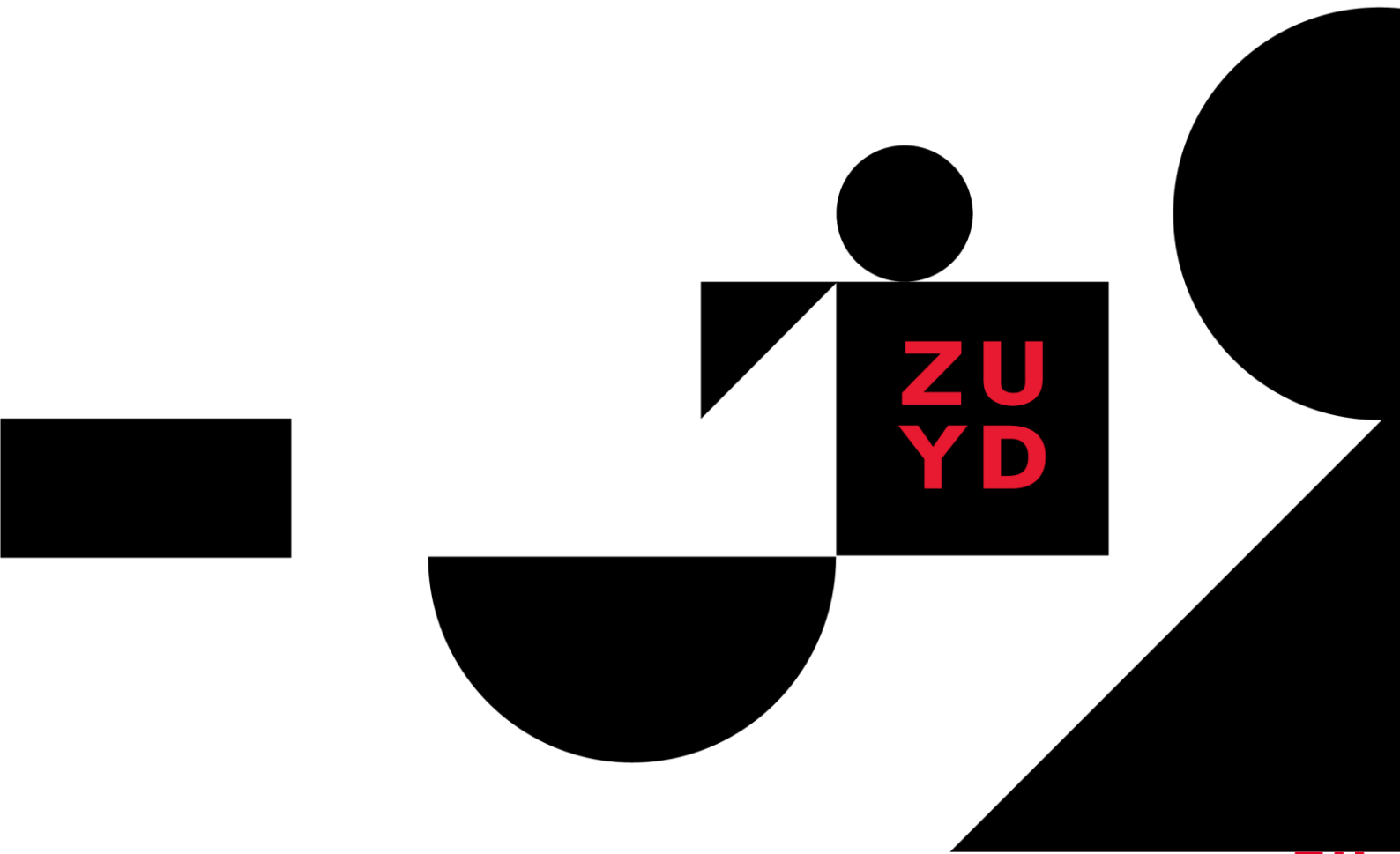
Zuyd Security Beleid – Webapplicaties

Versie 2.2

Vastgesteld door het CvB op 11-02-2025



Inhoudsopgave

1. Documentenbeheer

Revisiehistorie

Revisiedatum	Samenvatting veranderingen	Door	Versie
06-09-2022	Verwerking review opmerkingen M&C, FB&ICT, Juridische afdeling, FG&PO.	D. Heynen	0.9
04-10-2022	Website beleid vastgesteld door portefeuillehouder Olaf van Nugteren.	D. Heynen	1.0
11-09-2023	Taalkundige correcties + naamgeving document + diverse toevoegingen	D. Heynen	1.2
26-09-2023	Vastgesteld door CvB	R. Sterken	2.0
xx-xx-2025	Minor Update (Managementsamenvatting toegevoegd + naam/scope verduidelijking + kleine aanpassingen)	D. Heynen	2.1
11-02-2025	Vastgesteld door CvB	R. Sterken	2.2

Documentatie

Er is gebruik gemaakt van de onderstaande informatie

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

Jaarlijkse vaststelling

Dit document is vastgesteld door:

Naam	Uitgiftedatum	Versie
CvB	11 februari 2025	2.2

2. Management Summary

De scope van het beleid betreft alle Zuyd systemen die een browser gebruiken om webapplicaties te benaderen. Hieronder vallen onder andere internetsites, extranetten, intranetten, software-as-service (SaaS)-applicaties en webservices.

Elke medewerker van Zuyd Hogeschool draagt bij aan de verantwoordelijkheid voor het inzetten en gebruiken van systemen zoals webapplicaties, met een focus op goede informatiebeveiliging en privacybescherming.

Externe aanvallen richten zich vaak op webapplicaties, die wereldwijd toegankelijk zijn via een browser. Dit beleid is ontworpen om het aanvalsvlak te minimaliseren en dataverlies of ongewenste wijzigingen in webapplicaties te voorkomen.

In grote lijn betekent dit bij het inzetten en gebruik van Zuyd webapplicaties het volgende:

- Er een contract inclusief SLA wordt opgesteld met de contractpartij die de bouw en het beheer van webapplicaties gaat verzorgen;
- Aantoonbare uitvoering van lifecycle-, patch-, release- en incident-management van alle door de contractpartij gebruikte relevante systemen en software;
- Inrichting van maatregelen (controls) om webapplicaties te beschermen tegen aanvallers;
- Website hosting geschiedt op een voor Zuyd Hogeschool dedicated systeem (Managed VPS). Hierbij is de website compleet afgeschermd en kan deze onafhankelijk van andere systemen gebruikt en beveiligd worden.

Het webapplicatie security beleid biedt een overzicht van de verantwoordelijkheden en maatregelen die nodig zijn om de informatiebeveiliging binnen Zuyd Hogeschool te waarborgen. Het benadrukt de noodzaak van voortdurende aandacht voor beveiliging en privacy in een steeds veranderende digitale omgeving.

3. Zuyd Security Beleid – Webapplicaties

3.1. Inleiding

Elke medewerker van Zuyd is mede verantwoordelijk bij het inzetten en gebruiken van systemen zoals webapplicaties en de daarbij behorende systemen voor een goede informatiebeveiliging en aandacht voor privacy (persoonsgegevens). Veel aanvallen van buitenaf zijn gericht op externe systemen zoals webapplicaties. Mede daar dit de systemen zijn die vanaf elke plek in de wereld te bereiken zijn.

Dit beleid is er op gericht het aanvalsvlak zo klein mogelijk te maken en daarmee dataverlies of ongewenste mutatie op webapplicaties en de achterliggende systemen 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 voor dit beleid passende onderdelen geselecteerd die een onderwijsinstelling in ieder geval geregeld moet hebben. Het heeft sterke raakvlakken met meerdere beheersdoelstellingen uit dit kader (te weten: NBA ID: CO.01, NBA ID: IM.01, NBA ID: IM.03, NBA ID: OR.01, NBA ID: OR.02, NBA ID: OR.03, NBA ID: SC.01, NBA ID: SC.04, NBA ID: SM.03, NBA ID: SM.06, NBA ID: SM.07, NBA ID: SM.10) maar dient met name als een uitwerking van de beheers doelstelling **NBA ID SM.10** in het domein ***Vertrouwelijkheid & Integriteit***.

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

Het beleid voor webapplicaties van Zuyd Hogeschool is opgesteld met als doel de risico's te beperken van de schending van:

- Vertrouwelijkheid (bijv. onbedoelde blootstelling van gegevens);
- Integriteit (bijv. defacing);
- Beschikbaarheid (bijv. verlies, of blootstelling van sensitieve gegevens door malware of ransomware).

3.5. Scope

De scope van het beleid betreft alle Zuyd systemen die een browser gebruiken om webapplicaties te benaderen. Hieronder vallen onder andere internetsites, extranetten, intranetten, software-as-service (SaaS)-applicaties en webservices.

3.6. Beleid

Bij webapplicaties dienen buiten de Zuyd baseline richtlijnen ook de volgende richtlijnen te worden toegepast:

1. Er een **contract** wordt opgesteld met de contractpartij die de bouw en het beheer van webapplicaties gaat verzorgen. Hierin is opgenomen dat:
    a. Het de contractpartij is toegestaan om, onder dezelfde contractueel vastgelegde afspraken, (een) subverwerker(s) in te schakelen voor de bouw van de website en/of het beheer (website hosting).
    Kaders:
        I. deze subverwerker(s) dient/dienen aan dezelfde contractuele voorwaarden en kaders te voldoen als de contractpartij/verwerker;
        II. Voldoende zekerheid ten aanzien van continuïteit van de geboden dienstverlening, dit ter beoordeling van de CISO.
    b. Bij website hosting dit geschiedt op een voor Zuyd Hogeschool dedicated Managed VPS (Virtual Private Server). Hierbij is de website compleet afgeschermd en kan onafhankelijk van andere systemen gebruikt en beveiligd worden. (SURF SB.16.006)
2. Er een **service level agreement** wordt vastgelegd, dat minimaal bevat (Control: NBA ID SC.01):
    a. De gegevens van de webapplicatie leverancier, die verantwoordelijk is voor de bouw en het beheer. Deze wordt daarbij gezien als contractpartij en verwerker. (Control: NBA ID SM.03)
    Kaders: de hosting partij dient ISO27001 gecertificeerd te zijn gedurende de gehele contractperiode voor het hosten van de afgenomen relevante webapplicatie.
    b. De aantoonbare uitvoering van lifecycle-, patch-, release- en incident-management van alle door de contractpartij gebruikte relevante systemen en software voor de bouw en/of het beheer van de webapplicatie. (Control: NBA ID CO.02, NBA ID IM.01, NBD ID IM.03 en Control: NBA ID SM.06))
    Kaders:
        i. uitvoering van updates & onderhoud op het systeem (onderliggende operating systeem) en de gebruikte applicaties/web-interfaces (software libraries & plug-ins) dient minimaal elke 14 dagen te geschieden (SURF SB.1.008);
        ii. scanproces op kwetsbaarheden van het systeem ingericht ter ondersteuning van i. (operating system, webhosting platform en de daarin aanwezige plug-ins);
        iii. naast onder punt ii gevonden kwetsbaarheden tevens openbaar bekende of gevonden kwetsbaarheden gepubliceerd of door Zuyd gemeld worden overeenkomstig de aard van de kwetsbaarheid, zo snel als mogelijk, doch uiterlijk binnen 48 klokuren gemitigeerd;
        iv. uitschakelen van alle niet benodigde features en services (system hardening) conform (SURF SB.16.005);
        v. upgrade (release management) naar een hogere applicatie/web interface (software libraries & plug-ins) versie benodigd voor de uitvoering van i en iii is onderdeel van de werkzaamheden.
    c. Inrichting van maatregelen (controls) om de webapplicatie te beschermen tegen aanvallers. (Control: NBA ID SM.02, Control: NBA ID SM.03, Control: NBA ID OR.02 en Control: NBA ID SM.10)
    Kaders:
        i. mitigerende maatregelen m.b.t. de OWASP top tien (https://owasp.org/Top10/) inrichten en bijhouden (SURF SB.14.006);
        ii. webapplicaties worden dual-stack ingericht (zowel IPv4 als IPv6);
        iii. voor de uitvoering van de website (systemen) mogen geen voor de functionaliteit onnodige (UDP/TCP) poorten openstaan;
        iv. gebruik maken van RPKI om route hijacks te voorkomen;

v. plaatsing security.txt bestand van Zuyd op de website om het voor security onderzoekers mogelijk te maken kwetsbaarheden te melden aan Zuyd;
vi. er dient te allen tijde gebruik te worden gemaakt van geldige certificaten verstrekt via de Certificaat Autoriteit (CA) van Zuyd Hogeschool (SURF SB.5.003);
vii. de DNS records zijn voorzien van een digitale handtekening (DNSSEC)
viii. gebruik maken van richtlijnen voor encryptie van verbindingen conform SURF Baseline (SURF SB.3.001), basisbeveiliging.nl en minimaal een B score bij SSLLabs.com (SSL Rating Score);
ix. alle gevoelige data in rust dient versleuteld te zijn;
x. gebruik maken van HTTPS (inclusief redirect en compression);
xi. HTTP security headers om gebruikers te beschermen:
    a. X-Frame-Options;
    b. X-Content-Type-Options;
    c. Content-Security-Policy;
    d. Referrer-Policy Existence.
xii. om een veilige verbinding te forceren, dient HTTP Strict Transport (HSTS) aan te staan;
xiii. malware scanning op alle bestanden geplaatst door gebruikers en systemen;
xiv. persoonsgegevens, tokens en wachtwoorden zijn niet zichtbaar in een URL of HTTPS verzoek (GET/POST/PUT/PATCH/DELETE);
xv. bij het gebruik van invulformulieren, een check inbouwen om aan te tonen dat degene die het plaatst een mens is, deze check mag daarbij conform AVG geen persoonsgegevens verzamelen.

d. Opnemen van een boeteclausule bij overtreding van de onder punt 2b & 2c genoemde kaders. Hierbij is het uitgangspunt dat Zuyd per overtreding een boete claimt van 5000 euro. De nadere omschrijving van het boetebeding wordt vooraf door de eigenaar afgestemd met JZ. (Control: NBA ID SC.04)

3. Het gebruiken van de webapplicatie als (bulk)mail (relay) systeem voor domeinen van Zuyd is niet toegestaan.
4. Een **verwerkersovereenkomst** met de contractpartij wordt afgesloten als deze (bijzondere) persoonsgegevens, waar Zuyd Hogeschool verantwoordelijk voor is, gaat: verzamelen, vastleggen, bewaren, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen én indien er tussen Zuyd Hogeschool en de contractpartij sprake is van een verwerkingsverantwoordelijke – verwerkersrelatie.
5. Indien (bijzondere) persoonsgegevens verwerkt worden moet MFA van toepassing zijn op de toegang tot de systemen en data.
6. De eigenaar draagt er zorg voor dat gebruikers instructies krijgen om de webapplicatie op een juiste manier te benaderen (bijvoorbeeld via een bookmark/koppeling op intranet).
7. Het is Zuyd Hogeschool toegestaan om periodiek **pentests** en/of (onaangekondigde) **vulnerability assessments** t.a.v. de websiteapplicatie van contractpartij(en) uit te voeren. (Control: NBA ID SM.07)
8. Het **domeinhouderschap** van de website belegd wordt bij Zuyd Hogeschool. (Control: NBA ID OR.01)

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