikte back-up media.
- Back-ups worden bewaard op een veilige locatie.
- Backups die niet versleuteld of gewist kunnen worden inclusief back-ups offline opslaan.
- Alleen geautoriseerde personen zich toegang kunnen verschaffen tot de gemaakte back-ups.

3. Zuyd Security Beleid – Backup

3.1. Inleiding

Dit beleid is erop gericht om Zuyd data te beschermen en daarmee invloeden op de informatiebeveiliging zoals op de vertrouwelijkheid (dataverlies), integriteit (corruptie) of beschikbaarheid (ransomware) te voorkomen.

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: BC.01, NBA ID: BC.02, NBA ID: BC.03, NBA ID: GO.02, NBA ID: DM.01, NBA ID: DM.02, NBA ID: DM.03, NBA ID: DM.04, NBA ID: DM.06, NBA ID: OP.02, NBA ID: SM.13) maar dient met name als een uitwerking van de beheers doelstelling **NBA ID: OP.02 & NBA ID: BC.03** in het domein *IT Operatie & Bedrijfscontinuïteitsmanagement*.

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.
- Enterprise Architectuur - Kroonjuwelen
  - Het document dat een actueel overzicht bevat van de kroonjuwelen.

3.4. Doel

Het doel van dit beleid is het beschermen van Zuyd data tegen verlies. Door regelmatig kopieën van gegevens te maken, kan Zuyd informatie herstellen in het geval van:

- Cyberaanvallen zoals ransomware;
- Onbedoelde verwijdering en/of corruptie van bestanden;
- Hardware storingen of systeemcrashes;
- Natuurrampen of ander calamiteiten.

Een effectief backup beleid zorgt ervoor dat Zuyd snel kan herstellen van dataverlies, waardoor:

- Downtime wordt geminimaliseerd;
- Bedrijfsprocessen kunnen worden voortgezet;
- Financiële verliezen worden beperkt;
- Naleving wet- en regelgeving (waaronder SURF CMM3 normenkader).

3.5. Scope

In scope is alle Zuyd data van Zuyd systemen. In het algemeen bepaalt de systeemeigenaar daarbij of de Zuyd data van zijn systeem wordt geback-upt en wat er wordt geback-upt. De systeemeigenaar legt voor zijn systeem een back-up strategie vast. Dus, ook de argumentatie waarom er wordt besloten géén back-up te maken.

Alleen voor de zogenaamde kroonjuwelen van Zuyd bestaat een back-up-plicht vanuit het CvB.

3.6. Beleid

Voor systeemeigenaren gelden de volgende security richtlijnen met betrekking tot de backup van Zuyd data:

- Er een back-up strategie wordt vastgesteld en deze wordt vastgelegd in een document. Minimaal bevat dit document:
    a. De argumentatie waarom een backup al dan niet noodzakelijk is.
    b. De soort gegevens (bestanden, databases, enz.) die worden ge-backupt, met welke frequentie en eventueel een overzicht van de gegevens die bewust niet worden geback-upt. (Control: SURF SB.2.001)
    Kaders: Gegevens dienen minimaal eens per 24 uur ge-backupt te worden.
    c. De maximale duur voor het maken van een backup, en tevens de maximale duur voor het uitvoeren van een restore. (Control: SURF SB.2.001)
    d. Bewaarperiode van de back-up, met inachtneming van relevante wet- en regelgeving, dan wel gedragscodes (Selectielijst hogescholen), dan wel het noodzakelijkheidscriterium. (Control: SURF SB.2.003)
    e. Een duidelijk overzicht van de bevoegde personen, inclusief hun functies en namen, die gemachtigd zijn om een restore-actie goed te keuren. Dit overzicht bevat tevens een gedetailleerd escalatiemodel dat specificeert wie op welk moment bij een herstelactie betrokken moet worden en wie vervolgens verantwoordelijk is voor de evaluatie en goedkeuring van de herstelde data.
    f. Een plan en uitvoering voor het periodiek testen van restore acties conform BIV classificatie. (Control: SURF SB.2.001)
    Kaders: Minimaal is het verplicht te testen of de data bruikbaar te restoren is.
- Er is technische documentatie aanwezig voor zowel de back-up als de restore van data, zodat herinrichting en foutherstel van verwerkingen mogelijk is. (Control: SURF SB.2.001)
- Er een audit-trail wordt bijgehouden van minimaal:
    a. de resultaten van back-up als de (test) restore activiteiten; (Control: SURF SB.2.001)
    b. toegang tot de back-up data en uitgevoerde back-up en restore activiteiten; (Control: SURF SB.2.003)
    c. de verblijfplaats van gebruikte back-up media. (Control: SURF SB.2.003)
- Back-ups worden bewaard op een locatie die zodanig gekozen is, dat een incident of calamiteit (bijv. brand) die leidt tot schade aan de oorspronkelijke data, niet kan leiden tot schade aan de back-up of de mogelijkheid tot een restore over te gaan. (Control: SURF SB.2.001, SB.2.003)
- Ervoor gezorgd wordt dat door een ransomware aanval de backups niet versleuteld of gewist kunnen worden, door back-ups tevens offline op te slaan. (Control: SURF SB.2.001, SB.2.003)
- De fysieke en logische toegang tot de back-ups zodanig is ingeregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.
- Er aantoonbare uitvoering van een lifecycle en patch management van de gebruikte back-up tooling is. (Control: SURF SB.1.008)

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