Hanze

Kader Informatiebeveiliging en privacy

2026 - 2031

share your talent. move the world.

Inhoudsopgave

1. Inleiding 4
1.1. Context 4
1.2. Doel 4
1.3. Reikwijdte en toepassingsgebied 4
1.4. Definities en afkortingen 4
2. Context 5
2.1. De Hanze en haar context [4.1] 5
2.2. De behoefte en verwachtingen van belanghebbenden [4.2] 5
2.3. De reikwijdte van het ISMS [4.3] 5
3. Management 6
3.1. Uitgangspunten van ons kader [5.2] 6
3.2. Privacy beginselen 6
3.3. Privacy verplichtingen 7
4. Structuur van Hanze kader 9
4.1. Betrokkenheid, leiderschap en verantwoordelijkheden [5.1, 5.2, 5.3] 9
4.1.1. Betrokkenheid en leiderschap [5.1, 5.2] 9
4.1.2. Rollen en verantwoordelijkheden [5.3] 9
4.1.3. Three lines 9
5. Risicomanagement 10
5.1. ISMS-risico's en (bij)sturing door management [6.1, 8.1, 9.1] 10
5.2. Operationeel risicomanagement [6.2, 8.2, 8.3] 10
6. Mensen en middelen 11
6.1. Middelen voor informatiebeveiliging en privacy [7.1] 11
6.2. Kennis en competenties [7.2, 7.3] 11
6.3. Documentatie en communicatie [7.4, 7.5] 11
7. Continue verbeteren 12
7.1. Audits en compliance monitoring [9.2] 12
7.2. Directiebeoordeling en strategische evaluatie [9.3] 12
7.3. Afwijkingen en corrigerende maatregelen [10.1, 10.2] 12
8. Bijlages 13
8.1. Beleidspiramide 13

Documentinformatie

Dit document maakt onderdeel uit van een complete set (piramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag kaders in de beleidspiramide.

Datum	07-03-2025
Goedkeuring verantwoordelijke	
Auteur	Gert Douma en Michel Boot
Verantwoordelijke	Catrinus van der Meer
Versie	1.0
Classificatie	Publiek

Versiebeheer

Versie	Auteur	Datum	Wijziging
0.5	Gert Douma en Michel Boot	07-03-2025	Aanpassingen rollen en taken en juiste benaming documenten
0.6	Erik Post	16-04-2025	Review
0.6	Catrinus van der Meer	25-04-2025	Opmerkingen over ISMS en managementsysteem
1.0	Gert Douma en Erik Post	24-06-2025	Aanpassingen doorgevoerd

Distributielijst

Versie	Datum	Ontvanger	Doel
0.6	25-04-2025	Catrinus van der Meer	Review en goedkeuring
1.0	08-07-2025	MT INF	Review en accordering

Samenhang met andere documenten

Naam	Bovenliggend	Gelijk niveau	Onderliggend
Rollen- en taken			x
Alle regelingen rondom informatiebeveiliging en privacy			x
Samenwerken aan kwaliteit	x		
Integrale veiligheid en Crisisplan		x	
Kader Risicomanagement		x	

Verwijzingen naar NBA en ISO27001

Kader	Verwijzing (tags)
NBA	GO.01
ISO27001:2023	4.1; 4.2; 4.3; 5.1; 5.2; 5.3; 6.1; 6.2; 7.1; 7.2; 7.3; 7.4; 7.5; 8.1; 8.2; 8.3; 9.1; 9.2; 9.3; 10.1; 10.2 In de tekst staan de verwijzingen als […]

1. Inleiding

1.1. Context

Dit document beschrijft het kader informatiebeveiliging en privacy van de Hanze vanaf datum ondertekening door College van Bestuur en vervangt hiermee het voorgaande privacy- en securitybeleid 2021-2025.

Dit Kader informatiebeveiliging en privacy, gebaseerd op NEN-ISO/IEC 27001:2022, stelt kaders en geeft richting. Op tactisch en operationeel niveau is dit kader aangevuld met onderwerp specifieke documenten (regelingen, processen en procedures).

1.2. Doel

De Hanze zet met dit Kader informatiebeveiliging en privacy een volgende stap in het versterken van de cyberweerbaarheid, groei in het volwassenheidsniveau en in het beschermen van informatie en persoonsgegevens. Hiermee borgen we een veilige leer- en werkomgeving voor onze studenten, medewerkers, docenten en onderzoekers. Het belang hiervan is groot met de snelle evolutie in technologie, veranderende dreigingslandschappen en de toenemende complexiteit van wettelijke vereisten.

1.3. Reikwijdte en toepassingsgebied

Bij de Hanze wordt informatieveiligheid breed geïnterpreteerd. Het heeft betrekking op alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie), die de Hanze of haar relaties genereren en beheren.

Het kader is tijd- en locatie-onafhankelijk en geldt dus 24x7 ook als men op een andere locatie dan op het terrein van onze instelling met informatie of informatievoorziening van onze instelling werkt, zoals thuis, in de trein, bij een andere organisatie of tijdens reizen naar het buitenland.

1.4. Definities en afkortingen

CvB	College van Bestuur
FAIR	Findable (vindbaar), Accessible (toegankelijk), Interoperable (interoperabel), Reusable (herbruikbaar)
ISMS	Information Security Management System is het raamwerk van beleid, kaders, regelingen, processen, procedures en controles waarmee een organisatie haar doelstellingen op een gestructureerde en controleerbare manier bereikt.
Informatiebeveiliging/ Security	Geheel van maatregelen en processen die zijn ontworpen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen.
Privacy	Recht van individuen om controle te hebben over hun persoonlijke informatie en hoe deze informatie wordt verzameld, gebruikt, gedeeld en beschermd.
Beschikbaarheid	Zorgt ervoor dat informatie, systemen en processen toegankelijk zijn en gebruik kunnen worden wanneer dat nodig is.
Integriteit	Waarborgt de nauwkeurigheid en volledigheid van informatie en de verwerkingsmethoden.
Vertrouwelijkheid	Zorgt ervoor dat informatie alleen toegankelijk is voor geautoriseerde personen en niet worden onthuld aan onbevoegde individuen, entiteiten of processen.
GRC-applicatie	Applicatie die instellingen helpt bij het beheren van hun governance, risico's en nalevingsverplichtingen.

2. Context

2.1. De Hanze en haar context [4.1]

De visie van Hanze is gericht op het maken van een impact op de wereld door de kracht van de regio te versterken en mensen te ondersteunen in hun levenslange ontwikkeling. Daarnaast wordt onderzoek en onderwijs veelal verricht op basis van publieke financiering hetgeen vraagt om transparantie en zorgvuldigheid van onze bedrijfsvoering. Diezelfde transparantie wordt verwacht ten aanzien van onderzoeksdata op basis van het FAIR-principe (Findable, Accessible, Interoperable, Reusable). Tegelijkertijd verwachten onderzoekspartners en bedrijven waar we mee samenwerken dat hun informatie vertrouwelijk wordt behandeld. Op basis van het cyberdreigingsbeeld bevat dit kader de uitgangspunten voor zowel informatiebeveiliging als privacy om daarmee een bijdrage te leveren aan de kennisveiligheid binnen onze instelling en het ecosysteem waarin wij ons bevinden. Dit document vormt de basis om eisen aan de beschikbaarheid, integriteit en vertrouwelijkheid van processen, informatie en systemen te realiseren.

2.2. De behoefte en verwachtingen van belanghebbenden [4.2]

De verwachtingen zijn afhankelijk van de rol van de belanghebbenden.

- Medewerkers verwachten een omgeving waarin de data en systemen voor het werk betrouwbaar en veilig zijn en waarin hun privacy geborgd is.
- Studenten verwachten een omgeving waarin de data en systemen voor de studie betrouwbaar en veilig zijn en waarin hun privacy geborgd is.
- Onderwijsinstellingen, onderzoekspartners en stagebedrijven verwachten een vertrouwelijke en betrouwbare omgang met hun informatie en onderzoeksdata. Daarnaast mag onze omgeving geen bron vormen voor eventuele malafide activiteiten.
- Respondenten en andere deelnemers aan onze onderzoeken verwachten dat hun gegevens veilig zijn en hun privacy geborgd is.
- Het Ministerie van OCW verwacht dat ons bestuur controle heeft over de staat van de informatiebeveiliging en in staat is om daar in detail over te rapporteren.
- Koepelorganisaties verwachten dat we gezamenlijk in staat zijn om als sector een veilig ecosysteem te realiseren.

Deze verwachtingen vormen de basis voor een correcte classificatie van data (en/of informatie) om vervolgens bijpassende technische, fysieke, mensgerichte en/of organisatorische maatregelen te kunnen toepassen.

2.3. De reikwijdte van het ISMS [4.3]

Het Information Security Management System (ISMS) omvat alle aspecten van informatieveiligheid in de processen van onderwijs, onderzoek, bedrijfsvoering en alle daaruit voortvloeiende activiteiten die namens en/of voor de Hanze worden uitgevoerd.

Bij de Hanze wordt informatieveiligheid breed geïnterpreteerd. Het heeft betrekking op alle vormen van formeel vastgelegde informatie (dus niet alleen digitale informatie), die onze instelling of haar relaties genereren en beheren.

Het beleid is tijd- en locatie-onafhankelijk en geldt dus 24x7 ook als men op een andere locatie dan op het terrein van onze instelling met informatie of informatievoorziening van onze instelling werkt, zoals thuis, in de trein, bij een andere organisatie of tijdens reizen naar het buitenland.

3. Management

3.1. Uitgangspunten van ons kader [5.2]

Centraal uitgangspunt van ons kader zijn de gebruikers van onze informatie en systemen. Om de beschikbaarheid, integriteit en vertrouwelijkheid te borgen hanteren we de volgende uitgangspunten binnen de Hanze:

1. Werken we risicogebaseerd
We baseren de te treffen maatregelen op de mogelijke veiligheidsrisico's van onze gegevens, processen, informatievoorzieningen en -systemen.

2. Is iedereen verantwoordelijk
Iedereen is verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

3. Wordt het Kader informatiebeveiliging en privacy altijd en overal gevolgd
Informatiebeveiliging zit in het DNA van onze instelling en is integraal onderdeel van al onze werkzaamheden.

4. Hanteren we Security by Design
Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering van onze gegevens, processen, informatievoorzieningen en -systemen.

5. Hanteren we Security by Default
Informatievoorzieningen en -systemen standaard zijn geconfigureerd met de meest veilige instellingen.

6. Heeft iedereen toegang tot alleen dat wat nodig is
Gebruikers hebben alleen toegang tot gegevens, processen, informatievoorzieningen en -systemen die zij nodig hebben voor hun werkzaamheden.

7. Gaan we uit van controle in plaats van blind vertrouwen
We hanteren een gelaagd beveiligingsmodel waarbij we verifiëren of aan voorwaarden voor toegang tot en het gebruik van gegevens, processen, informatievoorzieningen en -systemen is voldaan.

3.2. Privacy beginselen

De Hanze is zich bewust van het belang van privacy en werkt hierbij volgens de beginselen van de Algemene Verordening Gegevensbescherming (hierna: AVG):

1. Rechtmatigheid, behoorlijkheid en transparantie
Verwerkingen moeten gebaseerd zijn op een rechtmatige grondslag, mogen niet nadelig, discriminerend, onverwacht of misleidend zijn voor betrokkenen en hierover moet open en duidelijk gecommuniceerd worden. Hierbij wordt onder andere rekening gehouden met de wettelijke taken die hogescholen hebben op basis van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

2. Doelbinding
De Hanze verzamelt alleen gegevens voor een gerechtvaardigd doel dat specifiek is en vooraf uitdrukkelijk wordt omschreven. Verwerking van deze gegevens gebeurt dan ook alleen met hetzelfde doel als die waarvoor ze verzameld zijn of een doel dat daarmee verenigbaar is.

3. Dataminimalisatie
Bij het verwerken van gegevens houdt de Hanze zich aan het principe: 'zo min mogelijk'. De Hanze verwerkt in ieder geval niet meer gegevens dan nodig om het doel van de verwerking te bereiken.

4. Juistheid
De Hanze zorgt ervoor dat de gegevens binnen de organisatie juist zijn. Om dat te bewerkstelligen worden gegevens geactualiseerd indien nodig en worden betrokkenen geïnformeerd over hun rechten met betrekking tot hun gegevens zoals het rectificeren daarvan.

5. Opslagbeperking

Bij het opslaan van gegevens wordt rekening gehouden met bewaartermijnen. De Hanze volgt hierbij in eerste instantie de Selectielijst voor hogescholen die is opgesteld op basis van de Archiefwet 1995. Hierdoor voldoet de Hanze aan de wettelijke verplichtingen en wordt het informatiebeheer zo efficiënt mogelijk georganiseerd. Verder bewaart de Hanze gegevens niet langer dan nodig om het doel te bereiken waarvoor deze zijn verzameld, zoals de AVG voorschrijft.

6. Vertrouwelijkheid en integriteit

De Hanze gaat verantwoordelijk om met persoonsgegevens. Gegevensverwerkingen worden dan ook goed beveiligd, waarbij rekening wordt gehouden met de strengere regels voor bijzondere persoonsgegevens.

7. Verantwoordingsplicht

De Hanze is verantwoordelijk voor de naleving van de AVG en zijn beginselen. Dit kan worden aangetoond door het documenteren van het Kader informatiebeveiliging en privacy en verdere documentatie betreffende (persoons)gegevensverwerkingen. Een voorbeeld hiervan is het register van verwerkingen.

3.3. Privacy verplichtingen

De Hanze houdt rekening met de verplichte maatregelen uit de AVG om te voldoen aan zijn verantwoordingsplicht. Hierbij houdt de Hanze zich allereerst aan de algemene verplichting om passende technische en organisatorische maatregelen te nemen om te verzekeren en aan te kunnen tonen dat de gegevens worden verwerkt in overeenstemming met de AVG. Verder houdt de Hanze zich aan de volgende verplichtingen:

1. Privacy by design en by default

Bescherming van persoonsgegevens is bij de ontwikkeling van dit Kader informatiebeveiliging en privacy meegenomen en ingebouwd. Bij de ontwikkeling van nieuwe systemen worden standaardinstellingen zodanig gekozen dat de bescherming van persoonsgegevens wordt verzekerd.

2. Registerplicht

De Hanze legt alle processen waarin persoonsgegevens verwerkt vast in een verwerkingsregister en deze kan worden aangetoond.

3. Gegevensbeschermingseffectbeoordeling

Als de Hanze voornemens is een verwerking uit te voeren die ‘een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen’ wordt op deze verwerking eerst een gegevensbeschermingseffect-beoordeling (data protection impact assessment: DPIA) uitgevoerd. Hierdoor kunnen de effecten op betrokkenen worden bepaald en beoordeeld.

4. Functionaris voor gegevensbescherming

De Hanze heeft een functionaris voor gegevensbescherming aangesteld die intern toezicht houdt op de gegevensverwerkingen binnen de Hanze en adviseert over toepassing en naleving van de AVG.

5. Meldplicht en registerplicht datalekken

De Hanze meldt een datalek aan de toezichthoudende autoriteit, de Autoriteit Persoonsgegevens, als het waarschijnlijk is dat de inbreuk risico’s voor de rechten en vrijheden van natuurlijke personen met zich meebrengt. Verder houdt de Hanze een datalekregister bij waarin ook datalekken worden meegenomen die niet gemeld hoeven te worden.

6. Privacyverklaring

De Hanze heeft verschillende privacyverklaringen opgesteld waaruit blijkt welke persoonsgegevens de Hanze verwerkt en waarom.

7. Overeenkomsten

Voor de uitwisseling van persoonsgegevens met derden sluit de Hanze de nodige verwerkers- danwel gegevensuitwisselingsovereenkomsten. Als deze uitwisseling plaatsvindt met betrekking tot een land buiten de Europese Economische Ruimte (derde landen) draagt de Hanze er zorg voor dat aan de vereisten van de AVG wordt voldaan.

8. Betekenis voor privacyrechten

De Hanze draagt er zorg voor dat gehoor kan worden gegeven aan betrokkenen die een beroep doen op hun privacyrechten uit de AVG. De systemen, processen en interne organisatie worden daarom mede ingericht op deze privacyrechten.

4. Structuur van Hanze kader

De structuur van ons kader is opgebouwd in vier lagen (zie Bijlage 1 Beleidspiramide). De bovenste laag is het kader informatiebeveiliging en privacy en is beschreven in dit document. Verdere specificering van het Kader informatiebeveiliging en privacy is vastgelegd in de onderliggende standaarden, regelingen en procedures.

4.1. Betrokkenheid, leiderschap en verantwoordelijkheden [5.1, 5.2, 5.3]

4.1.1. Betrokkenheid en leiderschap [5.1, 5.2]

Het College van Bestuur (CvB) toont leiderschap en betrokkenheid door ervoor te zorgen dat het kader informatiebeveiliging en privacy en de doelstellingen in lijn zijn met de strategische richting van de Hanze. De eisen van het managementsysteem worden geïntegreerd in de processen van onderwijs, onderzoek en bedrijfsvoering, en hiervoor zijn de benodigde middelen beschikbaar gesteld. Het CvB communiceert het belang van effectieve informatiebeveiliging en privacy, zorgt dat de doelstellingen worden behaald, ondersteunt medewerkers in hun bijdragen aan het systeem, bevordert continue verbetering en spreekt andere managementrollen aan op hun verantwoordelijkheden.

4.1.2. Rollen en verantwoordelijkheden [5.3]

Het CvB draagt er zorg voor dat er binnen de Hanze duidelijkheid bestaat over verantwoordelijkheden en bevoegdheden van rollen met betrekking tot informatiebeveiliging en privacy. Het CvB kent de verantwoordelijkheden en bevoegdheden toe voor het waarborgen van de naleving van het kader informatiebeveiliging en privacy en voor het rapporteren over de prestaties ervan. Dit wordt nader beschreven in de regeling: Rollen en taken Privacy en Security.

4.1.3. Three lines

Het CvB zorgt ervoor dat duidelijke lijnen van verantwoordelijkheid zijn vastgesteld. Binnen de Hanze wordt ‘Three lines’ gehanteerd voor effectieve controle en governance van informatiebeveiliging en privacy. Dit is beschreven in het beleidsdocument ‘Samen werken aan kwaliteit’. Binnen deze structuur is de eerste lijn verantwoordelijk voor operationeel management en daarmee de toepassing van de standaarden en voor informatiebeveiliging. De tweede lijn voorziet de eerste lijn van een passend en uitvoerbaar kader informatiebeveiliging en privacy en ondersteunt het risicomanagementproces. De derde lijn is verantwoordelijk voor interne audits.

5. Risicomanagement

5.1. ISMS-risico’s en (bij)sturing door management [6.1, 8.1, 9.1]

Het CvB neemt bij het inrichten van het managementsysteem voor informatiebeveiliging en privacy zowel de in- als externe context in overweging (hoofdstuk 2). Hierbij worden risico's en kansen geïdentificeerd om de beoogde resultaten te behalen en ongewenste effecten te voorkomen of te verminderen, met als doel voortdurende verbetering te realiseren. We nemen concrete acties om de geïdentificeerde risico's en kansen aan te pakken en bepalen hoe we deze in onze processen integreren, implementeren en evalueren. Daarnaast definiëren en passen we een procedure toe voor de behandeling van informatiebeveiligings- en privacyrisico's. Dit omvat het selecteren van passende opties voor risicobehandeling, het vaststellen van beheersmaatregelen en het verkrijgen van goedkeuring van risico-eigenaren volgens het Kader Risicomanagement.

5.2. Operationeel risicomanagement [6.2, 8.2, 8.3]

Het CvB stelt informatiebeveiligings- en privacy doelstellingen vast die voortvloeien uit dit Kader informatiebeveiliging en privacy, die meetbaar zijn, en rekening houden met geldende eisen en risicobeoordelingen. We monitoren, communiceren, actualiseren en documenteren deze doelstellingen.

Bij het opstellen van plannen, ontwikkelen of aanpassen van processen bepalen we wat er moet gebeuren, welke middelen nodig zijn, wie verantwoordelijk is, wanneer acties zijn voltooid en hoe resultaten worden geëvalueerd.

De Hanze voert periodiek, en altijd bij belangrijke wijzigingen, risicobeoordelingen uit op het gebied van informatiebeveiliging en privacy. Hierbij wordt rekening gehouden met vooraf vastgestelde criteria voor risicobeoordeling en -acceptatie. De uitkomsten van deze beoordelingen worden gedocumenteerd vastgelegd.

Ook implementeert de Hanze het risicobehandelingsplan voor zowel informatiebeveiliging als privacy en bewaren we gedocumenteerde informatie over de resultaten van de risicobehandeling volgens de regeling Data Protection Impact Assessment

6. Mensen en middelen

6.1. Middelen voor informatiebeveiliging en privacy [7.1]

Het CvB bepaalt en maakt de middelen (systemen, processen en budgetten) beschikbaar die nodig zijn voor het opzetten, implementeren, onderhouden en voortdurend verbeteren van het managementsysteem voor informatiebeveiliging en privacy en voor het uitvoeren van dit Kader informatiebeveiliging en privacy.

6.2. Kennis en competenties [7.2, 7.3]

De Hanze identificeert de vereiste vaardigheden (competenties en bewustzijn) voor in- en externe medewerkers die taken uitvoeren die de beschikbaarheid, integriteit en/of vertrouwelijkheid beïnvloeden. We waarborgen dat deze medewerkers bekwaam zijn, onder andere op basis van het bewustwordings- en opleidingsplan. Indien nodig ondernemen we stappen om de benodigde vaardigheden te ontwikkelen en evalueren we de doeltreffendheid van deze inspanningen.

Medewerkers die werkzaamheden verrichten namens, voor en/of binnen de Hanze dienen zich bewust te zijn van het Kader informatiebeveiliging en privacy, hun rol bij het bevorderen van de doeltreffendheid van het information security managementsysteem (ISMS) en de consequenties van het niet naleven van de eisen van dit managementsysteem.

6.3. Documentatie en communicatie [7.4, 7.5]

Het managementsysteem voor informatiebeveiliging van de Hanze omvat onder andere documentatie behorende bij dit beleidsdocument en andere informatie die de organisatie nodig acht voor de effectiviteit van het managementsysteem.

Bij het creëren en bijwerken van deze documentatie zorgt de Hanze ervoor dat elk stuk een duidelijke identificatie en beschrijving heeft, inclusief een titel, datum, auteur of referentienummer en in het juiste format en medium is opgesteld. Verder worden ze beoordeeld en goedgekeurd op geschiktheid en volledigheid.

Gedocumenteerde informatie, zoals het managementsysteem voor informatiebeveiliging en privacy, en relevante documenten, is actueel, beschikbaar en wordt adequaat beveiligd tegen verlies van vertrouwelijkheid, ongeoorloofd gebruik en manipulatie.

Het beheer van deze documentatie omvat verschillende activiteiten waaronder distributie, toegang, opslag, behoud, beheersing van wijzigingen en uiteindelijke bewaring of vernietiging. Externe documentatie die nodig is voor het managementsysteem voor informatiebeveiliging wordt ook geïdentificeerd en beheerd op een manier die passend is voor onze instelling.

De Hanze identificeert in opdracht van het CvB welke interne en externe communicatie relevant is voor het managementsysteem voor informatiebeveiliging, inclusief het bepalen van de onderwerpen, het tijdstip, de doelgroep en de communicatiemethoden.

7. Continue verbeteren

7.1. Audits en compliance monitoring [9.2]

Met regelmaat voert de Hanze in- en externe audits uit om te bepalen of opzet, bestaan en werking van het kader informatiebeveiliging en privacy aantoonbaar voldoen aan zowel de in- en externe normen.

De Hanze stelt een auditplan (inclusief frequentie, methoden, verantwoordelijkheden) vast, voert dit uit en rapporteert de resultaten. Bij het opzetten van het auditplan wordt rekening gehouden met het belang van de betrokken processen en eerdere auditresultaten.

7.2. Directiebeoordeling en strategische evaluatie [9.3]

Het CvB beoordeelt regelmatig het managementsysteem voor informatiebeveiliging van de Hanze op voortdurende geschiktheid, volledigheid en doeltreffendheid.

Hierbij wordt aandacht besteed aan de status van verbeterpunten uit eerdere managementreviews, relevante veranderingen in de context en naar de behoeften en verwachtingen van belanghebbenden. Ook worden trends in afwijkingen en corrigerende maatregelen, resultaten van monitoring en auditresultaten meegenomen. Daarnaast wordt feedback van belanghebbenden, resultaten van risicobeoordelingen en de status van het risicobehandelingsplan beoordeeld, evenals kansen voor continue verbetering.

De managementreviews (4, 8 en 12 maand rapportages) resulteren in beslissingen voor continue verbetering en wijzigingen in het managementsysteem voor informatiebeveiliging en privacy, ondersteund door gedocumenteerde informatie.

7.3. Afwijkingen en corrigerende maatregelen [10.1, 10.2]

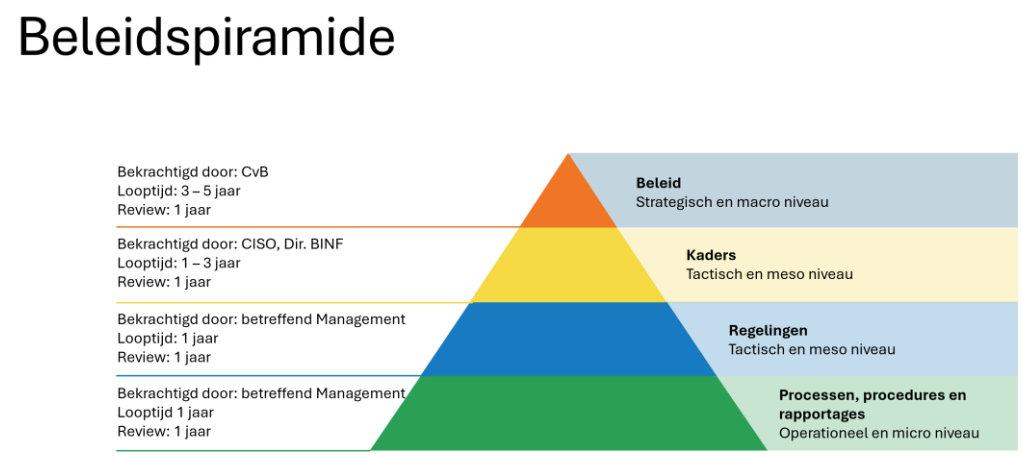
Onze instelling waarborgt het voortdurend verbeteren van het managementsysteem voor informatiebeveiliging door middel van een Plan, Do, Check, Act-cyclus. Zie Beleidsdocument ‘Samenwerken aan kwaliteit’.

Bij het constateren van afwijkingen reageren we adequaat en treffen passende maatregelen. Daartoe identificeren en beoordelen we deze afwijkingen en oorzaken. Vervolgens evalueren we de effectiviteit van deze corrigerende maatregelen en passen indien nodig wijzigingen toe in ons management voor informatiebeveiliging en privacy. Als bewijs leggen we de aard van de afwijkingen, de genomen maatregelen en de resultaten van de corrigerende acties vast.

8. Bijlages

8.1. Beleidspiramide

De beleidspiramide van onze instelling bestaat uit vier lagen: beleid, kaders, regelingen, rapportages en formats.



Figuur 1. Beleidspiramide

1. Beleid

Op het 1e niveau is het strategisch beleid beschreven: het waarom.
Beleid wordt formeel bekrachtigd door het CvB en heeft een looptijd van 3 tot 5 jaar.

2. Kader

Op het 2e niveau is zijn de beleidsondersteunende (tactische) standaarden beschreven: het wat.
Standaarden worden formeel bekrachtigd door het betreffende management. Dit kan afhankelijk van het onderwerp zijn de CISO, CIO, Directeur ICT etc. De standaarden kennen een looptijd van 1 tot 3 jaar.

3. Regelingen

Op het 3e niveau zijn de (tactische) regelingen beschreven: het hoe.
Regelingen worden formeel bekrachtigd door het betreffende management. De regelingen kennen een looptijd van 1 jaar.

4. Procedure, processen en rapportages

Op het 4e en laagste niveau van de beleidspiramide zijn de operationele procedures, processen en rapportages beschreven. Deze worden formeel bekrachtigd door het betreffende management. Ook deze documenten kennen een looptijd van 1 jaar.

5. Review proces

Aan het einde van de looptijd worden de vastgestelde documenten in onze beleidspiramide herzien, of als hiertoe op basis van ontwikkelingen eerder aanleiding voor is.
Minimaal eens per jaar worden de documenten beoordeeld op actualiteit. Ook als er geen aanpassingen benodigd zijn wordt dit vastgelegd. De documenten worden hierbij voorzien van een nieuw versienummer.

share your talent.
move the world.

Dienst Informatisering (BINF)