Zuyd Security Beleid – Systeemgegevens-uitwisseling

Versie 1.2

Vastgesteld door het CvB op 11-02-2025

Inhoudsopgave

1. Documentenbeheer

Revisiehistorie

Revisiedatum	Samenvatting veranderingen	Door	Versie
02-12-2022	Draft versie	D. Heynen	0.1
12-12-2022	Verder uitwerking/verdieping	D. Heynen	0.3
13-02-2023	Verwerking review opmerkingen IM en FB&ICT,	D. Heynen	0.6
03-03-2023	Verwerking review opmerkingen Juridische afdeling en FG&PO.	D. Heynen	0.9
21-09-2023	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

Systeemgegevensuitwisseling bij Zuyd betreft de overdracht van gegevens tussen interne systemen en/of met externe systemen. Dit proces, ook wel "integratie" genoemd, kan plaatsvinden via standaardkoppelingen of via de Enterprise Service Bus (ESB) van Zuyd.

Scope:

- De scope van het beleid betreft alle systemen waar met toestemming van de eigenaar een integratie mee tot stand gebracht wordt om systeemgegevens (Zuyd data) mee uit te wisselen.

Kernpunten:

- Veiligheid: Integraties moeten de beschikbaarheid, vertrouwelijkheid en integriteit van Zuyd-data waarborgen.
- Verantwoordelijkheid: De eigenaar van het Zuyd systeem draagt de eindverantwoordelijkheid voor het systeem en de data.
- Autorisatie: Alleen de eigenaar van het leverende Zuyd systeem mag toestemming geven voor het inrichten, aanpassen of verwijderen van integraties.

Deze aanpak zorgt voor een gecontroleerde en veilige gegevensuitwisseling binnen de Zuyd-omgeving, waarbij de verantwoordelijkheid duidelijk is belegd bij de systeemeigenaren.

3. Zuyd Security Beleid – Systeemgegevensuitwisseling

3.1. Inleiding

Men spreekt over data-uitwisseling (systeemgegevensuitwisseling) als er Zuyd data tussen Zuyd systemen of tussen Zuyd en niet Zuyd systemen wordt uitgewisseld. Deze koppeling tussen systemen wordt in jargon "integratie" genoemd. Voor de integraties kan gebruikt worden gemaakt van standaardkoppelingen en daarnaast kan worden voorzien in koppelingen met de bestaande Enterprise Standard Bus (ESB) van Zuyd. De te gebruiken integraties dienen veilig te zijn en zowel de beschikbaarheid, vertrouwelijkheid als integriteit van de Zuyd data te waarborgen.

De (eind)verantwoordelijkheid van het Zuyd systeem en de Zuyd data ligt te allen tijde bij de eigenaar van het systeem. Het is daarom dat alleen de eigenaar van het leverende Zuyd systeem toestemming mag verlenen om integraties ten behoeve van systeemgevensuitwisseling in te laten richten, aanpassen of verwijderen.

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: DM.01, NBA ID: DM.03, NBA ID: DM.05, NBA ID: ID.01, NBA ID: ID.02, NBA ID: ID.03, NBA ID: ID.05, NBA ID: OR.01, NBA ID: SM.04, NBA ID: SM.05, NBA ID: SM.06, NBA ID: SM.07, NBA ID: SM.10, NBA ID: SM.12) maar dient met name als een uitwerking van de beheers doelstelling **NBA ID: DM05** in het domein ***Data 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.
- https://www.noraonline.nl/wiki/SIG_Evaluation_Criteria_Security_-_Guidance_for_producers
  - Document van NORA dat API Security beschrijft.
- https://publicatie.centrumvoorstandaarden.nl/api/adr/
  - Document van de overheid over API Design Rules.
- https://www.ssh.com/academy/ssh/openssh
  - Document over SSH en OpenSSH beveiliging.

3.4. Doel

Dit beleid is opgesteld om bij integraties ten behoeve van systeemgegevensuitwisseling tussen Zuyd systemen of tussen Zuyd en niet-Zuyd systemen de beschikbaarheid, integriteit en vertrouwelijkheid te borgen. Dit door alleen met toestemming van de systeemeigenaar integraties te realiseren en bij systeemgegevensuitwisseling dataverlies of ongewenste mutaties aan Zuyd data te voorkomen en/of te beperken.

3.5. Scope

De scope van het beleid betreft alle Zuyd systemen waar met toestemming van de eigenaar een integratie mee tot stand gebracht wordt om systeemgegevens (Zuyd data) mee uit te wisselen.

3.6. Beleid

Bij integraties tussen Zuyd systemen of tussen Zuyd en niet-Zuyd systemen voor systeemgegevensuitwisseling dienen buiten de Zuyd baseline richtlijnen ook de volgende richtlijnen te worden toegepast:

1. Elke integratie ten behoeve van systeemgegevensuitwisseling mag alleen met expliciete schriftelijke toestemming van de eigenaar van het Zuyd systeem dat de data afgeeft ingericht worden. De toestemming moet duidelijk en specifiek aanduiden welke gegevens worden uitgewisseld, voor welke doel, met wie en voor hoe lang de systeemgegevensuitwisseling plaats zal vinden. (Control: NBA ID OR.01, SURF SB.06.010)
2. Bij systeemgegevensuitwisseling van Zuyd systemen is het uitwisselen en gebruik van de Zuyd data uitsluitend toegestaan waar voor het initiële doel waarvoor de systeemeigenaar toestemming heeft gegeven bij het inrichten van de koppeling. (Control: NBA ID DM.01)
3. In beginsel wordt vanwege de uniformiteit alleen gebruik gemaakt van gegevensuitwisseling via de Zuyd Enterprise Service Bus (ESB). (Control: NBA ID DM.05)
4. De volgende technische maatregelen dienen ingericht te zijn voor systeemgegevensuitwisseling:
    a. Standaard dient een event driven of request response two-way Web-Based API gebruikt te worden voor elke integratie met Zuyd systemen; (Control: NBA ID DM.03, NBA ID DM.05, NBA ID ID.02, NBA ID ID.03, NBA ID SM.10)
    Kaders:
        i. zet message based overdracht van gegevens via API calls in;
        ii. tijdens de verwerking dient gebruik gemaakt te worden van veilige API's op basis waarvan additionele gegevens uit externe bronnen kunnen worden ingelezen en verwerkt; (Nora: SWP_U.12.01);
        iii. default REST/JSON API over HTTPS, met als alternatief SOAP over HTTPS of RESTXML over HTTPS;
        iv. application Programming Interface (API)-URL's geven geen gevoelige informatie, zoals de API-sleutel, sessie-tokens enz. weer; (Nora: SWP_U.12.02)
        v. er dient gebruik gemaakt te worden van veilige Application Programming Interfaces (API's), die (automatisch) gebruikersdata scheiden van applicatiecode, waarmee code injection kwetsbaarheden zoals Structured Query Language (SQL) injection, XML injection en Cross-Site Scripting (XSS) worden voorkomen; (Nora: SWP_U.12.03)
        vi. er dient gebruik gemaakt te worden van veilige Application Programming Interfaces (API's) die bufferlengtes controleren, waarmee kwetsbaarheden als Buffer- en Integer overflow worden voorkomen; (Nora: SWP_U.12.04)
        vii. alle data in transit moet met TLS (versie 1.2 of hoger) encryptie beveiligd zijn; (SURF SB.3.001)
        viii. mitigerende maatregelen m.b.t. de OWASP top tien (https://owasp.org/Top10/) inrichten en bijhouden;
        ix. alle gevoelige opgeslagen data (data at rest) dient versleuteld te zijn;
        x. voor authenticatie geldt dat standaard gebruik gemaakt wordt van een Identity Provider (IdP)-server via het OAuth 2.0 protocol op basis van certificaten, alleen als dit niet mogelijk dan met Client ID & Client Secret en als dat niet mogelijk is dan met Bearer tokens;

xi. gebruik IP Whitelist, indien mogelijk, om de toegang via API's tot systeemgegevens vanuit interne en externe systemen te beperken;
xii. verberg gevoelige informatie in alle beheerinterfaces die niet direct deel uitmaken van de applicatie waar de gegevens door beheerd worden;
xiii. (security)testen van API samenwerking met backend systemen;
xiv. gebruik JSON- of XML-schemavalidatie en controleer parameters zijn wat ze zouden moeten zijn (string, integer etc.) om SQL-injectie of XML-bom te voorkomen.

b. Als een two-way Web-API niet mogelijk is dan kan door de externe partij SFTP gebruikt worden in combinatie met een API integratie (ESB) met Zuyd systemen; (Control: NBA ID DM.03, NBA ID DM.05, NBA ID ID.02, NBA ID ID.03, NBA ID ID.05, NBA ID SM.10)
Kaders SFTP:
i. Default authenticatie via middels certificaten, met als alternatief gebruikersnaam/wachtwoord of;
ii. na vijf opeenvolgende foutieve inlogpogingen het SFTP account blokkeren;
iii. hosting van aparte SFTP Server op het Linux operating systeem uitsluitend door Zuyd Hogeschool per dienst;
iv. uitvoering van updates & onderhoud op het systeem (onderliggende operating systeem) en OpenSSH dient minimaal elke kalendermaand te geschieden;
v. de toegang is beperkt tot de noodzakelijk bestanden en mappen op de SFTP server benodigd voor de gegevensuitwisseling via de koppeling;
vi. de externe partij gebruikt een SFTP-client (SSH File Transfer Protocol)
vii. alleen het gebruik van AES encryptie middels aes128-ctr,aes192-ctr,aes256-ctr is toegestaan;
viii. minimale key length is 2048, waar mogelijk heeft een key length van 4096 de voorkeur;
ix. integriteitscontrole (Hash/MAC) is toegestaan gebruikmakend van SHA-2 hashfuncties, middels hmac-sha2-256,hmac-sha2-512;
x. SSH Host key algoritmes middels ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-rsa, ssh-dss;
xi. SSH Key uitwisseling algoritmes middels ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521;
xii. gebruik IP Whitelist, indien mogelijk, om de toegang via SFTP tot systeemgegevens vanuit interne en externe systemen te beperken;
xiii. herauthenticatie is vereist bij inactieve sessies langer dan 15 minuten;
xiv. verwijder de banner van het SFTP login scherm of pas deze aan zodat de gebruikte SFTP server versie niet gemeld wordt.

c. Mitigerende maatregelen m.b.t. de OWASP top tien (https://owasp.org/Top10/) inrichten en bijhouden; (Control: NBA ID SM.12)
d. Plan voor onmiddellijke upgrade/patch van de (third party) libraries aanwezig om bij kwetsbaarheden zo snel mogelijk te patchen; (Control: NBA ID SM.06)
e. Secure by design principes worden toegepast op de API en SFTP koppelingen en scripts
f. Beperk het aantal beheerders en verdeel de toegang in verschillende rollen; (Control: NBA ID ID.02, NBA ID.03, NBA OR.02)
g. Wachtwoordlengte van minimaal 16 karakters;
h. Wachtwoorden met encryptie salted hashed opslaan (SHA-2); (Control: NBA ID ID.01)
i. Wachtwoorden/tokens[1] jaarlijks vervangen; (Control: NBA ID ID.05)
j. Audit logs van publiek benaderbare systemen bevatten wel payload; (Control: NBA ID SM.04)

[1] Bij niet gebruikerstoepassingen (bijv. API) kan de gebruiker niet gevraagd worden voor MFA.

k. Reduceer audit log tot de minimaal benodigde informatie om de gebeurtenis vast te leggen; (Control: NBA ID SM.04)
l. Audit logs mogen geen persoonlijk identificeerbare gegevens bevatten tenzij deze geanonimiseerd worden via b.v. UUID; (Control: NBA ID DM.05)

5. Alle beveiligingsgebeurtenissen van applicaties (API/SFTP) die binnen Zuyd gefaciliteerd worden, worden via het Zuyd SIEM/SOC gemonitored. (Control: NBA ID SM.04)

6. Het is Zuyd Hogeschool toegestaan om vulnerability assessments en pentests t.a.v. de integratie systemen van de contractpartij(en) uit te voeren. (Control: NBA ID SM.07)

7. Er zijn binnen FB-ICT procedures aanwezig voor de systeemeigenaar om integraties ten behoeve van systeemgegevensuitwisseling met Zuyd systemen in te richten, wijzigen en beëindigen binnen Zuyd Hogeschool. (Control: NBA ID OR.01)

8. Er zijn binnen het CSIRT procedures voor het reageren op beveiligingsincidenten en inbreuken waarbij API's betrokken zijn, inclusief protocollen voor het melden en onderzoeken van incidenten en voor het nemen van passende corrigerende maatregelen. (Control: NBA ID SM.07)

9. Er zijn binnen het CSIRT procedures voor het regelmatig testen en evalueren van de beveiliging van API-integraties, inclusief het gebruik van kwetsbaarheidsscans en andere tools om potentiële beveiligingsrisico's te identificeren en aan te pakken. (Control: NBA ID SM.05)

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