Zuyd Security Bbueleid – E-mail

Versie 1.2

Vastgesteld door het CvB op 21-10-2025

Inhoudsopgave

1. Documentenbeheer

Revisiehistorie

Revisiedatum	Samenvatting veranderingen	Door	Versie
15-01-2023	Draft versie	D. Heynen	0.1
28-06-2023	Verder uitwerking/verdieping	D. Heynen	0.3
12-09-2023	Verwerking review opmerkingen FB&ICT, Juridische afdeling, FG&PO.	D. Heynen	0.95
02-10-2023	Concept versie voor CvB met alle opmerkingen incl IM verwerkt.	D. Heynen	0.96
16-01-2024	Zuyd Security Beleid Website vastgesteld door CvB.	R. Sterken	1.0
09-09-2025	Minor Update, template Zuyd, url koppelingen, tekstuele aanpassing.	D. Heynen	1.1
21-10-2025	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

Jaarlijkse vaststelling

Dit document is vastgesteld door:

Naam	Uitgiftedatum	Versie
CvB	21 oktober 2025	1.2

2. Managementsamenvatting

Communicatie is een belangrijk onderdeel van elk bedrijf en organisatie, dit geschiedt via een aantal communicatiekanalen waarvan het e-mail kanaal er een is. Het is echter ook een bron van informatiebeveiligingsrisico's zoals: het onderscheppen van informatie die tussen twee partijen wordt uitgewisseld, of het onbedoeld binnenhalen van ransomware. Om de risico's te beperken is het belangrijk om een informatiebeveiligingsbeleid te hebben dat specifiek gericht is op e-mail communicatie.

Dit beleid beschermt informatie van Zuyd tegen ongeoorloofde toegang of wijziging bij het verzenden of ontvangen via e-mail. Tevens beschrijft dit beleid de regels en richtlijnen voor het gebruik van het e-mail communicatiekanaal, evenals de maatregelen die worden genomen om de **beschikbaarheid, integriteit** en **vertrouwelijkheid** van de informatie te waarborgen.

In grote lijn betekent dit voor de Zuyd medewerkers (waaronder extern/inhuur) en studenten tijdens het gebruiken van het e-mail communicatiekanaal het volgende:

- Alle zakelijke communicatie dient te verlopen via het verstrekte Zuyd e-mailadres. Gebruik geen privé e-mailadressen of andere persoonlijke contactgegevens voor zakelijke doeleinden.
- Het geautomatiseerd doorsturen van Zuyd e-mail naar externe e-mail adressen is niet toegestaan.
- Het is toegestaan om e-mails en bijlagen zelfstandig door te sturen, maar gebruikers dienen ervoor te zorgen dat vertrouwelijke informatie uitsluitend wordt gedeeld met personen die daar recht op hebben.
- Gebruik van een (gedeelde) Zuyd e-mailbox kan alleen via het eigen Zuyd account.

3. Zuyd Security Beleid – E-mail

3.1. Inleiding

Het e-mail beleid gaat over hoe e-mail communicatie van Zuyd wordt beschermd. Dit kan bijvoorbeeld betrekking hebben op het voorkomen van spam en phishing, koppeling met (SaaS) systemen, encryptie bij gevoelige informatie en het gebruik van authenticatie bij het verzenden van e-mails naar het internet.

Communicatie is een belangrijk onderdeel van elk bedrijf en organisatie. Het is echter ook een potentiële bron van beveiligingsrisico's zoals: het onderscheppen van informatie die tussen twee partijen wordt uitgewisseld bij het gebruikmaken van e-mails. Om de risico's te beperken is het belangrijk om een beveiligingsbeleid te hebben dat specifiek gericht is op e-mail communicatie. Dit beleid moet ervoor zorgen dat deze communicatie van Zuyd veilig is en dat de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie wordt beschermd. In dit beleid worden de richtlijnen beschreven voor het gebruik van, en koppeling met, Zuyd e-mail systemen, en de procedure voor incidenten die betrekking hebben op de beveiliging van deze vorm van communicatie.

3.2. Relatie tot SURF CMM Toetsingskader

Dit beleid is gekoppeld aan de uitgangspunten in het SURF Audit Toetsingskader[1]. SURF schrijft: "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.03, DM.05, SM.01,, SM.04, SM.05, SM.07, SM.10, SM.11 en SM.12) maar dient met name als een uitwerking van de beheers doelstelling **NBA ID: SM.01 en SM.12** in het domein ***Security 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 de baseline van het informatiebeveiligingsbeleid van Zuyd beschrijft.
- Privacybeleid Zuyd Hogeschool
  - Het document dat het privacybeleid van Zuyd beschrijft.
- Regeling ICT Gebruik
  - Artikel 5 – Gebruik van e-mail.

3.4. Doel

Dit beleid is opgesteld met als doel Zuyd informatie te beschermen tegen ongeoorloofde toegang of wijziging als deze via het communicatiekanaal e-mail wordt verzonden of ontvangen. Dit beleid beschrijft de regels en richtlijnen voor het gebruik van het e-mail communicatiekanaal, evenals de maatregelen die worden genomen om de **beschikbaarheid, integriteit** en **vertrouwelijkheid** van de informatie te waarborgen.

3.5. Scope

Dit document bevat beleidsregels voor het versturen en ontvangen van (Zuyd) informatie (Zuyd-data) via e-mail door medewerkers (inclusief externen en ingehuurd personeel) en studenten van Zuyd.

3.6. Beleid

Bij het gebruik van het e-mail communicatiekanaal dienen buiten de richtlijnen zoals vastgelegd in het document Baseline Informatiebeveiliging ook de volgende richtlijnen te worden toegepast:

- Bij alle e-mail communicatie van Zuyd wordt uitsluitend gebruikgemaakt van het centrale Zuyd e-mail systeem. Dit geldt ook voor SaaS oplossingen.
- Het @zuyd.nl domein moet als uitgangspunt gebruikt worden als verzendadres.
- Om activiteiten van gebruikers te kunnen traceren naar uniek identificeerbare gebruikers verloopt toegang tot de (gedeelde) mailbox altijd via het persoonlijke Zuyd account.
- Er worden geen inloggegevens voor toegang tot de gedeelde mailbox verstrekt.
- Gebruik voor je werk (of studie) alleen het e-mailaccount dat door Zuyd is verstrekt. Het gebruik van andere e-mail systemen voor zakelijke doeleinden dan het Zuyd e-mail systeem is niet toegestaan.
- Binnen het Zuyd netwerk is het niet toegestaan om (koppelingen naar) eigen e-mail servers op te zetten, in te richten of te gebruiken.
- Het geautomatiseerd doorsturen van Zuyd e-mail naar externe e-mail adressen is niet toegestaan.
- Het gebruiken van de webapplicatie/hosting platform als (bulk)mail (relay) systeem voor domeinen van Zuyd is, omdat dat niet aansluit bij het beheersen van gegevensstromen en systemen, niet toegestaan.
- Het gebruik van het Zuyd e-mail systeem voor bulk e-mails is, omdat dat niet aansluit bij het beheersen van gegevensstromen en systemen, niet toegestaan.
- Versturen van bulk e-mail mag uitsluitend met goedkeuring van M&C en de door hen aangewezen kanalen.
- Vertrouwelijke geclassificeerde informatie en persoonsgegevens mogen niet verstuurd worden via e-mail. Gebruik hiervoor geschikte alternatieven zoals SURFfilesender.
- Bij verspreiden van documenten via de e-mail dient dit bij voorkeur te gebeuren door een link naar documenten te delen in de bewuste e-mail. Dit is veiliger dan het versturen van documenten als bijlage bij een e-mail.
- De volgende technische maatregelen dienen ingericht te zijn op systemen (dat geldt zowel voor Zuyd systemen als SaaS oplossingen) die worden gebruikt voor e-mail communicatie:

    Kaders:

    i. Er is bescherming in de mailflow (inkomend en uitgaand) van e-mails tegen phishing en malware;
    ii. SMTP verbindingen worden beveiligd met SPF, DKIM en DMARC;
    iii. SMTP verbindingen zijn versleuteld met TLS. Het gebruik van STARTTLS (waarmee een versleutelde verbinding geforceerd wordt als deze onversleuteld is) wordt gedoogd;
    iv. Het gebruik van de Zuyd SMTP relay is alleen toegestaan door FB-ICT geautoriseerde systemen (dat geldt zowel voor Zuyd systemen als SaaS oplossingen);
    v. Bij e-mail communicatie dient de informatie voorzien te zijn van encryptie in transit;
    vi. Het gebruik van andere domeinen dan de Zuyd domeinen voor het versturen van e-mail berichten met Zuyd data is niet toegestaan.

- De systeemeigenaar beperkt het aantal beheerders en verdeelt daarbij de toegang in verschillende rollen.
- Realtime monitoren en managen van securitybeveiligingsgebeurtenissen van Zuyd e-mail systemen verloopt via het Zuyd SIEM/SOC.
- Er is een procedure voor het reageren op informatiebeveiligingsincidenten en inbreuken waarbij e-mail en Zuyd e-mail systemen betrokken zijn, inclusief protocollen voor het melden en onderzoeken van incidenten en voor het nemen van passende corrigerende maatregelen.
- Er zijn procedures voor het regelmatig testen en evalueren van de beveiliging van Zuyd e-mail systemen, inclusief het gebruik van kwetsbaarheidsscans en andere tools om potentiële beveiligingsrisico's te identificeren en aan te pakken.

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