Zuyd Security Beleid – E-mail

Zuyd Hogeschool

Versie 1.0

Vastgesteld door het CvB
op 16-01-2024

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

Documentatie

Er is gebruik gemaakt van de onderstaande informatie

Naam	Auteur	Status
Informatiebeveiligingsbeleid Zuyd Hogeschool versie 2023	CISO Zuyd Hogeschool	Definitief
Normenkader Informatiebeveiliging versie 2.0 (SURF)	Alf Moens	Definitief

Goedkeuringen

Dit document is goedgekeurd door:

Naam	Uitgiftedatum	Versie
CvB	16-01-2024	1.0

2. Management Summary

Communicatie is een belangrijk onderdeel van elk bedrijf en organisatie, dit geschiedt via een aantal communicatiekanalen waarvan het e-mail kanaal er een is van is. 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, of het onbedoeld binnenhalen van ransomware. Om de risico's te beperken is het dus belangrijk om een beveiligingsbeleid te hebben dat specifiek gericht is op e-mail communicatie.

Dit beleid is opgesteld om 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.

In grote lijn betekent dit voor de Zuyd gebruiker (medewerker en student) van het e-mail communicatiekanaal het volgende:

- voor alle zakelijke uitingen wordt het Zuyd e-mailadres gebruikt;
- autoforward is niet mogelijk vanaf het Zuyd e-mailadres;
- zelfstandig doorsturen van bijlagen is mogelijk, maar gebruikers wordt geadviseerd om goed na te denken over de vertrouwelijkheid van de data;
- 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 daarnaast 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 procedures voor incidenten die betrekking hebben op de beveiliging van deze vorm van communicatie.

3.2. Relatie tot andere beleidsstukken

Dit beleid is gekoppeld aan de uitgangspunten in het SURF Audit Toetsingskader[1]. "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 beheers doelstellingen uit dit kader (te weten: NBA ID: ID.01, NBA ID: ID.02, NBA ID: ID.03, NBA ID: DM.03, NBA ID: DM.05, NBA ID: SM.01, NBA ID: SM.04, NBA ID: SM.07, NBA ID: SM.10, NBA ID: SM.11 en NBA ID: SM.12) maar dient met name als een uitwerking van de beheers doelstelling **NBA ID: SM.12 en NBA ID: SM.01** 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.
- Privacybeleid Zuyd Hogeschool
    - Het document dat het privacybeleid van Zuyd beschrijft.

3.4. Doel

Dit beleid is opgesteld om 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

De beleidsuitgangspunten in dit document hebben betrekking op het door Zuyd gebruikers (medewerkers en studenten) versturen en ontvangen van (Zuyd) informatie gebruikmakend van het e-mail communicatiekanaal.

3.6. Beleid

Bij het gebruik van het e-mail communicatiekanaal gelden de volgende security richtlijnen:

1. Bij alle e-mail communicatie van Zuyd wordt uitsluitend gebruikgemaakt van het centrale Zuyd e-mail systeem. Dit geldt ook voor SaaS oplossingen. (Control: NBA ID: ID.01)
2. Het @zuyd.nl domein moet als uitgangspunt gebruikt worden als verzendadres. (Control: NBA ID: ID.01)
3. Om activiteiten van gebruikers te kunnen traceren naar uniek identificeerbare gebruikers verloopt toegang tot de (gedeelde) mailbox altijd via het persoonlijke Zuyd account. (Control: NBA ID: ID.01)
4. Er worden geen inloggegevens voor toegang tot de gedeelde mailbox verstrekt. (Control: NBA ID: ID.01)
5. 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. (Control: NBA ID: ID.01)
6. Binnen het Zuyd netwerk is het niet toegestaan om (koppelingen naar) eigen e-mail servers op te zetten, in te richten of te gebruiken. (Control: NBA ID: DM.05)
7. Het geautomatiseerd doorsturen van Zuyd e-mail naar externe e-mail adressen is niet toegestaan. (Control: NBA ID: DM.03)
8. Vertrouwelijke geclassificeerde informatie en (bijzondere) persoonsgegevens mogen niet verstuurd worden via e-mail. Gebruik hiervoor geschikte alternatieven zoals SURFfilesender. (Control: NBA ID: DM.05)
9. Bij verspreiden van documenten via de e-mail dit bij voorkeur doen 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. (Control: NBA ID: DM.05)
10. 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; (Control: NBA ID: SM.11)
    ii. SMTP verbindingen worden beveiligd met SPF, DKIM en DMARC; (Control: NBA ID: SM.12)
    iii. SMTP verbindingen maken gebruik van STARTTLS of beter; (Control: NBA ID: SM.12)
    iv. Het gebruik van de Zuyd SMTP relay is alleen toegestaan aan daarvoor geautoriseerde systemen (dat geldt zowel voor Zuyd systemen als SaaS oplossingen); (Control: NBA ID: SM.12)
    v. Bij e-mail communicatie dient de informatie voorzien te zijn van encryptie in transit; (Control: NBA ID: SM.10)
    vi. Het gebruik voorkomen van andere domeinen dan de Zuyd domeinen voor het versturen van e-mail berichten. (Control: NBA ID: ID.01)
11. De systeemeigenaar beperkt het aantal beheerders en verdeel de toegang in verschillende rollen. (Control: NBA ID ID.02, NBA ID.03, NBA OR.02)
12. Realtime monitoren en managen van beveiligingsgebeurtenissen van Zuyd e-mail systemen verloopt via het Zuyd SIEM/SOC. (Control: NBA ID SM.04)

13. Er zijn procedures voor het reageren op beveiligingsincidenten 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. (Control: NBA ID: SM.07)
14. 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. (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.