|  |
| --- |
| Strategisch beleid Informatiebeveiliging  Template |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |  |
|  |  |

**Documentinformatie**

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



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader |  |
| ISO27001 | 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 |

**Creative Commons**

Afbeelding met symbool, schermopname, biljartbal

Automatisch gegenereerde beschrijvingDit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc176513760)  [1 Inleiding 5](#_Toc176513761)  [1.1 Doel van het beleid 5](#_Toc176513762)  [1.2 Reikwijdte en toepassingsgebied 5](#_Toc176513763)  [1.3 Definities en afkortingen 5](#_Toc176513764)  [2 Context van de Instelling 7](#_Toc176513765)  [2.1 De Instelling en haar context (4.1) 7](#_Toc176513766)  [2.2 De behoefte en verwachtingen van belanghebbenden (4.2) 7](#_Toc176513767)  [2.3 De reikwijdte van het ISMS (4.3) 7](#_Toc176513768)  [3 Management 8](#_Toc176513769)  [3.1 Uitgangspunten van ons beleid (5.2) 8](#_Toc176513770)  [3.2 Structuur van ons beleid 8](#_Toc176513771)  [3.3 Betrokkenheid, leiderschap en verantwoordelijkheden (5.1, 5.2, 5.3) 9](#_Toc176513772)  [4 Risicomanagement 10](#_Toc176513773)  [4.1 ISMS-risico’s en (bij)sturing door management (6.1, 8.1, 9.1) 10](#_Toc176513774)  [4.2 Operationeel risicomanagement (6.2, 8.2, 8.3) 10](#_Toc176513775)  [5 Mensen en middelen 11](#_Toc176513776)  [5.1 Middelen voor informatiebeveiliging (7.1) 11](#_Toc176513777)  [5.2 Kennis en competenties (7.2, 7.3) 11](#_Toc176513778)  [5.3 Documentatie en Communicatie (7.4, 7.5) 11](#_Toc176513779)  [6 Continu verbeteren 12](#_Toc176513780)  [6.1 Audits en compliance monitoring (9.2) 12](#_Toc176513781)  [6.2 Directiebeoordeling en strategische evaluatie (9.3) 12](#_Toc176513782)  [6.3 Afwijkingen en corrigerende maatregelen (10.1, 10.2) 12](#_Toc176513783)  [7 Vaststelling 13](#_Toc176513784)  [Bijlage 1 Beleidspiramide 14](#_Toc176513785)  [1.1 Beleid 14](#_Toc176513786)  [1.2 Standaard 14](#_Toc176513787)  [1.3 Richtlijn 14](#_Toc176513788)  [1.4 Procedure, processen en handleidingen 14](#_Toc176513789)  [1.5 Review proces 14](#_Toc176513790) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4, Hieronder een voorbeeld.

Dit is de vernieuwde versie van het strategisch informatiebeveiligingsbeleid van onze instelling. Het vorige document was gebaseerd op een versie uit [JAAR] en bevatte zowel strategische uitgangspunten als een aantal tactische en operationele elementen zoals rollen inclusief taken en verantwoordelijkheden binnen [AFDELING] en het melden van incidenten. Deze versie beperkt zich tot het daadwerkelijk strategisch informatiebeveiligingsbeleid, zodat aanpassingen minder vaak hoeven plaats te vinden.

Het primaire doel van dit beleid is het geven van richting aan onze informatiebeveiliging zodat de beschikbaarheid, vertrouwelijkheid en integriteit van informatie in de primaire processen van onze instelling zo goed mogelijk worden geborgd. Kwetsbaarheden in systemen of ongeautoriseerde toegang tot onderwijs-, onderzoeks- en valorisatie-informatie kunnen immers de waarde van een [INSTELLING]-diploma, behaalde cijfers of de legitimiteit van onderzoeks-conclusies ondermijnen. Intern uitgangspunt voor dit document is het ‘Strategisch Kader Integrale Veiligheid’. Extern uitgangspunt voor dit document is de NEN-ISO/IEC 27001:2023-norm aangezien dit wereldwijd de ‘best practice’ vormt voor informatiebeveiliging op strategisch niveau. Achter hoofdstuk- en paragraaftitels zijn de verwijzingen naar relevante ISO-normen opgenomen.

# Inleiding

Dit document beschrijft het strategisch informatiebeveiligingsbeleid van onze instelling vanaf datum ondertekening van College van Bestuur en vervangt hiermee het voorgaande beleid.

Dit strategisch informatiebeveiligingsbeleid, gebaseerd op NEN-ISO/IEC 27001:2023, stelt kaders en geeft richting. Op tactisch en operationeel niveau is dit beleid aangevuld met onderwerp specifieke documenten (standaarden, richtlijnen, procedures en handleidingen).

## Doel van het beleid

Onze instelling versterkt met dit strategisch informatiebeveiligingsbeleid de cyberweerbaarheid, de groei in het volwassenheidsniveau en de bescherming van informatie en persoonsgegevens. Hiermee borgen we een veilige leer- en werkomgeving voor onze studenten, medewerkers, docenten en onderzoekers.

## Reikwijdte en toepassingsgebied

Bij onze instelling 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.

## Definities en afkortingen

|  |  |
| --- | --- |
| CvB | College van Bestuur |
| FAIR | Uitgangspunten voor onderzoeksdata: Findable (vindbaar), Accessible (toegankelijk), Interoperable (interoperabel), Reusable (herbruikbaar) |
| ISMS | Information Security Management System: een set van afspraken en procedures om informatiebeveiliging te organiseren |
| 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. |

# Context van de Instelling

## De Instelling en haar context (4.1)

Onze onderwijsinstelling helpt studenten in een kwetsbare levensfase groeien en ontwikkelen en vervult een maatschappelijke rol in haar regio. 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, Reuseable). Tegelijkertijd verwachten onderzoekspartners en bedrijven waar we mee samenwerken dat hun informatie vertrouwelijk wordt behandeld. Op basis van het cyberdreigingsbeeld bevat dit strategisch beleidsdocument de uitgangspunten voor informatiebeveiliging 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.

## 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 van 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.

## De reikwijdte van het ISMS (4.3)

Om te voorkomen dat de hiervoor genoemde verwachtingen van belanghebbenden geschaad worden, organiseren we onze informatieveiligheid met behulp van een proces genaamd Information Security Management System (ISMS). Hiermee monitoren en verbeteren we continue de informatiebeveiliging binnen alle processen in onderwijs, onderzoek, bedrijfsvoering en daaruit voortvloeiende activiteiten die namens en/of voor onze instelling worden uitgevoerd. Het ISMS is verder toegelicht in hoofdstuk 4.

# Management

## Uitgangspunten van ons beleid (5.2)

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

1. **werken we risico gebaseerd**

We baseren de te treffen maatregelen op de mogelijke veiligheidsrisico’s van onze gegevens, processen, informatievoorzieningen en -systemen en op de risicobereidheid (risk appetite) van het CvB.

1. **is iedereen verantwoordelijk**

Iedereen voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

1. **wordt het informatiebeveiligingsbeleid altijd en overal gevolgd**

Informatiebeveiliging zit in het DNA van onze instelling en is integraal onderdeel van al onze werkzaamheden.

1. **hanteren we Security en Privacy by Design**

Informatiebeveiliging en bescherming van persoonsgegevens en privacy is vanaf de start een integraal onderdeel van ieder project of iedere verandering van onze gegevens, processen, informatievoorzieningen en -systemen.

1. **hanteren we Security en Privacy by Default**

Informatievoorzieningen en -systemen standaard zijn geconfigureerd met de meest veilige instellingen.

1. **heeft iedereen toegang tot alleen dat wat nodig is**

Gebruikers hebben alleen toegang tot gegevens, processen, informatievoorzieningen en -systemen passend bij hun functie en rollen.

1. **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.

## Structuur van ons beleid

De structuur van ons beleid is opgebouwd in vier lagen (zie Bijlage 1 Beleidspiramide). De bovenste laag is het strategisch informatiebeveiligingsbeleid en is beschreven in dit document. Verdere specificering van het informatiebeveiligingsbeleid is vastgelegd in de onderliggende standaarden, richtlijnen, procedures en handleidingen.

## Betrokkenheid, leiderschap en verantwoordelijkheden (5.1, 5.2, 5.3)

### Betrokkenheid en leiderschap (5.1, 5.2)

Het College van Bestuur (CvB) toont leiderschap en betrokkenheid door ervoor te zorgen dat het informatiebeveiligingsbeleid en de doelstellingen in lijn zijn met de strategische richting van onze instelling. De eisen van het managementsysteem (ISMS) integreren we in de processen van onderwijs, onderzoek en bedrijfsvoering. Het CvB communiceert het belang van effectieve informatiebeveiliging, 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.

### Rollen en verantwoordelijkheden (5.3)

Het CvB draagt er zorg voor dat er binnen onze instelling duidelijkheid bestaat over verantwoordelijkheden en bevoegdheden van rollen met betrekking tot informatiebeveiliging. Het CvB kent de verantwoordelijkheden en bevoegdheden toe voor het waarborgen van de naleving van het informatiebeveiligingsbeleid en voor het rapporteren over de prestaties ervan.

### Three lines

Het CvB zorgt ervoor dat duidelijke lijnen van verantwoordelijkheid zijn vastgesteld. Binnen onze instelling hanteren we hiervoor ‘Three lines’ voor effectieve controle en governance van informatiebeveiliging. Binnen deze structuur is de eerste lijn verantwoordelijk voor operationeel management en daarmee de toepassing van de standaarden en richtlijnen voor informatiebeveiliging. De tweede lijn voorziet de eerste lijn van passend en uitvoerbaar informatiebeveiligingsbeleid en ondersteunt het risicomanagementproces. De derde lijn is verantwoordelijk voor interne audits.

# Risicomanagement

## ISMS-risico’s en (bij)sturing door management (6.1, 8.1, 9.1)

Onze instelling neemt bij het plannen van het managementsysteem voor informatiebeveiliging 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 deze 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 informatiebeveiligingsrisico's. Dit omvat het selecteren van passende opties voor risicobehandeling, het vaststellen van beheersmaatregelen en het verkrijgen van goedkeuring van risico-eigenaren.

We stellen criteria vast voor deze processen en implementeren ze conform deze criteria. Gedocumenteerde informatie wordt beschikbaar gesteld in de benodigde omvang en diepgang om het vertrouwen te waarborgen dat de processen volgens planning zijn uitgevoerd. Geplande wijzigingen in onze (informatiemanagement-)processen beheren we en worden evenals onbedoelde wijzigingen geëvalueerd om indien nodig corrigerende maatregelen te nemen. Extern geleverde processen, producten of diensten worden tevens gecontroleerd en gemonitord door onze instelling.

Onze instelling stelt vast wat wanneer en door wie moet worden gemonitord en gemeten, inclusief processen en beheersmaatregelen voor informatiebeveiliging, en bepaalt de methoden voor het monitoren, meten en analyseren. Gedocumenteerde informatie is beschikbaar als bewijs van de resultaten. Onze instelling evalueert de prestaties van de informatiebeveiliging en de doeltreffendheid van het managementsysteem voor informatiebeveiliging.

## Operationeel risicomanagement (6.2, 8.2, 8.3)

Onze instelling stelt informatiebeveiligingsdoelstellingen vast die in lijn zijn met het informatiebeveiligingsbeleid, meetbaar zijn, en rekening houden met geldende eisen en risicobeoordelingen. We monitoren, communiceren, actualiseren en documenteren deze doelstellingen.

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

Onze instelling voert regelmatig of bij belangrijke veranderingen risicobeoordelingen voor informatiebeveiliging uit, waarbij we rekening houden met vastgestelde criteria voor risicobeoordeling en acceptatie, en bewaart gedocumenteerde informatie over de resultaten van deze beoordelingen.

Tevens implementeert onze instelling het risicobehandelingsplan voor informatiebeveiliging en bewaren we gedocumenteerde informatie over de resultaten van de risicobehandeling.

# Mensen en middelen

## Middelen voor informatiebeveiliging (7.1)

Onze instelling 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 voor het uitvoeren van dit informatiebeveiligingsbeleid.

## Kennis en competenties (7.2, 7.3)

Onze instelling 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. 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 onze instelling dienen zich bewust te zijn van het informatiebeveiligingsbeleid, hun rol bij het bevorderen van de doeltreffendheid van het informatiebeveiligingsmanagementsysteem en de consequenties van het niet naleven van de eisen van dit managementsysteem.

## Documentatie en Communicatie (7.4, 7.5)

Het managementsysteem voor informatiebeveiliging van onze instelling 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 onze instelling 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 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.

Onze instelling identificeert 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.

# Continu verbeteren

## Audits en compliance monitoring (9.2)

Met regelmaat voert onze instelling in- en externe audits uit om te bepalen of opzet, bestaan en werking van het informatiebeveiligingsbeleid aantoonbaar voldoen aan zowel de in- en externe normen.

Onze instelling 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.

## Directiebeoordeling en strategische evaluatie (9.3)

Het CvB beoordeelt periodiek het managementsysteem voor informatiebeveiliging van onze instelling op voortdurende geschiktheid, toereikendheid 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. Tevens 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 resulteren in beslissingen voor continue verbetering en wijzigingen in het managementsysteem voor informatiebeveiliging, ondersteund door gedocumenteerde informatie.

## 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.

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. Als bewijs leggen we de aard van de afwijkingen, de genomen maatregelen en de resultaten van de corrigerende acties vast.

# Vaststelling

Dit beleid is aldus vastgesteld.

[Plaats], [Datum].

[NAAM]

[HET COLLEGE / DE RAAD VAN BESTUUR].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]

1. Beleidspiramide

De beleidspiramide van onze instelling bestaat uit vier lagen: beleid, procedures, richtlijnen en procedures.



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.

* 1. Standaard

Op het 2e niveau is zijn de beleidsondersteunende (tactische) standaarden beschreven: het wat.

Standaarden worden formeel bekrachtigd door de gemandateerde functionaris(sen). Dit kan / kunnen afhankelijk van het onderwerp zijn de CISO, CIO, Directeur ICT etc. De standaarden kennen een looptijd van 1 tot 3 jaar.

* 1. Richtlijn

Op het 3e niveau zijn de (tactische) richtlijnen beschreven: het hoe.

Richtlijnen worden formeel bekrachtigd door het betreffende management. De richtlijnen kennen een looptijd van 1 jaar.

* 1. Procedure, processen en handleidingen

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

* 1. 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.