dialogic

Onderzoek voor *onderbouwd* beleid.



Rapport

Kennisveiligheidsbeleid versterkt

Sectorbeeld kennisveiligheid 2026

Auteurs

dr. Timon de Boer

ir. Iris van Vugt

ir. Sonja Kleter

José van der Geest Msc.

Femke van Wijk Msc.

dr. Maarten van Doorn

drs. Johan Bokdam

dr. Ingrid Wakkee

In samenwerking met

Oberon

onderzoek | advies

Rapport

Kennisveiligheidsbeleid versterkt

Sectorbeeld kennisveiligheid 2026

Auteurs

dr. Timon de Boer
ir. Iris van Vugt
ir. Sonja Kleter
José van der Geest Msc.
Femke van Wijk Msc.

dr. Maarten van Doorn
drs. Johan Bokdam
dr. Ingrid Wakkee

Opdrachtgever

Ministerie voor Onderwijs, Cultuur en Wetenschap

Publicatienummer

2025.073-11028

Citeren als

Dialogic & Oberon (2026). Kennisveiligheidsbeleid versterkt. Sectorbeeld kennisveiligheid 2026. In opdracht van het Ministerie voor Onderwijs, Cultuur en Wetenschap

Datum

21 april 2026

Beeld omslag

Pexels via Pixabay

Inhoud

Managementsamenvatting 5

1 Inleiding 8

1.1 Achtergrond van het onderzoek 8
1.2 Doel en vraagstelling 9
1.3 Onderzoeksmethode 9
1.4 Leeswijzer 11

2 Kennisveiligheid en academische kernwaarden 13

2.1 De gebruikte definitie van het begrip kennisveiligheid 14
2.2 De relatie tussen kennisveiligheid en academische kernwaarden 14
2.3 Het bespreken van dilemma's bij kennisveiligheid 17

3 Juridische kaders en gedragscodes 20

3.1 Ontwikkeling beleid juridische kaders en gedragscodes 21
3.2 Concrete kaders en codes 23

4 Het inschatten van risico's 25

4.1 Toetsing kennisveiligheidsrisico's 25
4.2 Risico-inschatting als onderdeel van het kennisveiligheidsbeleid 27
4.3 Internationale partnerorganisaties en personen 28

5 Risicomanagement 29

5.1 Registratie internationale samenwerkingen 29
5.2 Niveau van verantwoordelijkheden en processen 32
5.3 Invulling rollen kennisveiligheidsbeleid 33

6 Fysieke en digitale beschermingsmaatregelen 36

6.1 Fysieke beschermingsmaatregelen 37
6.2 Digitale beschermingsmaatregelen 38
6.3 Samenhang met cyberbeleid 40
6.4 Reisdelegaties 41

7 Internationale partnerschappen 43

8 Personeelsbeleid 51

9 Doorontwikkeling van beleid 59
9.1 Voornemens instellingen doorontwikkeling van beleid 59
9.2 Behoeften van instellingen richting de Rijksoverheid 61
10 Conclusies 64
Bijlage 1. Samenstelling klankbordgroep 68
Bijlage 2. Vragenlijst self-assessment 69

Managementsamenvatting

In januari 2022 hebben de Nederlandse kennissector en de Rijksoverheid gezamenlijk de Nationale Leidraad Kennisveiligheid gepubliceerd. In 2023 en 2024 is met drie sectorbeelden een eerste inzicht gegeven in de stand van implementatie van de Leidraad door de kennisinstellingen. Op basis daarvan zijn nadere afspraken gemaakt tussen de minister, de sectororganisaties en instellingen en is toegezegd om de meting te herhalen. Het doel van deze eerste vervolgmeting is de ontwikkeling in de sector in kaart brengen en verder bijdragen aan een lerende aanpak, door de volgende onderzoeksvragen te beantwoorden:

1. Wat is anno 2026 de stand van implementatie van de Leidraad Kennisveiligheid onder universiteiten, hogescholen en KNAW- en NWO-institutenorganisaties?
2. Welke stappen zijn gezet ten opzichte van de nulmeting?
3. In hoeverre vinden kennisinstellingen dat ze ver genoeg zijn, gegeven hun zelf ingeschatte risicoprofiel?
4. Waarom hebben instellingen hun huidige beleidskeuzes gemaakt en *welke good practices* en dilemma's zien ze?

Om deze vragen te beantwoorden hebben Dialogic en Oberon tussen juni 2025 en maart 2026 een onafhankelijk onderzoek uitgevoerd, dat bestond uit een brede self-assessment en een verdiepende casestudy. Het onderzoek is begeleid door een klankbordgroep van inhoudsdeskundigen vanuit de koepelorganisaties en kennisinstellingen. Deze meting leidt tot de volgende conclusies.

Conclusie 1. De Leidraad Kennisveiligheid is breed geïmplementeerd. We zien dat op alle thema's van de Leidraad de meeste instellingen beleid hebben geïmplementeerd, waarbij het gemiddelde niveau verschilt per thema.

Conclusie 2. De Nederlandse kennissector heeft op vrijwel alle thema's vooruitgang geboekt ten opzichte van de vorige sectorbeelden, al is de ontwikkeling verschillend per thema, instelling en subsector. Waar instellingen in de nulmeting nog veelal beleid aan het vormgeven en vaststellen waren, zijn ze dat nu aan het uitvoeren en aan het evalueren. Kennisveiligheidsbeleid is geïnstitutionaliseerd, bewustzijn van kennisveiligheid is zowel verbreed als verdiept.

Conclusie 3a. De sector is nog niet volledig uitontwikkeld. Meer dan de helft van de instellingen – voornamelijk instellingen met een hoger zelf ingeschat risicoprofiel – wil nog stappen in volwassenheid zetten. Deze instellingen zien *real-time* registratie van internationale partnerschappen en bewustzijn onder medewerkers als grootste ontwikkelpunten.

Conclusie 3b. We zien duidelijke differentiatie binnen de sector. Het gewenste volwassenheidsniveau verschilt tussen instellingen, binnen subsector, en tussen thema's. Waar instellingen met een hoger zelf ingeschat risicoprofiel nog duidelijke ambities hebben, vindt een groep instellingen met een zelf ingeschat laag risicoprofiel zich uitontwikkeld omdat ze geen of weinig kennisveiligheidsrisico's kennen.

Conclusie 3c: De voornaamste verklaringen voor nog niet gerealiseerde ambities zijn beperkte tijd en capaciteit. Bewustzijn en draagvlak op de werkvloer kost tijd en het vrijmaken van tijd en de juiste expertise is een uitdaging. Sommige instellingen wachten voor vervolgstappen op duidelijkheid over de wet screening kennisveiligheid en de actualisatie van de Leidraad. Op specifieke onderwerpen missen instellingen concrete en hanteerbare bronnen, tools en adviezen voor het maken van gerichte risico-afwegingen van affiliaties en de sensitiviteit van onderzoeksthema's of technologieën.

Conclusie 4. De onderliggende dilemma's zijn dezelfde als in de nulmeting, er zijn wel stappen op gezet. Instellingen lopen net als in de nulmeting tegen dilemma's aan:.

- **Dilemma's tussen kennisveiligheid en academische kernwaarden k**omen in deze meting minder sterk naar voren dan tijdens de nulmeting. Een aantal instellingen geeft aan dat zij kennisveiligheid juist zien als mogelijkheid om academische kernwaarden te beschermen.
- **Proportionaliteit**. Voor instellingen met een lager risicoprofiel is het de vraag wat een passende en proportionele inzet moet zijn voor registratie, processen en functies voor risicomanagement.
- **Maatwerk versus duidelijk kaders en richtlijnen**. Instellingen zoeken naar een optimum tussen maatwerk en generieke richtlijnen. Instellingen maken vaak tijdrovende case-by-case afwegingen. Duidelijke kaders maken beslissingen efficiënter maar kennen risico's op schijnzekerheid en op het onnodig uitsluiten van samenwerkingen en kansen.
- **Voorkomen stigmatisering en discriminatie**. Bewustzijn van kennisveiligheid is voor instellingen essentieel, maar een focus op risicolanden , onzorgvuldig taalgebruik en generalisaties van case-by-case afwegingen brengen risico's op stigmatisering met zich mee.
- **Gelijk speelveld binnen de EU**. Verschillende nationale aanpakken - vrijblijvender of juist dwingender – van kennisveiligheidsbeleid leiden tot waterbedeffecten en bemoeilijken internationale samenwerkingen.

Conclusie 5. De sector is overwegend positief over de lerende aanpak van de Rijksoverheid maar heeft behoefte aan meer proactieve ondersteuning. Binnen hun institutionele autonomie zoeken

instellingen meer specifieke ondersteuning en richting vanuit de Rijksoverheid. Zij spreken specifiek de behoefte uit voor:

a) **Financiële ondersteuning**. Voor het financieren van beleid en (kostbare) mitigerende maatregelen.
b) **Handzame bronnen** voor het uitvoeren van een risicoanalyse en maken van bijbehorende afwegingen rondom affiliatie, onderzoeksonderwerp en het naleven van exportwetgeving.
c) **Een duidelijk(er) en concreet(er) handelingskader**. Belangrijk voor instellingen is dat ze zelf afwegingen kunnen blijven maken, maar daar verder en beter bij ondersteund worden.

1 Inleiding

1.1 Achtergrond van het onderzoek

In januari 2022 hebben de Nederlandse kennissector en de Rijksoverheid gezamenlijk de Nationale Leidraad Kennisveiligheid (hierna: de Leidraad) gepubliceerd, een richtinggevend document voor alle kennisinstellingen van Nederland. De Nationale Leidraad Kennisveiligheid introduceert kennisveiligheid als volgt (pp. 8-9):

"Met kennisveiligheid wordt (...) in de eerste plaats bedoeld: het voorkomen van ongewenste overdracht van sensitieve kennis en technologie met negatieve gevolgen voor onze nationale veiligheid en de Nederlandse innovatiekracht. Daarnaast gaat het om heimelijke beïnvloedings- en inmengingsactiviteiten van statelijke actoren in hoger onderwijs en wetenschap. Dergelijke beïnvloeding (*foreign interference*) kan leiden tot vormen van (zelf)censuur resulterend in aantasting van de academische vrijheid. Tot slot draait het bij kennisveiligheid om ethische kwesties die samenhangen met de samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd. Zo kunnen onderzoekers van uw instelling betrokken raken bij de ontwikkeling van technologie die in deze landen wordt ingezet bij de onderdrukking van de eigen burgers."

In het bestuursakkoord 2022 hoger onderwijs en wetenschap is afgesproken dat een externe audit zal plaatsvinden op de (mate van) implementatie van de Leidraad. Omdat het thema volop in ontwikkeling was, is die audit vormgegeven in de vorm van een nulmeting, die trapsgewijs bij universiteiten (inclusief UMCs), hogescholen en de instituten(organisaties) van NWO-I en de KNAW is uitgevoerd.

De drie sectorbeelden van de nulmeting gaven inzicht in de stand van implementatie van de Leidraad, good practices op aspecten van het kennisveiligheidsbeleid en dilemma's zoals de balans tussen academische waarden en nationale veiligheid, de verdeling van verantwoordelijkheden tussen instellingen en de nationale overheid en het voorkomen van stigmatisering. De sectorbeelden verantwoordden richting Tweede Kamer, departement en maatschappij hoe kennisveiligheidsbeleid vorm kreeg en in hoeverre afspraken uit het bestuursakkoord zijn uitgevoerd. Ook zijn op basis van de sectorbeelden nadere afspraken gemaakt tussen de minister en de sectororganisaties over enkele concrete onderdelen van het kennisveiligheidsbeleid. Ook gaven ze richting aan het

gesprek tussen minister en de raden van toezicht. De minister heeft tenslotte ook toegezegd om de meting te herhalen[1]. Dit rapport is het resultaat van deze vervolgmeting.

1.2 Doel en vraagstelling

Deze huidige meting moest resulteren in een sectorbeeld dat een vergelijkbare rol in het kennisveiligheidsbeleid vervult. Het sectorbeeld moest inzichten bevatten die voor materiedeskundigen op het departement en bij instellingen nuttig zijn, maar ook toegankelijk zijn voor een bredere groep lezers in politiek, bestuur en maatschappij. Tegelijk moest het gezamenlijk sectorbeeld ook voldoende oog hebben voor de kenmerken en specifieke vraagstukken van de verschillende kennisinstellingen, zonder individuele instellingen herkenbaar in beeld te brengen. Het onderzoek moest verder bijdragen aan een lerende aanpak. Daarom besteedden we ook weer aandacht aan dilemma's waarmee instellingen zich geconfronteerd zien en eventuele *lessons learned* waar instellingen van elkaar kunnen leren. Naast dit sectorbeeld ontvangen alle instellingen daarom een individuele terugkoppeling die alleen wordt gedeeld met hen, in de vorm van een instellingsbeeld waarin hun antwoorden worden gecontextualiseerd binnen het sectorbeeld.

De huidige meting Kennisveiligheid beantwoord daarbij de volgende onderzoeksvragen:

- Wat is anno 2026 de stand van implementatie van de Leidraad Kennisveiligheid onder universiteiten inclusief UMCs, hogescholen en KNAW- en NWO-institutenorganisaties?
- Welke stappen zijn gezet ten opzichte van de nulmeting?
- In hoeverre vinden kennisinstellingen dat ze ver genoeg zijn, gegeven hun zelfingeschatte risicoprofiel? Welke onderbouwing geven ze hiervoor?
- Waarom hebben instellingen hun huidige keuzes gemaakt en welke *good practices* en dilemma's zien ze?

1.3 Onderzoeksmethode

Om deze vragen te beantwoorden hebben we tussen juni 2025 en maart 2026 een onderzoek uitgevoerd, dat bestond uit een self-assessment en een verdiepende casestudy. Het onderzoek is begeleid door een klankbordgroep van inhoudsdeskundigen vanuit de kennisinstellingen die vanuit hun kennis over de inhoud en het veld ons als onderzoeksteam en het ministerie van OCW als

[1] Tweede Kamer, vergaderjaar 2024–2025, 31 288, nr. 1183

opdrachtgever adviseren over het onderzoek. De samenstelling van de klankbordgroep staat in bijlage 1.

1.3.1 Voorbereiding

De voorbereidingsfase begon met een startgesprek over de onderzoeksopzet met het ministerie van OCW. Direct daarna zijn we gestart met het uitwerken van de concept-vragenlijst aan de hand van de Leidraad en de ervaringen met de nulmeting. De vragenlijst in de nulmeting bestond voor een groot gedeelte uit open vragen, aangevuld met een aantal rubrics. Voor het vergelijkbaar maken van de ontwikkeling per thema ten opzichte van de nulmeting is wederom gewerkt met rubrics op een vijfpuntsschaal. Om recht te doen aan de verschillen in risicoprofiel tussen instellingen, is toegevoegd dat ook gevraagd wordt op welk niveau een instelling **wil** staan (ambitie).

Voor de invulling van de rubrics hebben we ons sterk laten inspireren door het UNL volwassenheidsmodel. Enerzijds omdat we weten hoeveel tijd het instellingen kan kosten om de vragenlijst in te vullen, anderzijds omdat de minister aan de Tweede Kamer heeft toegezegd instellingen die gebruik maken van het UNL-volwassenheidsmodel te ontlasten. Door de antwoordopties vergelijkbaar te houden met zowel de nulmeting als met dit model was de hoop dat de invullast voor (een deel van de) instellingen is beperkt én dat de vergelijkbaarheid/ontwikkeling in de tijd zichtbaar wordt. Het UNL-volwassenheidsmodel is niet bedoeld voor audits. Omdat de huidige meting een self-assessment is die zich richt op de volwassenheid van het beleidsproces, was onze inschatting aansluiten op het volwassenheidsmodel instellingen juist zou kunnen helpen. De vragenlijst is twee keer besproken met de klankbordgroep die voor dit onderzoek is ingesteld.

1.3.2 Vragenlijst

De vragenlijst voor de zelfevaluatie is eind augustus 2025 via een online beveiligde vragenlijstomgeving uitgezet onder contactpersonen van alle 74 betrokken kennisinstellingen, verdeeld over vier “subsectoren” (veertien universiteiten, 37 hogescholen, 12 KNAW-instituten, 9 NWO-instituten en de de centrale bureaus van KNAW en NWO-I). Deze is vervolgens door hen in samenspraak met andere relevante personen binnen de instelling ingevuld. Met de contactpersonen per instelling hielden we ook direct contact over de voortgang, eventuele vragen en tijdige oplevering. De vragenlijst is opgenomen in bijlage 2.

1.3.3 Verdiepende casestudy

Na de analyse van de vragenlijsten volgde een kwalitatief, verdiepend casestudy onderzoek bij acht verschillende instellingen. Doel was om meer kwalitatieve informatie op te halen over het implementatieproces van de Leidraad, risicomanagement en risicoanalyses en over geleerde lessen,

aandachtspunten en dilemma's. De informatie uit deze onderzoeksfase vult het brede beeld uit de vragenlijst aan met meer diepgaand inzicht.

Bij de selectie van cases hebben we gezocht naar een spreiding over achtergrondkenmerken en, op basis van de zelfevaluatie, over inhoudelijk relevante praktijken op omgang met verschillende type risico's en mate van vooruitgang op specifieke thema's. De criteria voor de selectie van cases en de leidraad voor de gesprekken zijn afgestemd en besproken met de opdrachtgever en de klankbordgroep. Vanwege anonimiteit van de deelnemende instellingen, is de uiteindelijke selectie gedaan door het onderzoeksteam en niet gecommuniceerd met de klankbordgroep of het ministerie van OCW.

Voor elke case voerden we gesprekken met betrokkenen op meerdere niveaus binnen de instelling. Hierbij onderscheiden we het centrale niveau (waaronder de bestuurlijk portefeuillehouder, het adviesteam en eventueel anderen), het decentrale niveau van faculteiten/instituten (waaronder decanen en onderzoeksleiders) en stafafdelingen zoals HR en integrale veiligheid. In totaal zijn 17 gesprekken gevoerd met 32 betrokkenen bij acht instellingen. Naast interviews analyseerden we – voor zover beschikbaar – relevante interne documentatie van de instelling.

1.3.4 Analyse en rapportage

Het onderzoeksteam heeft de door de instellingen aangeleverde informatie gecodeerd om vervolgens een inhoudelijke analyse op geaggregeerd niveau te maken. De rubrics en de gesloten vragen (ja/nee) zijn kwantitatief geanalyseerd. De resultaten uit die analyse en de analyse van de caseverslagen zijn integraal samengebracht in dit sectorbeeld.

1.4 Leeswijzer

Hoofdstuk twee tot en met acht geven de uitkomsten van de self-assessment en de verdiepende casestudy telkens integraal inhoudelijk weer. Deze hoofdstukken volgen de opzet en thema's van de Leidraad. Elk hoofdstuk start met een samenvatting van de belangrijkste conclusies op dat thema. Daarna geven we voor elk thema een figuur die de ontwikkeling van de sector samenvat. Daarbij presenteren we de scores van alle instellingen op de rubric-vragen in de nulmeting[2], hun huidige situatie en de door hen gewenste situatie. Zo komt ook in beeld op welk niveau instellingen gegeven hun risicoprofiel **willen** staan (ambitie). De niveaus zijn voor alle thema's gelijk (Geen

[2] Er zijn een paar nieuwe rubric vragen toegevoegd deze meting. Als er een verandering in vraagstelling heeft plaatsgevonden, geven we dit in de figuren weer met een sterretje bij de o-meting.

beleid, Initieel/in ontwikkeling, Herhaalbaar en/of gedefinieerd, Meetbaar en gemanaged, Continue verbetering), de inhoudelijke omschrijving verschilt per thema (zie vragenlijst bijlage 2).

In hoofdstuk negen bespreken we de voornemens die instellingen hebben voor de komende periode en de ondersteuningsvragen daarbij. In hoofdstuk tien brengen we alle resultaten bij elkaar en trekken we conclusies.

Omdat het doel van deze rapportage is om een beeld van de sector als geheel te geven en individuele instellingen niet herleidbaar moeten zijn, geven we alleen waar relevant én mogelijk verschillen of uitsplitsingen naar groepen instellingen weer, bijvoorbeeld over relevante eigenschappen die invloed hebben op hun risicoprofiel of aanpak.

2 Kennisveiligheid en academische kernwaarden

Samenvatting

- Stand 2026: Het begrip 'kennisveiligheid' wordt vaker herkend door medewerkers binnen de instellingen. Kennisinstellingen rapporteren spanningen tussen kennisveiligheid en academische kernwaarden, maar zien soms ook een versterkende relatie. De meeste instellingen hebben een eigen commissie of aanspreekpunt waar dilemma's besproken worden. Andere instellingen vinden dit niet relevant voor de focus van hun instelling of gebruiken een gezamenlijke commissie.
- Stappen ten opzichte van nulmeting: Een aantal instellingen heeft de definitie van kennisveiligheid uit de Leidraad toegepast op hun specifieke context. Dilemma's rondom kennisveiligheid zijn dezelfde als in de nulmeting, maar het bewustzijn rondom deze dilemma's is vergroot en het bespreken van deze dilemma's heeft bij een groot deel van de instellingen een formelere rol gekregen in het beleid.
- Vinden instellingen zichzelf ver genoeg gegeven hun risicoprofiel? Een aantal instellingen zou graag een meer nationale lijn hanteren voor het behandelen van dilemma's rondom non-discriminatie en inclusie, om de omgang met dilemma's beter te kunnen onderbouwen.
- Keuzes en dilemma's: Instellingen ervaren dilemma's tussen kennisveiligheidsbeleid en open science, academische vrijheid, ethiek, non-discriminatie en inclusiviteit. Een aantal instellingen geeft echter ook aan dat zij kennisveiligheid juist zien als mogelijkheid om academische kernwaarden te beschermen.

De Leidraad stelt dat "onderzoek in Nederland moet worden uitgevoerd in overeenstemming met de nationaal en internationaal aanvaarde normen van wetenschappelijk handelen. Het respecteren van deze kernwaarden is een voorwaarde om volwaardig mee te draaien in de academische gemeenschap". Activiteiten van statelijke actoren kunnen de deze kernwaarden onder druk zetten. In dit hoofdstuk analyseren we hoe instellingen kennisveiligheid definiëren, en hoe zij de relatie tussen kennisveiligheid en bovenstaande kernwaarden zien.

2.1 De gebruikte definitie van het begrip kennisveiligheid

Bijna de helft van de instellingen geeft aan dat de manier waarop het begrip kennisveiligheid wordt gehanteerd of gedefinieerd in de afgelopen twee jaar veranderd is. Het grootste deel van de toelichting gaat over de ontwikkelingen in de positie die kennisveiligheid heeft in (het beleid van) de instelling. Deze positie is vaak verstevigd of vergroot, als gevolg van bijvoorbeeld groter bewustzijn van kennisveiligheid binnen de instelling. Medewerkers van instellingen uit de cases herkennen het begrip 'kennisveiligheid' vaker en leggen zelf meer kennisveiligheidsvraagstukken op tafel. De meeste instellingen verwijzen in de toelichting niet naar de definitie die binnen de instellingen gehanteerd wordt, al geven enkele instellingen aan dat het begrip kennisveiligheid meer in de context van de eigen instelling is geplaatst.

De andere (ca.) helft van de instellingen heeft ontkennend geantwoord op deze vraag. Zij geven vooral aan dat ze geen aanleiding zagen om de definitie te veranderen en volgen meestal de definitie van de Leidraad.



Figuur 1. Ontwikkeling begrip kennisveiligheid

2.2 De relatie tussen kennisveiligheid en academische kernwaarden

Academische kernwaarden, zoals academische vrijheid en transparantie, liggen aan de basis van het beleid en functioneren van de kennisinstellingen. Kennisveiligheidsbeleid kan hier invloed op hebben: instellingen benoemen verschillende relaties tussen de kernwaarden en kennisveiligheid. Waar voor sommige instellingen kennisveiligheid vooral een beperking van hun kernwaarden is, zien andere instellingen kennisveiligheidsbeleid juist als kans voor het beschermen van deze

kernwaarden. Enkele instellingen geven zelfs aan dat kennisveiligheid één van de kernwaarden geworden is binnen hun beleid.

In deze paragraaf geven we hier een weergave van. We starten met de relatie met de vaak genoemde kernwaarden 'academische vrijheid', 'integriteit' en 'autonomie'. Vervolgens gaan we in op de kernwaarden 'transparantie' of 'open science'. Ten slotte beschrijven we de relatie tussen kennisveiligheidsbeleid en ethische dilemma's, inclusiviteit en non-discriminatie.

Kennisveiligheid en academische vrijheid, integriteit en autonomie

Een kernwaarde die in de vragenlijst vaak genoemd is, is 'academische vrijheid'. Academische vrijheid gaat over de vrijheid om keuzes te maken voor het doen van onderzoek (bijvoorbeeld thema's, vragen, te gebruiken data en in te zetten methoden), het delen van bevindingen en het geven van onderwijs[3]. Een aantal kennisinstellingen ziet kennisveiligheidsbeleid als beperkende factor voor academische vrijheid. Het borgen van kennisveiligheid vraagt immers om afwegingen in samenwerkingen die onderzoekers of instellingen aangaan, personeel dat wel of niet wordt ingehuurd en eventuele technologieën of concepten waaraan wordt gewerkt. In de cases wordt genoemd dat dit in sommige gevallen bepalend is voor de onderwerpen die onderzoekers kunnen onderzoeken en de informatie die ze daarvoor kunnen gebruiken.

Kennisveiligheid wordt door andere instellingen juist genoemd als beschermende factor voor academische vrijheid of integriteit. Door zorgvuldige afwegingen te maken op het gebied van kennisveiligheid, zien instellingen dat zij bijvoorbeeld heimelijke beïnvloeding kunnen voorkomen en daarmee de vrijheid en integriteit van hun onderzoekers kunnen beschermen. Kennisveiligheid beschermt daarmee de basisprincipes eerlijkheid, transparantie, onafhankelijkheid en verantwoordelijkheid die in de gedragscode wetenschappelijke integriteit genoemd worden.

Op basis van casestudy lijkt de balans tussen kennisveiligheid en academische vrijheid verschoven. Waar tijdens de nulmeting kennisveiligheid nog met name als beperking van academische vrijheid werd gezien, benaderen meer gesprekspartners het nu juist als versterking. Het draagvlak voor kennisveiligheidsbeleid binnen instellingen is volgens gesprekspartners gestegen.

Gesprekspartners en instellingen geven aan toenemend draagvlak deels komt door internationale geopolitieke ontwikkelingen en conflicten en de aandacht daarvoor in de media. Dit heeft volgens respondenten bijgedragen aan bewustzijn voor het belang van kennisveiligheidsbeleid. Ook is er in de afgelopen jaren intensief debat geweest in de kennissector over van de wenselijkheid van

[3] KNAW (2021) Academische vrijheid in Nederland. Een begripsanalyse en richtsnoer.

bepaalde wetenschappelijke samenwerking, los van kennisveiligheid. Voorbeelden die meermaals zijn genoemd zijn de samenwerking met fossiele industrie, tabaksindustrie en big tech. Hoewel deze dilemma's los van kennisveiligheid worden gezien heeft het bijgedragen aan een breder besef dat de Nederlandse kennissector niet zomaar met iedereen kan en wil samenwerken.

In de casestudy geven instellingen ook aan dat kennisveiligheidsbeleid impact kan hebben op de autonomie van de instelling. Enerzijds zouden instellingen bij een aantal afwegingen duidelijkere richtlijnen van de Rijksoverheid willen hebben om hun keuzes te legitimeren, anderzijds zijn kennisinstellingen bezorgd dat dit de manier waarop zij hun onderzoek beoordelen kan bepalen waardoor ze een deel van hun autonomie kwijt raken.

Kennisveiligheid en Open Science

In de vragenlijst is aan instellingen gevraagd op welke wijze in hun kennisveiligheidsbeleid aandacht is gegeven aan academische kernwaarden en Open Science. De meeste kennisinstellingen besteden in hun antwoord aandacht aan Open Science, en zetten Open Science vaak op hetzelfde niveau als andere kernwaarden. Zij zien transparantie van onderzoek, open access publicaties en FAIR data als belangrijke waarde of norm voor hun activiteiten, en redeneren daarbij vanuit het principe "zo open als mogelijk, zo gesloten als nodig". Opvallend is dat kennisinstellingen op deze vraag niet alleen antwoord geven over hoe (onder andere) Open Science opgenomen is in hun kennisveiligheidsbeleid, maar dat zij soms ook andersom redeneren: kennisveiligheid is voor sommige instellingen onderdeel van het Open Science-beleid. De meeste instellingen maken daarbij de keuze om eerst te kiezen voor veiligheid, en binnen die kaders zo open mogelijk te opereren.

Kennisveiligheid en ethiek, inclusiviteit en non-discriminatie

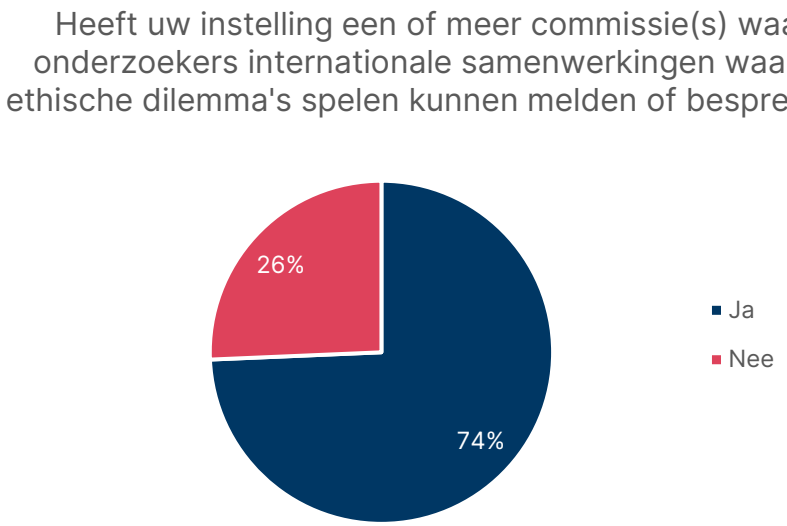
Veel onderzoeksdisciplines zijn in hoge mate internationaal georiënteerd. In de praktijk betekent dit dat onderzoekers gebruik maken van faciliteiten die slechts op enkele plekken ter wereld beschikbaar zijn, dat onderzoekers samenwerken met collega's uit andere landen of dat kennisinstellingen medewerkers aannemen die een internationale achtergrond hebben.

Het mitigeren van risico's op het gebied van kennisveiligheid vraagt van instellingen dat zij scherp zijn op samenwerking met personen en instellingen uit risicolanden. Het kan bijvoorbeeld zo zijn dat in Nederland ontwikkelde kennis gebruikt wordt door regimes die vrije wetenschapsbeoefening beperken of dat onderzoek vraagt om samenwerking met landen waar grondrechten niet worden gerespecteerd en de statelijke actor actief interfereert. Instellingen willen zorgen voor een veilige omgeving voor alle studenten en medewerkers, kennis van henzelf en samenwerkingspartners beschermen én tegelijk vrije samenwerking borgen en stigmatisering op basis van nationaliteit voorkomen. Dit is voor hen een complex dilemma.

Een aantal instellingen (voornamelijk hogescholen) heeft op dit moment geen beleid op het gebied van inclusiviteit en non-discriminatie *specifiek in het kader van kennisveiligheid*, omdat zij dit niet relevant vinden voor het type onderzoek dat aan hun instelling wordt uitgevoerd. Veel andere instellingen zouden graag het niveau een stap omhoog willen brengen. Over het algemeen geven instellingen aan dat ze reactief al veel doen, maar dat de bijbehorende beleidsprocessen daarbij nog niet ingeregeld hebben.

2.3 Het bespreken van dilemma's bij kennisveiligheid

Hiervoor hebben we weergegeven welke dilemma's instellingen zien als het gaat om hun kernwaarden en kennisveiligheid. De genoemde dilemma's kunnen zich voordoen op het niveau van beleid of op het niveau van individuele samenwerkingen of personeelsbeleidvraagstukken. In de case-study zien we dat het vaak gaat over dilemma's op het gebied van internationale samenwerking: kan in onderzoeken nog samengewerkt worden met kennisinstellingen uit risicolanden?



Figuur 2. Aanwezigheid commissies ter bespreking van ethische dilemma's

Ongeveer driekwart van de instellingen geeft aan commissie(s) te hebben waar onderzoekers zich kunnen melden of bespreken als deze samenwerkingen zorgen voor ethische dilemma's (zie Figuur 2). In de toelichting in de vragenlijst en in de cases zien we vier mogelijke vormen van deze commissies:

1) Een algemene onderzoekscommissie of ethische commissie, waar het thema kennisveiligheid (inclusief gevoelige samenwerkingen) ook besproken wordt. Andere genoemde

thema's die behandeld worden in dit soort commissies zijn bijvoorbeeld Open Science, wetenschappelijke integriteit en kwaliteitszorg. Deze commissies bestaan zowel op centraal niveau binnen instellingen als op faculteitsniveau.

2) Een aparte commissie die speciaal is ingericht voor kennisveiligheid. Deze commissies hebben in de regel een grote overlap met het adviesteam kennisveiligheid.
3) Een aparte commissie voor gevoelige samenwerking buiten kennisveiligheid om. Deze commissies richten zich vaak ook op ethische overwegingen buiten kennisveiligheid om, zoals vraagstukken over samenwerking met diverse externe partijen (bijvoorbeeld fossiele industrie of grote techbedrijven). Deze afwegingen worden nadrukkelijk niet gezien als kennisveiligheid. Sterker nog: sommige respondenten spreken de zorg uit dat deze samenwerkingen niet meer wordt aangegaan onder het mom van kennisveiligheid, terwijl het volgens hen daar niet aan gerelateerd is.
4) Een aantal instellingen heeft een individuele medewerker aangesteld die aanspreekpunt is bij vraagstukken op het gebied van kennisveiligheid.

Deze aanspreekpunten en commissies worden ingevuld op verschillende niveaus, zoals bijvoorbeeld op faculteitsniveau, op instellingsniveau of als onderdeel van het instellingsbestuur. Een aantal instellingen heeft commissies of aanspreekpunten op meerdere van deze niveaus. Instellingen die volgens de vragenlijst geen commissie(s) hebben, lichten vaak toe dat het instellen van een commissie voor de aard van hun onderzoek niet relevant is of dat ze gebruik maken van een extern adviesorgaan of commissie die gedeeld is met andere instellingen. In het laatste geval hebben sommige instellingen de vraag of er een commissie is met 'ja' beantwoord, maar andere instellingen antwoordden ontkennend. Eén instelling geeft aan dat de commissie op korte termijn wordt ingesteld.

Uit de toelichtingen in de cases en de vragenlijst blijkt dat de commissies of aanspreekpunten voor ethische dilemma's in een aantal instellingen een steeds 'formelere' plaats krijgen. Hun (initieel) tijdelijke status verandert bijvoorbeeld in een permanente verankering in het instellingsbeleid. Ze worden vaker standaard betrokken bij het opzetten van nieuwe (internationale) samenwerkingen of onderzoek. Bij andere instellingen denken commissies vooral mee op verzoek van een onderzoeker, maar niet als standaardpraktijk. Een aantal instellingen geeft aan dat dit ook vaker gebeurt: onderzoekers herkennen steeds vaker vraagstukken op het gebied van kennisveiligheid en weten de commissies of aanspreekpunten met deze vraagstukken te vinden.

Inhoudelijk valt op dat instellingen op verschillende manieren onderscheid maken tussen ethische dilemma's en kennisveiligheidsdilemma's - ondanks dat ethische kwesties een onderdeel van de Leidraad zijn, mits gekoppeld aan interferentie door een statelijke actor. Risico's rond het mogelijke misbruik van specifieke onderzoeksresultaten worden onder kennisveiligheid geschaard. In de

Leidraad wordt bij ethiek rondom kennisveiligheid verwezen naar samenwerking met zowel instellingen als personen (studenten of onderzoekers) uit risicolanden. Dit begrip wordt daarmee dus breder ingevuld dan de focus op onderzoek of resultaten daarvan.

Meerdere instellingen geven aan dat het adresseren van vraagstukken op instellingsniveau een complexe taak is en dat het wenselijk is dat dit meer integraal wordt aangepakt. De afwegingen over bijvoorbeeld gevoelige samenwerkingen kunnen nu verschillen per instelling, wat niet altijd als wenselijk wordt gezien. Sommige instellingen kiezen er soms voor om zelf keuzes maken over het wel of niet uitsluiten van bepaalde risicolanden, waarbij ze aangeven te hopen op een concrete richtlijn vanuit de Rijksoverheid. Dit zou (de schijn van) arbitraire keuzes op het gebied van kennisveiligheid kunnen voorkomen.

Op het vlak van internationale samenwerkingen zien we verbreding van de dilemma's rondom samenwerking met risicolanden en andere samenwerkingspartners. Instellingen zijn naar samenwerking met sommige landen anders gaan kijken in de afgelopen jaren waardoor het al bestaande dilemma rondom internationale samenwerking vaker speelt. Dit soort dilemma's worden in de hierboven beschreven gremia beschreven.

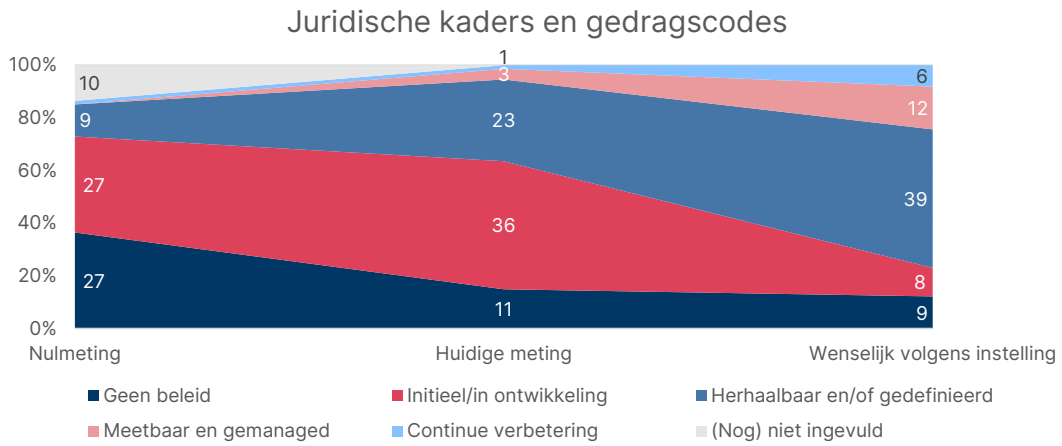
3 Juridische kaders en gedragscodes

Samenvatting

- Stand 2026: Nagenoeg alle instellingen bereiken minimaal een initieel niveau bij de vertaalslag van juridische kaders (zoals sanctie- en exportwetgeving) naar interne procedures.
- Stappen ten opzichte van nulmeting: Er is een duidelijke professionaliserings-slag gemaakt, instellingen zijn van individuele alertheid naar procedurele borging in de vorm van protocollen gegaan. Het aantal instellingen zonder specifiek beleid is gehalveerd.
- Vinden instellingen zichzelf ver genoeg gegeven hun risicoprofiel? Veel instellingen willen doorgroeien naar meetbare, cyclische processen. De realisatie hiervan stuit op de inhoudelijke complexiteit van de materie. Veel instellingen met een lager risicoprofiel vinden zich op dit thema wél ver genoeg ontwikkeld. Zij kiezen bewust voor een beperkte inzet omdat zij zware compliance-structuren voor hun lage risicoprofiel niet proportioneel vinden.
- Keuzes en dilemma's: Het voornaamste dilemma voor instellingen die hier wel risico's op signaleren is recht doen aan de complexe regelgeving met balans tussen input van de werkvloer, inzet van specifieke expertise en de beschikbare middelen.

Voor onderdelen van het kennisveiligheidsbeleid gelden een aantal bestaande juridische kaders en gedragscodes, zoals sanctie- en exportcontroleregelgeving. In dit hoofdstuk analyseren we in hoeverre de kennisinstellingen er volgens henzelf in zijn geslaagd om relevante wet- en regelgeving – zoals exportcontrole en sanctiewetgeving - in de context van kennisveiligheid te vertalen naar interne procedures.

3.1 Ontwikkeling beleid juridische kaders en gedragscodes



Figuur 3. Ontwikkeling van instellingen: beleid omtrent juridische kaders en gedragscodes

Wanneer we kijken naar de sector als geheel, is de belangrijkste conclusie dat de volwassenheid toegenomen is. Bij de nulmeting bevond een groot deel van de instellingen zich nog in de fase waarin er geen specifiek beleid op het gebied van juridische kaders voor kennisveiligheid (27 instellingen) en hadden 10 instellingen dit niet ingevuld. Dit beeld is bij de huidige meting gekanteld: het aantal instellingen op niveau 1 is meer dan gehalveerd tot elf en alle instellingen hebben zichzelf nu gescoord. De grootste groep (36) instellingen bevindt zich nu op niveau 2 ('Initieel/in ontwikkeling'). Uit de kwalitatieve toelichting blijkt dat dit concreet betekent: processen zijn gestart, maar implementatie is meestal nog tamelijk ad hoc. Een instelling geeft bijvoorbeeld aan dat dat er wel een werkgroep is ingericht, maar dat naleving nog sterk leunt op de eigen verantwoordelijkheid van de onderzoekers zelf.

Voor de groep van 23 instellingen die aangeven inmiddels het niveau 'Herhaalbaar en/of gedefinieerd' te hebben bereikt, zien we dat de naleving van juridische kaders en gedragscodes een vaster onderdeel is geworden van werkprocessen. Het grootste verschil met de groep die zich nog op het niveau 'initieel/in ontwikkeling' bevindt, is de aanwezigheid van vaste protocollen die consistent worden toegepast en een adviesteam dat per casus steeds dezelfde werkwijze hanteert. Een praktijkvoorbeeld uit een case illustreert dit verschil. Een instelling geeft aan dat tegenwoordig de HR-afdeling potentiële risico's signaleert, als onderdeel van de sollicitatieprocedure, en aan de bel trekt bij het adviesteam. Voorheen lag dit bij de onderzoeker zelf, en deden individuele onderzoekers zelf adviesaanvragen bij het Loket Kennisveiligheid. Inmiddels wordt dat altijd vanuit het adviesteam gedaan.

Het onderscheid tussen niveau 'herhaal en/of gedefinieerd' en 'meetbaar en gemanaged' lijkt op dit onderdeel dat tussen een advies dat al dan niet kan worden gevraagd en opgevolgd versus de aanwezigheid van dwang. Een van de weinige instellingen die zichzelf op niveau 'meetbaar en gemanaged' heeft geplaatst, licht toe dat de juridische check verplicht moet worden doorlopen voor het aangaan van elke internationale samenwerking of het aanstellen van elke nieuw vaste of tijdelijke medewerker. Het is dan dus niet mogelijk een nieuwe medewerker aan te nemen zonder dat de juridische vink is gezet. Eén universiteit geeft aan niveau 'continue verbetering' te bereiken, met als uitleg dat ze het juridisch kader in het afgelopen half jaar meermaals hebben geëvalueerd en aangescherpt.

De cases bij hogescholen laten zien dat zij bewust zoeken naar een proportionele inrichting van kennisveiligheidsbeleid, passend bij hun uiteenlopende risicoprofielen. Die proportionaliteit krijgt in de praktijk op verschillende manieren vorm: sommige hogescholen werken met een breed stroomschema of toetsingskader voor internationale samenwerkingen, terwijl andere vooral kiezen voor jaarlijkse checks, bewustwording en toetsing bij nieuwe of risicovolle partnerschappen. In de gesprekken benadrukken verschillende hogescholen dat zij willen voorkomen dat procedures vooral op papier bestaan, zonder goed aan te sluiten op hun feitelijke risico's en uitvoeringspraktijk. Vanuit die ervaring geven enkele bezochte hogescholen aan dat één uniforme Leidraad niet altijd logisch uitwerkt, omdat op papier vergelijkbare verwachtingen ontstaan voor instellingen met sterk verschillende risicoprofielen. De uitdaging ligt daarmee in differentiatie: stevige kaders waar de risico's daarom vragen, en een lichtere, proportionele invulling waar dat verdedigbaar is.

De uitdaging voor de groep die volgens zichzelf nog stappen moet maken (de 57% met een hoger ambitieniveau dan nu al gerealiseerd) ligt vooral in de toepassing van beleid. Verdere stappen worden met name belemmerd door de complexiteit van de materie. Verschillende instellingen geven in hun vragenlijsten aan dat individuele onderzoekers niet de expertise en tijd hebben om documenten zoals de EU sanctielijst, *EU guidelines on tackling foreign interference* of de dual-use verordening te lezen en goed te interpreteren. Het gevolg is dat kennis over sanctiewetgeving bij onderzoekers vaak niet of nauwelijks aanwezig is. Ook is bij de juridische afdeling de capaciteit en kennis om de vertaalslag van complexe wetgeving naar antwoorden op concrete vragen te maken soms beperkt, waardoor instellingen gedwongen zijn externe deskundigheid in te zetten. Vanuit deze ervaringen is er vraag naar toegankelijker samenvattingen, overzichten of praktisch beoordelingskaders gebaseerd op de onderliggende wet- en regelgeving.

De cases bevestigen dit beeld: de wetgeving is ingewikkeld en de geboden hulpmiddelen onvoldoende bruikbaar. Ook komen hier kritische geluiden over de toepasbaarheid van de EU dual-use verordening naar voren. Kennisinstellingen onderzoeken bovendien vaak losse componenten in plaats van eindproducten. Dit maakt de toepassing van regels over exportcontrole extra

ingewikkeld. Dus ook ondersteuning bij de interpretatie en toepassing van de ingewikkelde brondocumenten is gewenst. Een deel van de instellingen heeft de (juridische) kernvragen die onderzoekers moeten beantwoorden samengevat in een stroomschema of beslisboom, als opmaat voor een verdere inhoudelijke afweging door het adviesteam of een coördinator.

3.2 Concrete kaders en codes

Na de algemene rubric over het beleid van instellingen rondom juridische kaders en gedragscodes, vroegen we hen ook naar hun omgang met en ondersteuningsbehoefte op specifieke dossiers.

EU-exportcontrole en bepaling dual-use

De naleving van EU-exportcontrole is voor veel instellingen een groeiend aandachtsgebied. Waar kennisinstellingen met een technisch profiel dit vaak al procesmatig hebben ingericht (bijvoorbeeld via verplichte checks door experts), worstelen brede kennisinstellingen met de vraag of hoezeer deze wetgeving voor hen van toepassing is. Zij geven aan dat wetgeving voor exportcontrole slechts voor een klein deel van de organisatie geldt (bijvoorbeeld één bèta-faculteit), maar dat de wetgeving wel organisatiebrede compliance vereist. Dit leidt tot een zoektocht naar proportionaliteit: hoe tuig je beleid op dat niet de hele organisatie belast, maar wel de specifieke risico's afvangt?

Ook geven veel instellingen aan dat de vertaalslag van de complexe juridische regels naar de werkvloer erg lastig is. Alle type instellingen hebben behoefte aan duidelijkere richtlijnen, die meer gericht zijn op kennisinstellingen en aan versimpelde handvatten voor het beoordelen van wet en regelgeving.

Bepalen of een onderzoek mogelijke *dual-use* toepassing heeft, blijkt zeer complex en tijdrovend. De betreffende wetenschappers moeten hierbij altijd de inhoudelijke afweging ondersteunen, omdat zij de techniek het beste doorgronden. De afweging rond Technology Readiness Levels (TRL) compliceert dit vraagstuk aanzienlijk. Laag TRL-onderzoek is fundamenteel zonder directe toepassing, maar kent soms toch aanzienlijke risico's. De huidige conceptlijsten vinden onderzoekers vaak veel te generiek. Zij missen werkbare, specifieke beoordelingskaders voor hun eigen onderzoeksdomein. De roep om "gebruiksvriendelijke handvatten" leeft zeer breed: men wil geen beleidsdocumenten van 60 pagina's, maar beslisbomen, factsheets en voor kennisinstellingen aangepaste kaders die direct in de bedrijfsvoering kunnen worden gebruikt. Het grondig uitvoeren van checks vraagt (anders) om gespecialiseerd personeel dat schaars en duur is en een toename van (interne) administratieve druk en overhead.

Naast een behoefte aan concrete beoordelingskaders die werkbaar zijn voor de wetenschap, geven ook enkele instellingen aan dat ze over onvoldoende kennis en expertise beschikken om de exportverordening te interpreteren en te implementeren. In dit kader uiten enkele instellingen hun teleurstelling over de ondersteuning vanuit het Loket Kennisveiligheid. Zij geven aan dat adviezen voor concrete casuïstiek – bijvoorbeeld op het gebied van kwantumtechnologie – vaak onvoldoende praktisch toepasbaar zijn (geweest). De breed gedeelde conclusie is dat instellingen behoefte hebben aan duidelijkere richtlijnen, concretere kaders en meer toegespitste operationele ondersteuning.

Compliance sanctieregimes

Het merendeel van de sector, met name de hogescholen en niet-technische instellingen, vindt compliance met niet-EU sanctieregels of niet-EU exportcontrolemechanismen niet of nauwelijks relevant. De instellingen waar dit wel speelt – voornamelijk instellingen met een technisch profiel - hebben dit vaak contractueel afgedekt. De naleving is hierdoor vaak ad-hoc: pas als een contract met bijvoorbeeld een Amerikaanse partner of leverancier dit vereist, wordt er actie ondernomen. Er is minder sprake van proactief beleid dan bij de EU-exportregels. Een enkele instelling geeft aan dat de groeiende samenwerking met Defensie of partijen in de VS zal leiden tot een toenemende noodzaak om ook deze expertise structureel in huis te halen.

Voor een deel van de sanctiecompliance – met name het screenen van namen en entiteiten op sanctielijsten – geven instellingen aan dat deze toetsing relatief goed in bestaande inkoop- en samenwerkingsprocedures is in te passen. Sommige instellingen maken hiervoor gebruik van commerciële screeningtools, zoals die van Dun & Bradstreet. Dat betekent echter niet dat naleving van sanctieregimes als geheel eenvoudig of verder uitgekristalliseerd is dan exportcontrole. De interpretatie van met name verboden technische bijstand blijkt in de praktijk complex. Het gaat daarbij niet alleen om lijstchecks, maar ook om de vraag wanneer instructie, training, advies of het delen van praktische kennis onder sanctieregimes verboden is. In de vragenlijsten en interviews geven instellingen aan dat zij juist op dit punt behoefte hebben aan beter hanteerbare interpretatiekaders en ondersteuning.

Toepassing Leidraad

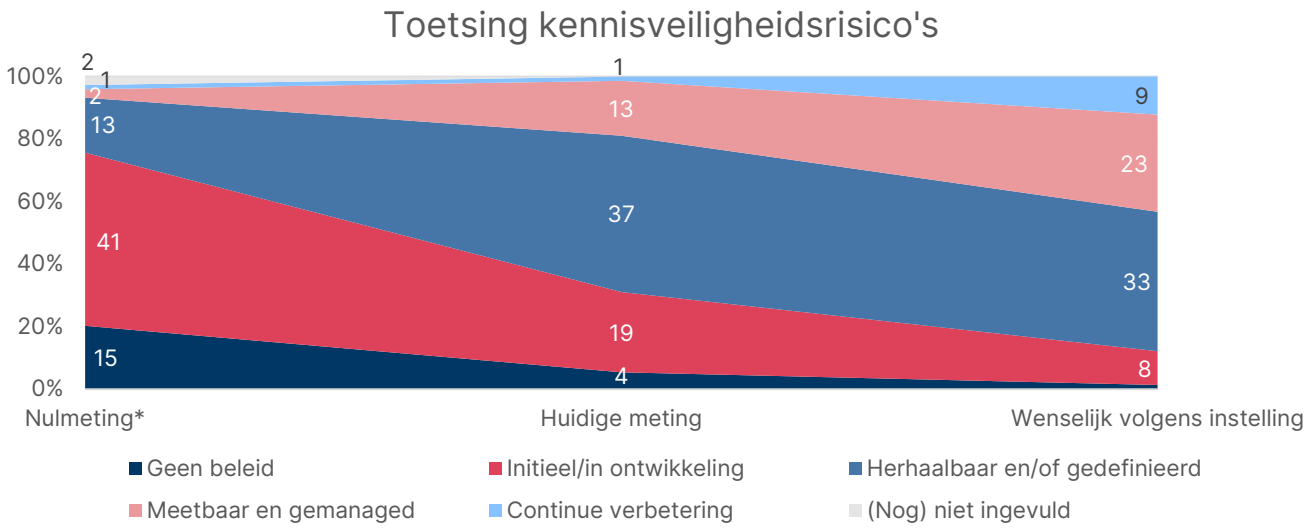
De Nationale Leidraad vormt voor alle instellingen het primaire ankerpunt van hun kennisveiligheidsbeleid. Instellingen vertalen deze lokaal naar hun eigen, specifieke toetsingskaders en procedures. Bij internationale samenwerkingen stuiten zij echter regelmatig op problemen hierin. Verschillende landen hanteren soms sterk afwijkend kennisveiligheidsbeleid. Dit levert in de praktijk zeer complexe juridische knopen op en het dwingt instellingen soms om waardevolle consortia voortijdig af te breken.

4 Het inschatten van risico's

Samenvatting

- Stand 2026: De grootste groep instellingen beschikt over vastgestelde toetsingskaders en procedures voor risico-inschatting (niveau 3).
- Stappen ten opzichte van nulmeting: Een duidelijke professionaliseringsslag is gemaakt: van een ad-hoc benadering naar procedures, logboeken, kaders en gestructureerde adviesteams.
- Vinden instellingen zichzelf ver genoeg gegeven hun risicoprofiel? Het beeld is gemengd. Een grote groep wil nog doorgroeien naar cyclisch geëvalueerde processen (niveau 4). Instellingen met een lager risicoprofiel vinden hun huidige niveau (bijv. een jaarlijkse analyse) proportioneel en adequaat.
- Keuzes en dilemma's. Dilemma's ontstaan doordat concepten zoals 'kroonjuwelen' en generieke conceptlijsten in de uitvoering vragen oproepen, met name rondom fundamenteel onderzoek (lage TRL-niveaus). Instellingen worstelen ook met het gebrek aan toegankelijke tools voor affiliatiecontrole.

4.1 Toetsing kennisveiligheidsrisico's



Figuur 4. Ontwikkeling van instellingen: beleid omtrent toetsing kennisveiligheidsrisico's

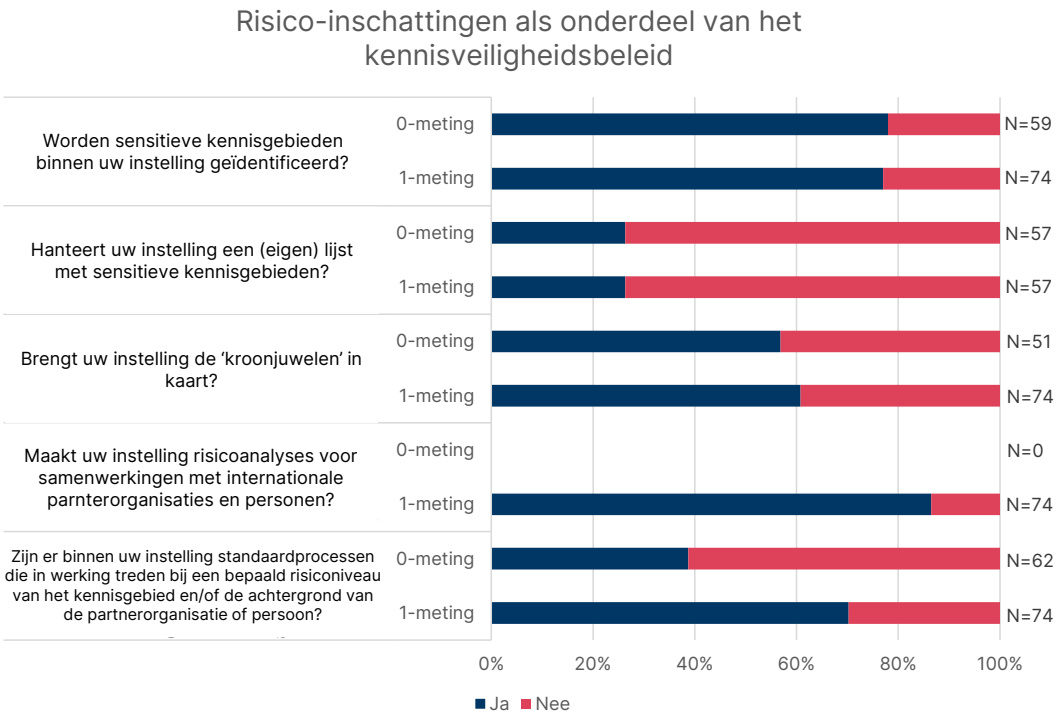
De Leidraad is bij de meeste instellingen op dit thema geïmplementeerd. De grootste groep instellingen (37) geeft op de huidige meting aan dat het beleid zich bevindt op niveau 'herhaalbaar en/of gedefinieerd'. Dit betekent dat binnen deze instellingen een expliciete risicobeoordelingsprocedure of een toetsingskader is vastgelegd. Uit de toelichting blijkt dat instellingen dit niveau vooral verbinden aan het inrichten van een beoordelingsproces maar ook aan het aanstellen van een contactpersoon en/of portefeuillehouder kennisveiligheid (zie ook hoofdstuk 5) en het vastleggen van hun verantwoordelijkheden rondom uitvoering en toezicht. In de praktijk krijgt dit niveau bijvoorbeeld vorm doordat adviesteams steeds vaker werken met bijvoorbeeld een levend document waarin eerdere casuïstiek wordt bijgehouden, wat zorgt voor een consistente risicoweging over verschillende afdelingen heen.

De sector is op dit vlak duidelijk volwassener geworden sinds de nulmeting. Het aandeel instellingen zonder beleid of met uitsluitend ad-hoc benaderingen is ten opzichte van de nulmeting sterk afgenomen. Dertien instellingen geven aan dat zij zich inmiddels bevinden op niveau 'meetbaar en gemanaged' – in de nulmeting waren dat er slechts twee. Dit houdt in dat kennisveiligheidsrisico's periodiek worden geëvalueerd en dat de risicobeoordelingsmethodologie actief wordt verbeterd. Het belangrijkste onderscheid met niveau 'herhaalbaar en/of gedefinieerd' is daarmee de aanwezigheid van een vastgestelde evaluatiecyclus, waarin evaluatie en bijstelling structureel zijn ingeregeld. Daarnaast geeft slechts één instelling aan te opereren op het niveau van continue verbetering, waarbij kennisveiligheid structureel is ingebed in bredere evaluatie- en verbetercycli. In de kwalitatieve toelichting benadrukt deze instelling dat medewerkers laagdrempelig terecht kunnen voor vragen en ondersteuning aangaande de risicobeoordeling.

Wat betreft het wenselijke niveau geven instellingen aan dat er de komende jaren nog ontwikkelmogelijkheden zijn. De meeste instellingen (33) geven aan dat voor hun instelling niveau 'herhaalbaar en/of gedefinieerd' wenselijk is: een gedefinieerde risicobeoordelingsprocedure of een toetsingskader. Daarnaast geven 23 instellingen aan dat zij het wenselijk vinden dat er sprake is van periodieke evaluatie en verbetering van de risicobeoordelingsmethodologie (niveau 'meetbaar en gemanaged'.

De reikwijdte van risico-inschattingen is met name bij universiteiten een knelpunt voor de doorontwikkeling. De cases laten zien dat een risico-inschatting op het niveau van een heel vakgebied lastig is. Instellingen benadrukken dat het risico zich veel vaker op projectniveau bevindt dan op het niveau van een heel vakgebied. Een te generieke screening leidt volgens hen tot onwerkbare administratieve druk. Voor veel instellingen met een lager risiconiveau is een jaarlijkse, overkoepelende risicoanalyse juist een bewuste, proportionele keuze.

4.2 Risico-inschatting als onderdeel van het kennisveiligheidsbeleid



Figuur 5. De risico-inschattingen die instellingen maken als onderdeel van het kennisveiligheidsbeleid

De meeste instellingen (57 van de 74, alle universiteiten) geven aan dat sensitieve kennisgebieden binnen hun instelling worden geïdentificeerd. De instellingen die dit doen, geven bijna allemaal aan dat ze dit niet op basis van een (eigen) lijst hebben gedaan. Zij maken veelal gebruik van bestaande lijsten zoals de conceptlijst sensitieve technologie van OCW, de TIM dual-use lijst en een lijst met sleuteltechnologieën van TNO.

Vierenveertig instellingen brengen hun kroonjuwelen in kaart, veelal in overleg met faculteiten en via de KWAS-vragenlijst die in de eerste fase van het kennisveiligheidsbeleid een rol speelde. In de praktijk blijkt deze risico-inschatting echter weerbarstig. In één case werd expliciet benoemd dat het begrip 'kroonjuwelen' voor onderzoekers verwarrend kan zijn, omdat het minder goed aansluit op de huidige, concretere risicoafweging aan de hand van uniforme risico-indicatoren en beslisbomen.

Daarnaast ontbreekt volgens instellingen in de landelijke lijsten vaak de nuance rondom de zogeheten Technology Readiness Levels (TRL). Kennisinstellingen werken vaak aan fundamenteel onderzoek (laag TRL), wat een ander veiligheidsrisico met zich meebrengt dan technologie die al

dusdanig vergevorderd is dat hij in de operationele omgeving gedemonstreerd is (hoog TRL). Ook ziet men verschillen in het onderzoeken of ontwikkelen van technologie of het gebruik van bepaalde (*off the shelf*) technologie in een onderzoek. De afwezigheid van dit onderscheid compliceert de interne risicoweging aanzienlijk.

4.3 Internationale partnerorganisaties en personen

Verreweg de meeste instellingen (64 van de 74) maken risicoanalyses voor samenwerkingen met internationale partnerorganisaties en personen. De meeste instellingen doen dit op het moment dat er een nieuwe samenwerking wordt aangegaan, of wanneer deze noodzaak blijkt uit een interne beslisboom. Bij het doorlopen van zo'n beslisboom fungeren zaken als een risicoland, militaire affiliaties of negatieve reisadviezen als rode vlaggen die leiden tot een weging door een centraal adviesteam. De instellingen voeren deze risicoanalyses vaak uit aan de hand van openbare bronnen, de Leidraad, de nieuw ontwikkelde appendix bij de Leidraad[4] en EU- en VN-sanctielijsten. Bij het wegen van affiliaties, banden van onderzoekers of instituten met statelijke of militaire organisaties in China mist de hele sector de ASPI-tracker. Veel instellingen maakten voor affiliatiecontroles intensief gebruik van deze database. Nu deze database achter een commerciële betaalmuur is geplaatst, is de risico-inschatting voor hen bemoeilijkt.

Tot slot hebben de meeste instellingen (52 van de 74) standaardprocessen die in werking treden bij een bepaald risiconiveau van het kennisgebied of de partner. Bij veel van deze instellingen wordt bij een hoger risiconiveau (na de initiële weging door het adviesteam) het uiteindelijke besluit geëscaleerd naar een hoger bestuursniveau, meestal de portefeuillehouder of het bestuur. Uit de case studies blijkt dat op dit niveau binnen sommige instellingen bijvoorbeeld is besloten om, op basis van zelfontwikkelde kaders, samenwerkingen met instellingen uit bepaalde landen überhaupt niet meer aan te gaan.

[4] Deze appendix, Indicatoren voor Risico-inschatting Internationale Samenwerkingen Kennisveiligheid (2025) is gezamenlijk ontwikkeld door de kennisinstellingen en de Rijksoverheid.

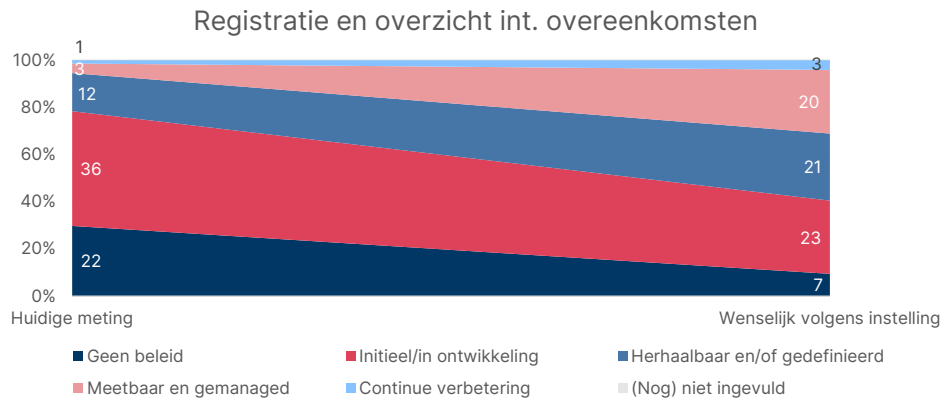
5 Risicomanagement

Samenvatting

- Stand 2026: Verantwoordelijkheden (portefeuillehouders, adviesteams) zijn bij bijna alle instellingen formeel belegd. Instellingen (waaronder alle universiteiten) hebben een overzicht van internationale samenwerkingen.
- Stappen ten opzichte van nulmeting: De inrichting van verantwoordelijkheden en de registratie van risico's is fors geprofessionaliseerd, formele adviesteams zijn opgericht en structureel geborgd.
- Vinden instellingen zichzelf ver genoeg gegeven hun risicoprofiel? Voor een derde van de sector is de volwassenheid van hun beleid omtrent risicomanagement voor nu voldoende, de helft van de instellingen wil nog verder ontwikkelen, vooral op het verbeteren van registratiesystemen.
- Keuzes en dilemma's: Ten aanzien van registratie werken vooral grote bredere instellingen nog aan goede, integraal en centrale registers. Instellingen met een lager risicoprofiel vinden zware lasten m.b.t registratie, processen en functies voor risicomanagement niet proportioneel.

5.1 Registratie internationale samenwerkingen

Van registreren naar registers



Figuur 6. Ontwikkeling van instellingen: beleid omtrent het registreren en overzicht houden van internationale overeenkomsten

De grootste groep instellingen (36 instellingen, 49%) bevindt zich op niveau 'Initieel/in ontwikkeling'. Er is op dit niveau wel overkoepelend zicht op partnerschappen, maar dit is vaak reactief en arbeidsintensief. Instellingen op dit niveau geven aan dat overzichten afhankelijk zijn van handmatig verzamelen binnen de faculteiten of dat lijsten op verschillende plekken in de organisatie worden geregistreerd, wat analyse lastig maakt. De stap naar de groep van 16% op niveau 3 'herhaalbaar' markeert de overgang van incidentele lijsten naar structurele borging in een centraal systeem. Universiteiten hebben allemaal een centraal overzicht van internationale partnerschappen dat periodiek en handmatig geactualiseerd wordt. Dit is een duidelijke vooruitgang ten opzichte van de nulmeting toen een universiteit dit had[5].

Bijna één derde (22 instellingen, 30%) van de instellingen geeft aan geen beleid op dit vlak te hebben. Het onderscheid met niveau 'initieel/in ontwikkeling' is dat hier vaak nog geen actieve inventarisatie plaatsvindt, ook niet handmatig. Vaak wordt door instellingen uit deze groep opgemerkt dat een centrale administratie (nog) niet als noodzakelijk wordt gezien, gezien het lage risicoprofiel of de kleinschaligheid van de instelling. Instellingen in deze groep geven aan dat registratie niet formeel geborgd is of volledig is belegd bij de individuele of onderzoeker, zonder dat er een centrale terugkoppeling is.

De helft van de sector vindt dan ook dat ze nog één volwassenheidsniveau moet stijgen om hun ambitie te halen. Dit is vaak de stap van een ad hoc lijst (niveau 'initieel/in ontwikkeling') naar een structureel register (niveau 'herhaalbaar/gedefinieerd'. Ook geven 22 instellingen aan dat niveau 'initieel/in ontwikkeling' voor hen voldoende is, meestal vanwege een beperkt aantal internationale partnerschappen.

Voor universiteiten lijkt deze uitdaging het grootst vanwege hun omvang en decentrale structuur. Faculteiten hebben traditioneel veel autonomie en een eigen administratie. Uit de toelichtingen blijkt dat universiteiten momenteel vaak werken met handmatige uitvragen of tijdelijke oplossingen om aan de informatiebehoefte te voldoen. Er wordt op dit moment wel geïnvesteerd in nieuwe systemen. Eén universiteit werkt bijvoorbeeld aan een centraal registratiesysteem dat vanaf 2028 operationeel moet zijn. In het verlengde hiervan leeft de nadrukkelijke wens om deze centrale registratie in de toekomst direct te koppelen aan geautomatiseerde affiliatiecontroles (due diligence tools), al hikken instellingen aan tegen de complexiteit en kosten om dit te bouwen.

[5] Zie hiervoor pagina 31 van het sectorbeeld kennisveiligheid universiteiten 2023

Bij hogescholen is de registratie van onderwijspartners (voor stages en uitwisselingen, vaak Erasmus+) meestal al goed op orde via bureaus voor internationalisering, die nieuwe risicochecks in bestaande procedures konden inpassen. De registratie van onderzoekspartners is bij hogescholen vaak minder ver ontwikkeld en meestal afhankelijk van individuele lectoren. Veel (kleinere) hogescholen geven daarnaast aan dat het optuigen van een apart registratiesysteem voor hen op dit moment niet proportioneel is.

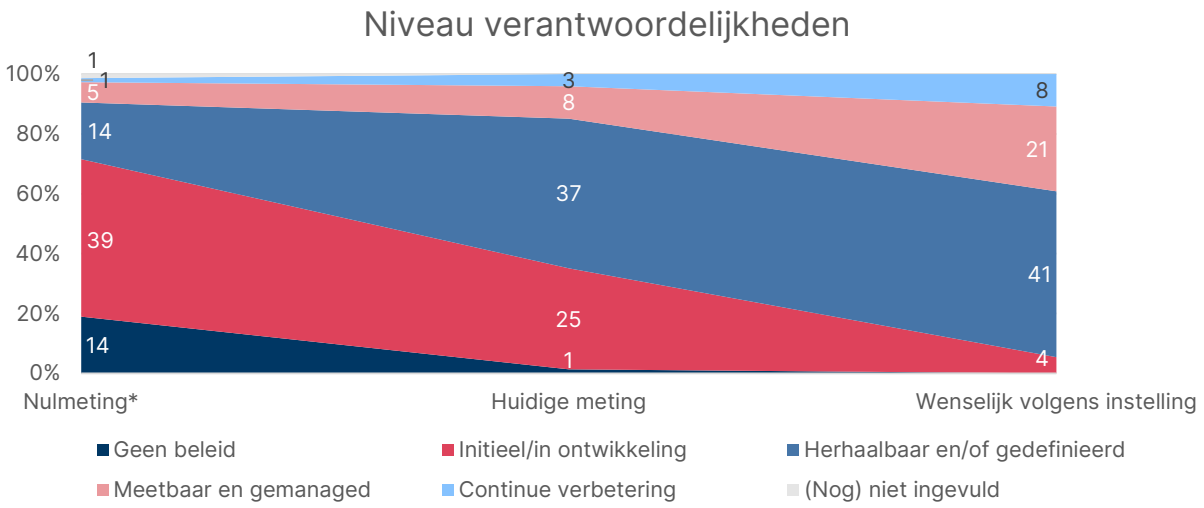
Veel instellingen geven dus aan dat contracten en samenwerkingen wel ergens geregistreerd staan, maar dat een 'druk op de knop' voor een totaaloverzicht nu nog niet mogelijk is. De kern van het probleem is vaak de historische inrichting van de systemen. Contracten voor onderzoek, onderwijs, en inkoop zitten vaak in gescheiden databases (bijv. SAP, Osiris, Mercell of specifieke CRM-systemen). Het samenbrengen van deze datastromen is een complexe IT- en governancepuzzel. De implementatie van robuuste, centrale systemen loopt in de praktijk bovendien soms forse vertraging op door een verloop onder schaars en gespecialiseerd IT- of securitypersoneel, hoorden we in verschillende cases. In de tussentijd roeien instellingen met de riemen die ze hebben; zo werken verschillende instellingen in afwachting van die integrale systemen tijdelijk met periodieke handmatige uitvragen die in losse Excel-bestanden worden bijgehouden. Uit de data blijkt dus dat het voor veel instellingen een lastige opgave is om te beschikken over een *real-time* actueel en centraal overzicht van hun internationale partnerschappen maar dat een overzicht dat jaarlijks geactualiseerd wordt goed lukt. De wens om in control te zijn botst vaak met de realiteit van decentrale systemen en versnipperde administraties.

Wat registreren instellingen?

Uit de uitkomsten van de vragenlijst blijken vrij grote verschillen in wat instellingen precies registreren over hun internationale partnerschappen. De basisregistratie omvat doorgaans NAW-gegevens van de partnerorganisatie, contactpersonen, de looptijd van de overeenkomst en financiële afspraken. Veel instellingen geven aan dat deze gegevens nodig zijn voor het functioneren van de samenwerking en daarom worden vastgelegd. Vanwege AVG-overwegingen noteren sommige instellingen alleen essentiële gegevens benodigd voor samenwerking en projectmanagement.

Een groep van zo'n 15 instellingen – met name onderzoeksinstellingen met een technisch profiel - gaat een stap verder en registreert ook standaard risico-indicatoren voor kennisveiligheid. Zij registreren bijvoorbeeld expliciet of een samenwerking betrekking heeft op sensitieve technologieën (vaak gebaseerd op de conceptlijst van de wet screening kennisveiligheid), of er sprake is van mogelijke *dual-use* toepassing, en wat het land van herkomst is (met speciale aandacht voor hoogrisicolanden). Soms verwijzen zij hierbij naar aanbevelingen uit de Leidraad Kennisveiligheid.

5.2 Niveau van verantwoordelijkheden en processen



Figuur 7. Ontwikkeling van instellingen: beleid omtrent het niveau van verantwoordelijkheden

Bijna alle instellingen hebben de verantwoordelijkheid voor het management van kennisveiligheids-risico's belegd. Daarmee heeft de sector sinds de nulmeting een duidelijke ontwikkeling doorgemaakt (zie figuur 7). In de nulmeting bevond het grootste deel van de instellingen zich nog in de fase van initieel/in ontwikkeling (39), waarin medewerkers zich op ad-hoc en informele basis bezighouden met kennisveiligheid. Daarnaast had een relatief groot aantal instellingen nog geen beleid (14).

In de huidige meting is dit beeld verschoven naar hogere niveaus, waarbij het zwaartepunt ligt op haalbaar en/of gedefinieerd (37). Dit betekent dat instellingen verantwoordelijkheden formeel hebben toegewezen en dat deze verantwoordelijkheden zijn gedocumenteerd. Uit de toelichting blijkt dat dit voor instellingen onder meer inhoudt dat een formeel adviesteam kennisveiligheid is ingericht en dat een portefeuillehouder kennisveiligheid is aangesteld. We zien bij meerdere instellingen dat naast het centrale adviesteam ook decentraal contactpersonen kennisveiligheid worden aangesteld. Het doel hiervan is om geformaliseerde verantwoordelijkheden in de academische praktijk werkbaar te houden, te zorgen voor korte lijnen, en te zorgen voor kennisveiligheidsadviseurs met inhoudelijke kennis over bepaalde onderzoeksgebieden.

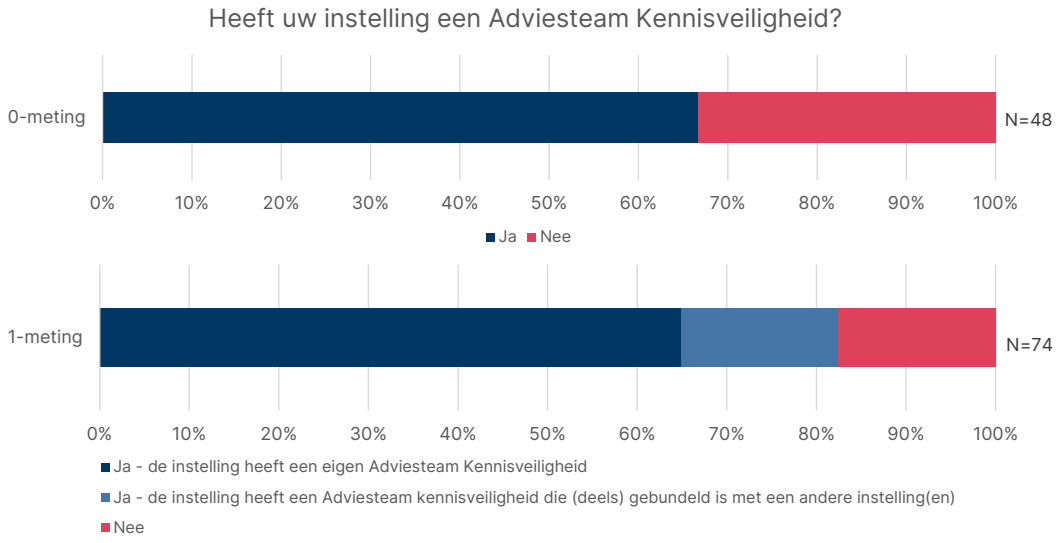
Acht instellingen bevinden zich op niveau 'meetbaar en gemanaged'. Het onderscheid met niveau 'herhaalbaar en/of gedefinieerd' is dat evaluatie en bijstelling structureel zijn ingericht als een periodiek proces. Binnen universiteiten is sprake van een duidelijke doorgroei; zij bevinden zich

uitsluitend op deze twee niveaus, binnen hogescholen is er ook ontwikkeling maar is het beeld in deze meting nog meer divers.

De meeste instellingen (41) zien niveau 'herhaalbaar en/of gedefinieerd' als de wenselijke eindsituatie, terwijl een substantiële groep wil doorgroeien naar de periodieke evaluatiecycli van niveau 'meetbaar en gemanaged'. Instellingen die zich in de huidige meting nog op initieel/in ontwikkeling bevinden (25), geven in de toelichting regelmatig aan dat kennisveiligheid binnen hun instelling beperkt speelt vanwege het karakter van de instelling.

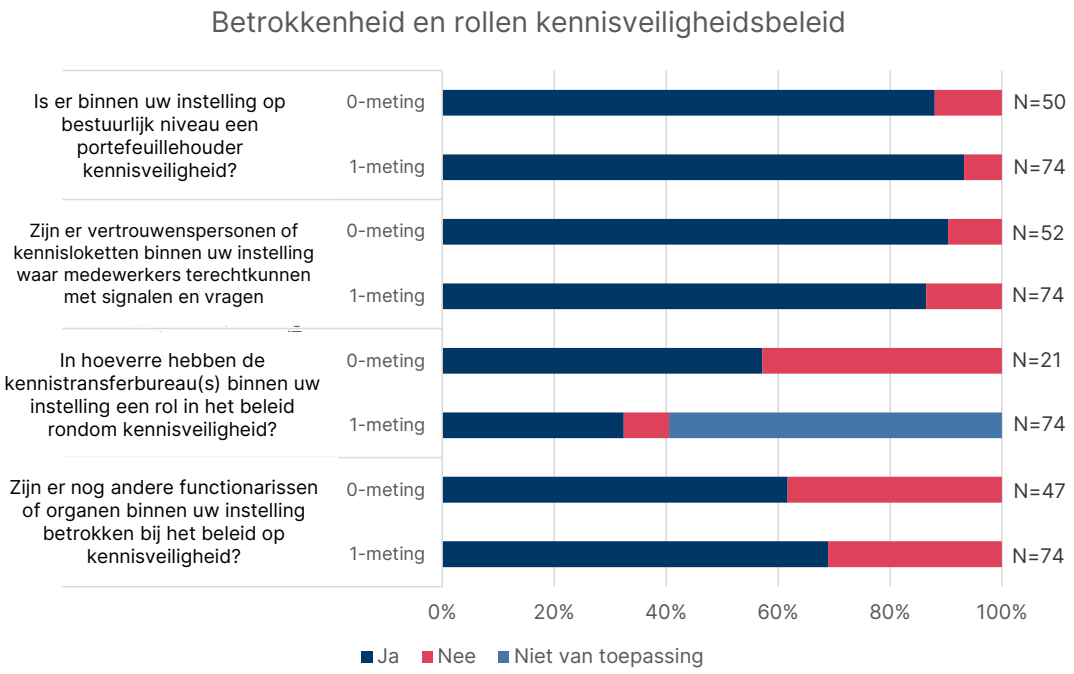
5.3 Invulling rollen kennisveiligheidsbeleid

Adviesteam kennisveiligheid



Figuur 81. Overzicht aanwezigheid van een adviesteam kennisveiligheid bij instellingen

De meeste instellingen – waarvan alle instellingen met een hoog risicoprofiel - hebben een eigen adviesteam kennisveiligheid. Deze teams zijn divers samengesteld, onder andere met (beleids)medewerkers Integrale Veiligheid, Juridische Zaken, CISO en HR. De praktijk laat zien dat de structurele aansluiting van HR bij deze teams een meerwaarde is, met name om veiligheidsrisico's al vroeg in sollicitatieprocedures te ondervangen. Kleinere kennisinstellingen kiezen er soms voor om het adviesteam te bundelen met andere instellingen om de collegiale belasting te verlagen.



Figuur 92. Overzicht van de rollen in en betrokkenen bij kennisveiligheidsbeleid

Portefeuillehouder kennisveiligheid

Bijna alle instellingen (71 van de 74) hebben op bestuurlijk niveau een portefeuillehouder. Deze functionaris heeft het mandaat over besluiten, veelal in samenspraak met het CvB, en draagt de eindverantwoordelijkheid voor het interne beleid. De drie andere instellingen zijn hogescholen, waarvan één er gezien het relatief geringe belang geen eigenstandige bestuurlijke portefeuille van maakt en twee er nog mee bezig zijn.

Vertrouwenspersonen

Bij 64 instellingen zijn er vertrouwenspersonen waar medewerkers terechtkunnen met signalen. Bij de helft van de instellingen deelt men specifieke kennisveiligheidsinformatie met deze personen of volgen zij trainingen. Uitdagingen blijven hier echter wel bestaan. De casuïstiek laat zien dat vertrouwenspersonen een rol kunnen spelen in het signaleren van risico's zoals heimelijke beïnvloeding of chantage van onderzoekers. Tegelijkertijd wordt geconstateerd dat internationale medewerkers die zijn opgegroeid in repressieve regimes dit soort institutionele loketten vaak wantrouwen.

Kennistransferbureau en overige functionarissen

Bij 24 instellingen speelt het kennistransferbureau (KTO) een actieve rol, met name vanwege de betrokkenheid bij de opzet van valorisatieprojecten waar veiligheidsrisico's kunnen spelen. Ook ICT-beheerders en stafdiensten worden door 51 instellingen genoemd als belangrijke uitvoerende partners binnen het beleid.

6 Fysieke en digitale beschermingsmaatregelen

Samenvatting

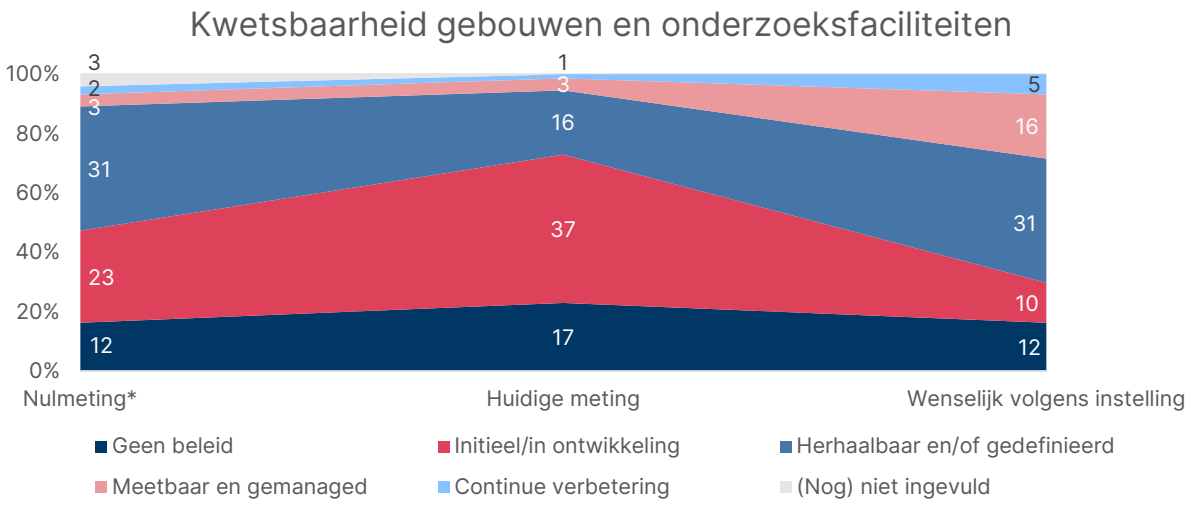
- Stand 2026: Ruim de helft van de instellingen (54 van de 74) heeft geen beleid of initieel beleid rondom fysieke beschermingsmaatregelen. Instellingen zijn zich bewust van de risico's die reisdelegaties meebrengen en hebben hier protocollen voor opgesteld. Ook is er beleid rondom werkgerelateerde reizen van eigen werknemers. Het aantal instellingen dat geen of initieel beleid heeft rondom digitale beschermingsmaatregels is kleiner (40 van de 74 instellingen).
- Stappen ten opzichte van nulmeting: De sector heeft weinig vooruitgang geboekt in de ontwikkeling van kennisveiligheidsbeleid rondom fysieke beschermingsmaatregelen. We zien dat de sector wel volwassener is geworden met betrekking tot beleid rondom digitale beschermingsmaatregelen. Het aantal instellingen dat rubricering toepast op sensitieve documenten is gelijk gebleven. Meer instellingen hebben een restrictief toegangsbeleid op onderzoeksgegevens en documenten geïmplementeerd.
- Vinden instellingen zichzelf ver genoeg gegeven hun risicoprofiel? De ambitieniveaus van instellingen liggen voor zowel fysieke als voor digitale beschermingsmaatregelen hoger dan het huidige niveau. Vier op de tien instellingen heeft het wenselijke niveau behaald voor beleid rondom fysieke en digitale beschermingsmaatregelen. Enkele (monosectorale) hogescholen en universiteiten geven aan dat zij gegeven hun risicoprofiel zichzelf als uitontwikkeld beschouwen.
- Keuzes en dilemma's: Instellingen benoemen weinig dilemma's met betrekking tot beleid rondom fysieke en digitale beschermingsmaatregelen. Wel is meermaals aangegeven dat het fysieke of digitale afschermen van sensitief onderzoek moeilijk uitvoerbaar en financieel kostbaar is. De open structuur van instellingen en de noodzaak de academische vrijheid te waarborgen maken het uitvoeren van afgeschermd onderzoek binnen een instelling complex. Een *good practice* is om te zorgen voor voldoende uitwisseling tussen kennisveiligheids- en cyberveiligheidsteams.

Een praktisch punt van aandacht binnen kennisveiligheid - nauw verbonden met risicomanagement - is de toegang tot fysieke en digitale omgevingen van instellingen. In andere woorden: het fysieke

en digitale toegangsbeleid. Het gaat hierbij om het voorkomen dat personen ongewenst toegang krijgen tot ruimtes en fysieke onderzoeksfaciliteiten of tot digitale gegevens. In dit hoofdstuk beschrijven we het toegangsbeleid van instellingen met betrekking tot fysieke middelen (paragraaf 6.1) en digitale middelen (paragraaf 6.2).

6.1 Fysieke beschermingsmaatregelen

De sector lijkt, ten opzichte van de nulmeting, weinig vooruitgang geboekt te hebben in de ontwikkeling van kennisveiligheidsbeleid rondom fysieke beschermingsmaatregelen – maar dit is niet met zekerheid te zeggen. Een directe vergelijking tussen de nulmeting en de huidige meting is namelijk niet volledig zuiver omdat instellingen tijdens de nulmeting in één vraag gevraagd te reflecteren op het beleid rondom digitale én fysieke beschermingsmaatregelen. Waar instellingen ten tijde van de nulmeting veelal herhaalbaar en/of gedefinieerd beleid hadden, geven ze nu vaker aan dat het beleid nog in ontwikkeling is (Figuur 10).



*Figuur 10. Ontwikkeling van instellingen: beleid omtrent de kwetsbaarheid van gebouwen en onderzoeksfaciliteiten. *Een directe vergelijking tussen de nulmeting en de huidige meting is niet volledig zuiver omdat instellingen tijdens de nulmeting in één vraag gevraagd te reflecteren op het beleid rondom digitale én fysieke beschermingsmaatregelen*

Enkele (monosectorale) hogescholen en universiteiten hebben geen beleid omtrent fysieke beschermingsmaatregelen en vinden zichzelf uitontwikkeld. Deze instellingen geven aan dat er op hun instelling geen sprake is van fysieke kwetsbaarheid van gebouwen in relatie tot kennisveiligheid. Bij instellingen die aangeven dat zij beleid in ontwikkeling ambiëren is vaak al wel toegangsbeleid geïmplementeerd, maar dit is niet specifiek op kennisveiligheid toegespitst. Omdat

fysieke toegang al geregeld is, heeft het doorontwikkelen van dit beleid met het oog op kennisveiligheid voor deze groep instellingen geen prioriteit.

In de gesprekken met instellingen is meermaals aangegeven dat het afschermen van sensitief onderzoek een uitdaging is voor de instelling. Ze geven aan dat een fysieke of digitale afscheiding moeilijk uitvoerbaar is – al wordt het als mitigerende maatregel al wel gedaan. Bovendien vinden instellingen deze mitigerende maatregel financieel kostbaar. De open cultuur van instellingen en de noodzaak de academische vrijheid te waarborgen maken het uitvoeren van afgeschermd onderzoek binnen een instelling complex. Het afschermen van onderzoek wordt bovendien complexer in contexten van consortia en multilaterale samenwerkingen, waarbij de controle over de uitvoering en de implementatie van veiligheidsmaatregelen minder direct is.

30 van de 74 instellingen (41%) hebben het wenselijke niveau voor beleid omtrent fysieke beschermingsmaatregelen ten tijde van de huidige meting reeds behaald. Logischerwijs geldt dit veelal voor instellingen met bescheiden ambities, hoewel ook enkele instellingen het wenselijkheidsniveau van beleid op niveau 'herhaalbaar en/of gedefinieerd' of niveau ´meetbaar en gemanaged' al hebben behaald.

6.2 Digitale beschermingsmaatregelen

Het beleid van instellingen rondom digitale beschermingsmaatregelen is over het algemeen volwassener dan het beleid rondom fysieke beschermingsmaatregelen. Dit geldt tevens voor de ambitieniveaus van de instellingen.

We zien dat de sector volwassener is geworden ten opzichte van de nulmeting, maar ook dat het gewenste volwassenheidsniveau nog niet is bereikt, zie Figuur 12. Echter is een directe vergelijking tussen de nulmeting en de huidige meting ook hier niet volledig zuiver omdat instellingen tijdens de nulmeting in één vraag gevraagd te reflecteren op het beleid rondom digitale én fysieke beschermingsmaatregelen. Meer instellingen hebben meetbaar en gemanaged beleid, terwijl minder instellingen aangeven geen beleid te hebben omtrent digitale beschermingsmaatregelen.

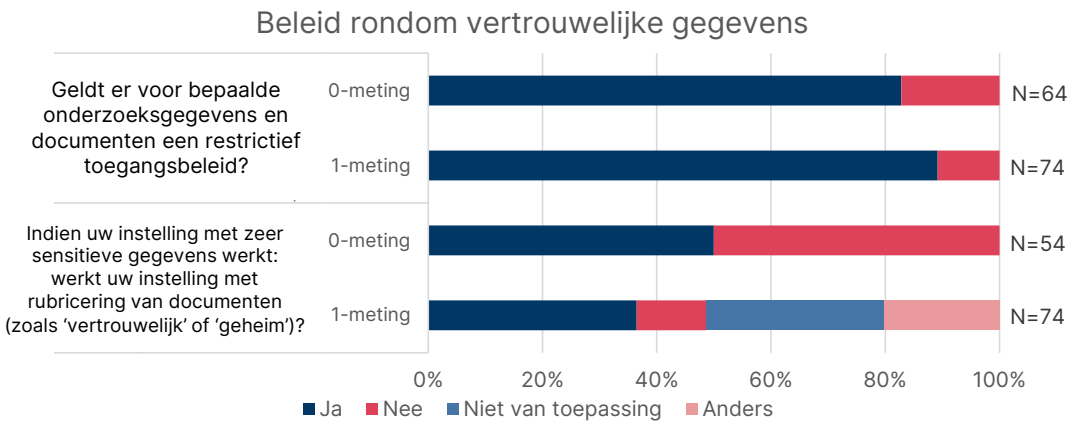
Uit gesprekken met enkele instellingen blijkt dat zij zich sinds de nulmeting bewuster zijn van de kennisveiligheidsrisico's die suboptimale beveiliging van de digitale infrastructuur meedraagt. Waar één instelling aangeeft dat het monitoren van de digitale infrastructuur is aangescherpt (en er een incident response team is opgezet), geeft een andere instelling aan hier nog stappen in te willen zetten. Deze instelling wil bijvoorbeeld systematischer pentesten uitvoeren. Meerdere instellingen geven aan dat zij uitdagingen ervaren in het compartimentaliseren van ICT-voorzieningen, maar

hebben in de vragenlijst niet gespecificeerd om welke dat gaat. In deze vervolgmeting is daar niet verder op ingegaan.

Meer instellingen hebben een restrictief toegangsbeleid op onderzoeksgegevens en documenten geïmplementeerd ten opzichte van de nulmeting (zie Figuur 11). Instellingen die dit sinds de nulmeting hebben geïmplementeerd, deden dat op verschillende manieren: via 1) role-based access, 2) afgeschermde omgevingen per project of 3) enkel voor persoonsgegevens. De instellingen gaan in de self-assessment niet in op de totstandkoming van dit beleid.

Onder hogescholen en universiteiten wisselt het niveau waarop het restrictieve toegangsbeleid wordt uitgevoerd. Waar sommige instellingen dit op projectniveau doen, geldt voor andere instellingen dat toegang op het niveau van lectoraat of zelf faculteit wordt bepaald. Weer andere instellingen hebben enkel bepaalde informatie (zoals ruwe onderzoeksgegevens) afgeschermd. De onderzoeksinstituten hanteren een restrictief toegangsbeleid voor (gevoelige) onderzoeksgegevens en documenten. Zij werken op een *need-to-know* basis en bepalen veelal op projectniveau wie tot welke informatie toegang heeft.

Negen instellingen geven aan dat zij in geen geval restricties plaatsen op de toegang tot (digitale) documenten (zie Figuur 11). Dit zijn veelal (monosectorale) hogescholen die vanwege hun focus weinig tot geen onderzoek doen dat sensitief is, waardoor zij de noodzaak van het afschermen van documenten niet groot achten.



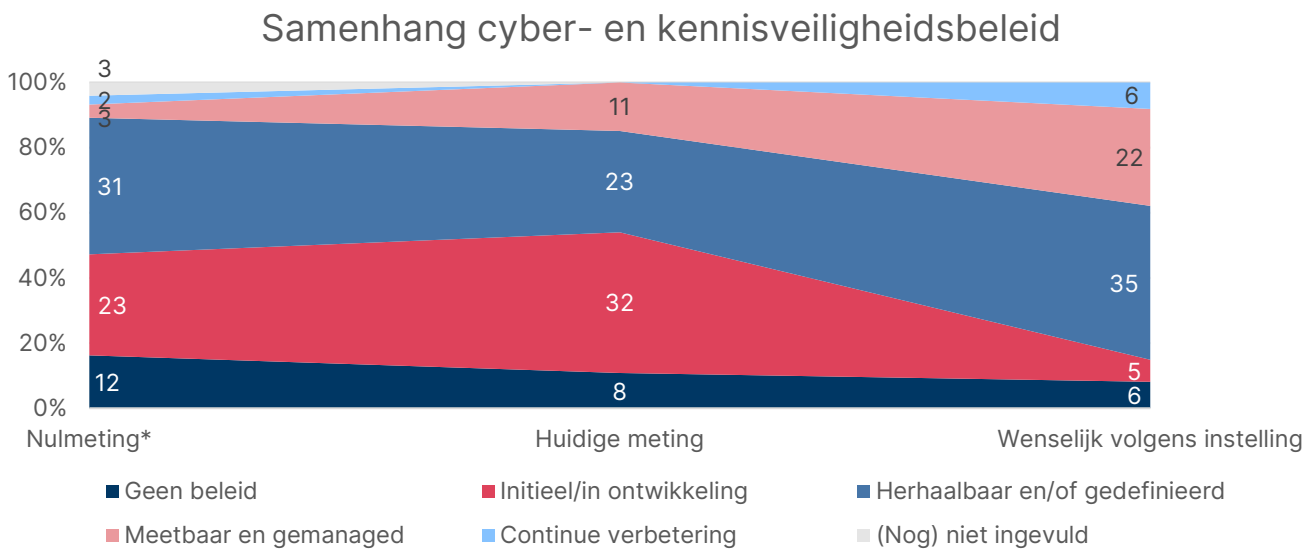
Figuur 11. Beleid van instellingen omtrent vertrouwelijke gegevens

Het aantal instellingen (27 van de 74) dat rubricering plaatst op zeer sensitieve gegevens is gelijk gebleven ten opzichte van de nulmeting. Het aandeel van de instellingen dat rubricering toepast lijkt echter te zijn afgenomen ten opzichte van de nulmeting. Dit is te verklaren door het hogere aantal instellingen dat de vraag heeft beantwoord (54 ten tijde van de nulmeting en 74 ten tijde

van de huidige meting). Daarnaast konden instellingen in de vervolgmeting antwoorden dat rubricering voor hen niet van toepassing is. Deze mogelijkheid was er niet in de nulmeting.

Opvallend is dat negen instellingen geen rubricering toepassen terwijl zij wel te maken hebben met sensitieve gegevens (zoals aangegeven in de self-assessment). Een derde van de instellingen (waaronder bijna exclusief monosectorale hogescholen) geven aan dat rubricering voor hen niet van toepassing is. De self-assessment bood geen mogelijkheid om toe te lichten waarom het voor hen niet van toepassing is. Andere instellingen geven aan dat het beleid hiervoor momenteel in ontwikkeling is, dat rubricering in de praktijk al wordt gedaan, of dat er enkel rubricering van toepassing is op persoonsgegevens maar niet op kennis sensitieve gegevens.

6.3 Samenhang met cyberbeleid



*Figuur 12. Ontwikkeling van instellingen: beleid omtrent digitale beschermingsmaatregelen. *Een directe vergelijking tussen de nulmeting en de huidige meting is niet volledig zuiver omdat instellingen tijdens de nulmeting in één vraag gevraagd te reflecteren op het beleid rondom digitale én fysieke beschermingsmaatregelen*

Instellingen die geen beleid of beleid in ontwikkeling hebben omtrent de kennisveiligheidsrisico's met betrekking tot digitale kwetsbaarheden erkennen de sterke verbondenheid van de thema's. Deze instellingen hebben vaak wel een cybersecurity- en kennisveiligheidsbeleid, maar deze opereren veelal los van elkaar. Instellingen met meer volwassen beleid geven opvallend vaker aan dat er uitwisseling plaatsvindt tussen de verantwoordelijken op de onderwerpen cybersecurity en kennisveiligheid.

De sector voorziet een hoog wenselijkheidsniveau voor de samenhang tussen kennisveiligheids- en cyberveiligheidsbeleid. 28 van de 74 instellingen (38%) hebben het wenselijke niveau van de samenhang tussen het cyberveiligheidsbeleid en het kennisveiligheidsbeleid reeds behaald. Het is echter niet duidelijk welke stappen de instellingen die nog niet tevreden zijn voorzien te zetten om deze hoge mate van volwassenheid te behalen. Elf instellingen (allen hogescholen) geven aan geen beleid of basaal beleid initieel/in ontwikkeling) te ambiëren. Deze instellingen geven aan dat zij geen kennis bezitten die kennisveiligheidsrisico's met zich meebrengt. Zij hebben wel cyberveiligheidsbeleid en ambiëren dít door te ontwikkelen, maar deze doorontwikkeling is niet toegespitst op meer samenhang met kennisveiligheidsbeleid.

6.4 Reisdelegaties

Het grootste deel van de instellingen heeft beleid omtrent bezoeken van buitenlandse reisdelegaties. Vaak is dit opgenomen in het algemene bezoekersprotocol. Instellingen geven aan dat alle bezoekers ten alle tijden onder begeleiding staan van een werknemer van de instelling. Voor bezoekers uit risicolanden worden in enkele gevallen aanvullende maatregelen genomen. Dit wordt vooraf bepaald in een risicoanalyse waar wordt gekeken naar het nut en de noodzaak van het bezoek. Aan de hand van deze analyse dient in sommige gevallen expliciet toestemming te worden gevraagd aan het bestuur. Eén instelling geeft aan dat in sommige gevallen laptops en telefoons ingeleverd dienen te worden. Een bredere groep instellingen noemt expliciet dat het niet is toegestaan om foto's te maken in de restrictieve ruimtes.

Uit de gesprekken blijkt dat veel instellingen tevens beleid hebben ontwikkeld voor werkbezoeken en dienstreizen van eigen personeel naar het buitenland. Zo worden medewerkers standaard geadviseerd om lege ('schone') laptops en telefoons mee te nemen op werkgerelateerde reizen, en mogen zij werkapparatuur niet meenemen op privéreizen naar risicolanden. Een enkele instelling geeft aan bij dienstreizen het advies van het ministerie van Buitenlandse Zaken op te volgen. Daarnaast voeren instellingen bewustwordingscampagnes om werknemers waakzaam te houden tijdens langdurige samenwerkingen. Hierin wordt aandacht besteed aan de rol van cadeaus in een samenwerking en wordt het belang van het meenemen van schone apparatuur naar hoog-risicolanden nogmaals benadrukt.

Ongeveer een kwart van de instellingen geeft aan dat zij geen beleid hebben rondom bezoeken van buitenlandse reisdelegaties. Hiervoor worden twee redenen genoemd: 1) de instellingen hebben geen ruimtes met restrictief toegangsbeleid, of 2) de instellingen krijgen zelden bezoek van buitenlandse reisdelegaties.

Enkele instellingen geven aan dat het nog niet altijd duidelijk is wanneer er buitenlandse delegaties op de campus zijn of dat er geen meldingsplicht is. Het feit dat deze instellingen hierop reflecteren geeft echter aan dat zij bewust zijn van de risico's die dit oplevert.

7 Internationale partnerschappen

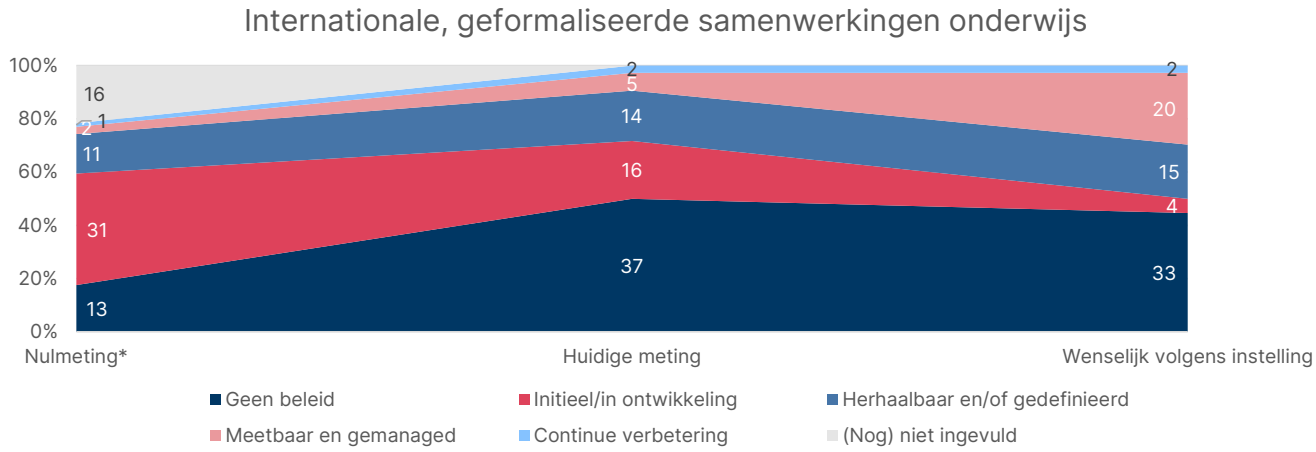
Samenvatting

- Stand 2026: De huidige stand van zaken ligt grotendeels in lijn met de Leidraad. We zien een beperkt aantal instellingen met procedures of beleid rondom het periodiek evalueren van lopende samenwerkingen, dit wordt wel aanbevolen door de Leidraad.
- Stappen ten opzichte van de nulmeting: Veel instellingen hebben stappen gezet in het ontwikkelen van hun kennisveiligheidsbeleid op internationale partnerschappen. Op sommige onderdelen heeft een groep instellingen geconcludeerd dat apart beleid niet relevant is waardoor de groep zonder beleid op een paar onderwerpen is gegroeid.
- Vinden instellingen zichzelf ver genoeg gegeven hun risicoprofiel? Een deel van de instellingen (voornamelijk hogescholen) benadrukt meermaals dat ze via eigen risicoanalyses hebben vastgesteld zelf een laag risicoprofiel te hebben, niet of incidenteel samen te werken met het buitenland of voornamelijk samen te werken met Europese buurlanden. De overige instellingen zijn bezig met (verdere) ontwikkeling van hun internationale partnerschappen beleid in lijn met aanbevelingen van de Leidraad.
- Keuzes en dilemma's: meerdere instellingen geven aan dat ze beperkte *due diligence* kunnen toepassen door het kleine aantal hulpmiddelen dat ter ondersteuning beschikbaar is. Instellingen noemden ook meermaals dat ze zien dat andere landen losser of juist strenger kennisveiligheidsbeleid hanteren, wat internationale samenwerking waarbij je voldoet aan ieders beleid moeilijk maakt.

7.1.1 Het kennisveiligheidsbeleid ten aanzien van internationale samenwerking op onderwijs en onderzoek

De Leidraad Kennisveiligheid besteedt apart aandacht aan het risicomanagement van internationale partnerschappen. In de Leidraad wordt opgemerkt dat duidelijke afspraken vooraf, binnen een internationaal partnerschap, mogelijke kennisveiligheidsrisico's kunnen mitigeren. In deze meting hebben we instellingen gevraagd naar de huidige en wenselijke status van hun

kennisveiligheidsbeleid rondom het aangaan van geformaliseerde internationale partnerschappen, uitgesplitst in onderwijs en onderzoek.

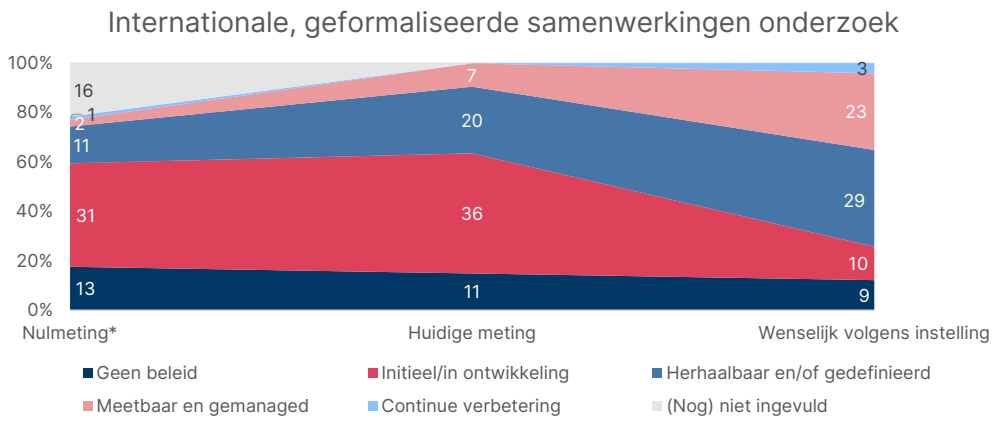


Figuur 13. Ontwikkeling van instellingen: beleid omtrent internationale samenwerkingen (onderwijs)

In de huidige meting zien we een grote groep instellingen zonder kennisveiligheidsbeleid op internationale, geformaliseerde samenwerkingen op onderwijs (zie Figuur 10). Dit lijkt een toename ten opzichte van de nulmeting, maar dit komt door een verschil in vraagstelling: in de nulmeting werden onderwijs en onderzoek niet apart uitgevraagd, nu wel. In de nulmeting gaf het grootste deel van de instellingen aan initieel/in ontwikkeling beleid te hebben, al had een deel van de instellingen ook geen antwoord gegeven op deze vraag.

Als we naar de toekomst kijken, zien we dat een grote groep instellingen het ook wenselijk vind geen beleid te hebben. Dit zijn deels de kennisinstellingen die geen onderwijsopdracht hebben en hier dus ook geen beleid op hoeven te maken. Een ander deel van deze groep – bestaande uit hogescholen - geeft aan geen internationale geformaliseerde onderwijssamenwerkingen te hebben en vindt het daarom ook niet nodig om beleid hierop te ontwikkelen.

Aan de bovenkant van het figuur zien we wel een kleine groei in instellingen die herhaalbaar, meetbaar of continue verbeterd beleid hebben. Als we kijken naar het wenselijke niveau is daar een splitsing tussen instellingen die geen beleid willen en instellingen die gedefinieerd/meetbaar beleid wenselijk achten.



Figuur 14. Ontwikkeling van instellingen: beleid omtrent internationale samenwerkingen (onderzoek)

Als we kijken naar samenwerkingen op onderzoek zien we een ander beeld (zie figuur 14). In de huidige meting geeft de helft van de instellingen aan dat hun kennisveiligheidsbeleid op internationale, geformaliseerde samenwerking op onderzoek in de initiële/in ontwikkeling fase zit. De verdeling van instellingen over de verschillende niveaus is redelijk hetzelfde gebleven ten opzichte van de nulmeting. De voornaamste verandering is dat we van de 16 instellingen die in de nulmeting de rubric niet hadden ingevuld nu wel informatie hebben.

Kijkend naar het aangegeven wenselijke niveau van kennisveiligheidsbeleid zien we dat de meeste instellingen wensen hun beleid verder te ontwikkelen richting 'herhaalbaar/gedefinieerd' of 'meetbaar en gemanaged'. Een deel van de instellingen, wederom voornamelijk instellingen met een laag risicoprofiel, geeft aan dat beleid hierop niet passend is. De meesten lichten toe dat ze geen internationale samenwerkingen aangaan op het gebied van onderzoek of dat het niet relevant is gezien het soort onderzoek dat de instelling verricht en/of door de beperkte omvang van de instelling.

7.1.2 Interne procedures rondom het aangaan van internationale partnerschappen

Due diligence

De Leidraad geeft aan dat het belangrijk is om *due digilence* toe te passen in het nagaan van de achtergrond van de potentiële samenwerkingspartner. Dit is nadrukkelijk van belang voor samenwerkingen met hoog risicolanden of onderzoek rondom sensitieve kennisgebieden.

Het overgrote deel van de instellingen geeft aan dat er interne procedures aanwezig zijn rondom *due diligence* in het nagaan van de achtergrond van een buitenlandse partner of opdrachtgever. Een deel van de instellingen heeft dit verwerkt binnen algemeen beleid rondom samenwerkingen. Een ander deel van de instellingen geeft aan dit alleen ad hoc toe te passen als er sprake is van

een mogelijke samenwerking met risicolanden. Wie zien dat vooral een aantal hogescholen aangeven dat ze geen beleid hebben of dat het niet relevant is voor hun instelling, bijvoorbeeld doordat hun partners zich allemaal binnen de Europese Unie bevinden. Dit is ook genoemd in gesprekken binnen de casestudy als onderbouwing voor weinig of geen beleid.

In zowel de self-assessments als de cases werd naar voren gebracht dat er beperkte mogelijkheden zijn om *due diligence* op achtergrond van partners te doen doordat er relatief weinig hulpmiddelen beschikbaar zijn om dit uit te voeren. Er zijn bronnen, maar deze kosten instellingen meestal geld. Sommige instellingen maken hier wel gebruik van. Desalniettemin kwam meermaals de wens naar voren voor een lijst of informatiedocument dat Europees afgestemd is dat informatie geeft over buitenlandse samenwerkingspartners (met een hoog risico), o.a. ter vervanging van de Australische ASPI-tracker.

In de cases kwam ook meermaals naar voren dat er verschillen zijn ontstaan of kunnen ontstaan in de mate van *due diligence* en de mate van striktheid van het kennisveiligheidsbeleid tussen verschillende samenwerkingspartners. Dit kan leiden tot een situatie waarin je niet kan voldoen aan elkaars beleid en voorschriften, waardoor een samenwerking niet mogelijk is. In de gesprekken werd het belang benadrukt van een Europees gedragen kennisveiligheidsbeleid (gelijk speelveld) om dit soort situaties te voorkomen. Ook zou dit moeten voorkomen dat Nederlandse kennisinstellingen niet kunnen meedoen aan internationale consortia en voorkomen dat onderzoekers hun onderzoek vanuit een buurland gaan uitvoeren om onder (strengere) Nederlandse regels uit te komen.

Of bij *due diligence* juridische en veiligheidsexpertise wordt ingeschakeld verschilt per instelling. Een deel van de instellingen geeft aan altijd juridische expertise in te schakelen rondom nieuwe samenwerkingen. Een deel geeft aan juridische en veiligheidsexpertise in te schakelen indien er een risico wordt gezien na het doorlopen van kennisveiligheidsprocedures. Dit is in lijn met de Leidraad, waarin instellingen worden aangeraden om juridische en veiligheidsexpertise in te schakelen voornamelijk als het gaat om samenwerkingen met betrekking op sensitieve kennisgebieden met een partner met een verhoogd risicoprofiel. In een van de cases wordt bijvoorbeeld een schema benoemd dat een onderzoeker kan doorlopen waarop verschillende acties volgen. Als kennisveiligheidsrisico's worden gesignaleerd, geven veel instellingen aan ook het eigen adviesteam kennisveiligheid in te schakelen.

Aangaan partnerschappen

Voordat een instelling een definitieve samenwerking aangaat met een buitenlandse partner geven de meeste instellingen aan dat de aanwezige kennisveiligheidsprocedures worden doorgelopen en een afweging wordt gemaakt tussen de verschillende belangen rondom de samenwerking en of de

samenwerking past binnen het karakter en de strategie van de instelling. Als deze afwegingskaders zijn doorlopen wordt de samenwerking definitief aangegaan.

Een aantal instellingen (15) geeft aan geen partneracceptatie beleid te hebben omdat ze geen internationale samenwerkingen aangaan, dit slechts incidenteel doen en/of vanuit een eerdere risicoassessment hebben geconcludeerd een laag risicoprofiel te hebben. De combinatie van een laag risicoprofiel en het weinig tot incidenteel voorkomen van buitenlandse samenwerkingen is voor deze instellingen reden om geen standaard beleid hiervoor te ontwikkelen.

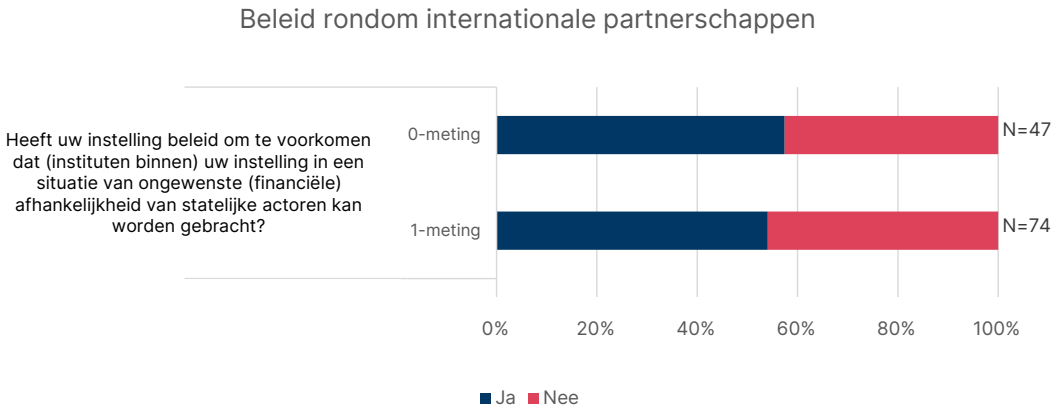
Beleggen van verantwoordelijkheid

De verantwoordelijkheid rondom het aangaan van internationale partnerschappen ligt voornamelijk op bestuurlijk niveau, bij het CvB of bij het hoofd van de faculteit of het domein. Het verantwoordelijke bestuurlijk niveau kan verschillen afhankelijk van het type en de grootte van het potentiële partnerschap, maar ook aan de grootte van de instelling zelf. Kleinere instellingen geven vaker aan de verantwoordelijkheid bij het CvB te leggen, grotere instellingen leggen deze verantwoordelijk vaak bij een lager bestuurlijk niveau afhankelijk van het type en grootte partnerschap.

Voor bijna de helft van de instellingen verschilt dit niet tussen partnerschappen rondom onderwijs of onderzoek (32 instellingen). Voor een deel van de instellingen (11 instellingen) is er een verschil in verantwoordelijkheid, waarbij (kleine) samenwerkingen op onderzoek vaker op lager bestuurlijk niveau worden goedgekeurd dan onderwijs samenwerkingen. Een aantal instellingen geeft aan dat men in samenwerkingen op onderzoek vaak meer bewustzijn lijkt te kennen rondom kennisveiligheidsrisico's dan op het onderwijsvlak.

7.1.3 Beleid rondom ongewenste (financiële) afhankelijkheid van statelijke actoren

De Leidraad benadrukt het belang van het stellen van een aantal vragen voorafgaand aan het aangaan van een overeenkomst, zoals waar de fondsen vandaan komen en of de financier economische of politieke belangen heeft bij een bepaalde uitkomst van het onderzoek. Het is belangrijk dat instellingen alert zijn om ongewenste (financiële) afhankelijkheid van statelijke actoren te voorkomen.



Figuur 15. Het beleid van instellingen rondom internationale partnerschappen op het vlak van ongewenste afhankelijkheid

Iets meer dan de helft (54%) van de instellingen geeft aan beleid te hebben rondom het voorkomen van (financiële) afhankelijkheid van statelijke actoren (zie Figuur 11). Deze verhouding is niet wezenlijk veranderd tegen opzichte van de nulmeting. Daarbij merken we wel op dat een deel van de instellingen in de nulmeting geen antwoord gegeven heeft op deze vraag.

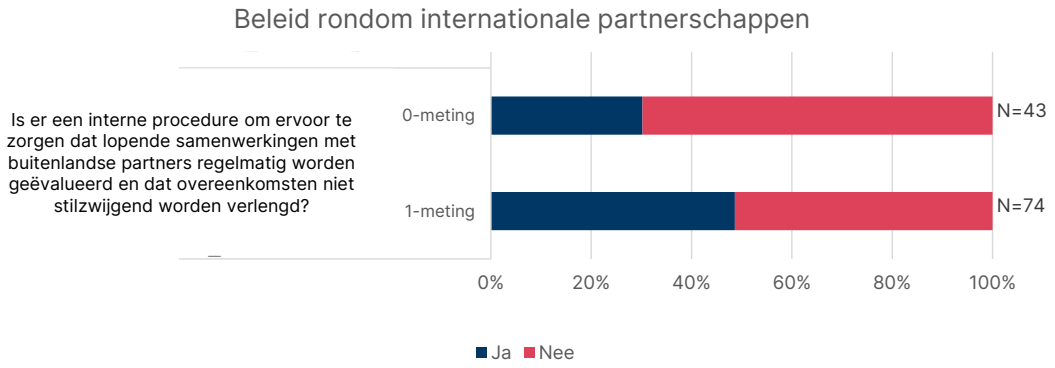
Als we in meer detail kijken naar de instellingen die geen beleid voeren, zien we dat de voornaamste reden hiervoor een laag risicoprofiel is. Deze groep bestaat vooral uit hogescholen, maar omvat ook enkele universiteiten. Deze groep instellingen geeft aan dat het niet relevant is voor hun instelling omdat ze incidenteel of niet samenwerken met buitenlandse partners. Omdat een buitenlandse samenwerking weinig voorkomt, verloopt dit proces via het CvB dat goed overzicht kan houden omdat het gaat om een klein aantal samenwerkingen. Ongewenste afhankelijkheid is verwerkt in algemeen kennisveiligheidsbeleid met verschillende niveaus van detail, maar heeft geen apart beleidsproces gekregen.

Deze uitkomst is redelijk in lijn met de wensen van de Leidraad. De Leidraad vraagt voornamelijk om bewustzijn rondom dit onderwerp en het besef dat ongewenste (financiële) afhankelijkheid ook stap voor stap kan ontstaan. De instellingen zonder beleid geven aan dat door de incidentele aard van buitenlandse samenwerkingen het eigen CvB genoeg overzicht houdt om potentiële ongewenste afhankelijkheid te signaleren.

7.1.4 Evaluatie procedures voor lopende internationale samenwerkingen

Het kennisveiligheidsbeleid rondom internationale partnerschappen is voornamelijk gebaseerd op het voorkomen van risico's aan de poort, voordat een partnerschap wordt aangegaan. Om vroegtijdig signalen op te vangen en knelpunten te kunnen adresseren wordt in de Leidraad aanbevolen om ook periodieke evaluatie van de samenwerking in te bouwen. Daarnaast wordt gesteld dat het

onverstandig is om samenwerkingen, voornamelijk samenwerkingen met een verhoogd risico door de partner of het kennisdomein, stilzwijgend te verlengen. Het advies is om de eigen organisatie zo in te richten dat er ook bij verlengingen genoeg tijd is om samenwerkingen opnieuw te analyseren op (nieuwe) risico's.



Figuur 16. Het beleid van instellingen rondom het evalueren van lopende partnerschappen en het voorkomen van stilzwijgend verlengen van overeenkomsten

Kijkend naar de aanwezigheid van interne procedures rondom het evalueren van lopende samenwerkingen met buitenlandse partners en of deze samenwerkingen niet stilzwijgend worden verlengd, zien we een duidelijke verandering ten opzichte van de nulmeting. Ten tijde van de nulmeting gaf 30 procent van de instellingen aan procedures te hebben, in de huidige meting is dit gestegen naar bijna de helft van de instellingen (49 procent).

Een groot deel van de instellingen geeft aan dat er geen stilzwijgende verlenging plaatsvindt, bijvoorbeeld doordat samenwerkingen projectgebonden zijn en daarom een einddatum kennen. Een ander deel heeft vanuit deze redenering nee geantwoord op de vraag. Een groot deel van de instellingen geeft aan dat er beleid is om bij een verlenging opnieuw een kennisveiligheidscheck te doen, voordat deze wordt goedgekeurd. Een aantal instellingen zijn dit beleid nog aan het ontwikkelen binnen een breder systeem rondom het managen van samenwerkingen. Een aantal instellingen geven aan dat beleid rondom het evalueren van lopende samenwerkingen nog niet is opgezet of in ontwikkeling is.

Als we in meer detail kijken zien we dat het merendeel van de groep die hier geen beleid opvoert aangeeft aan dat buitenlandse samenwerkingen te incidenteel zijn om hier aparte procedures voor op te zetten. Een kleiner aantal instellingen geeft aan dat dit nog in ontwikkeling is. Twee instellingen geven aan dat het niet bekend is of deze procedures aanwezig zijn.

In de cases kwam naar voren dat het evalueren van lopende samenwerkingen ook lastig kan zijn doordat bepaalde relaties al een lange periode bestaan en mensen ook persoonlijke relaties

hebben opgebouwd, het toetsen van kennisveiligheid kan resulteren in het termineren van een samenwerkingsrelatie wat voor individuele onderzoekers pijnlijk kan zijn voor hun onderzoek en in persoonlijke sfeer.

8 Personeelsbeleid

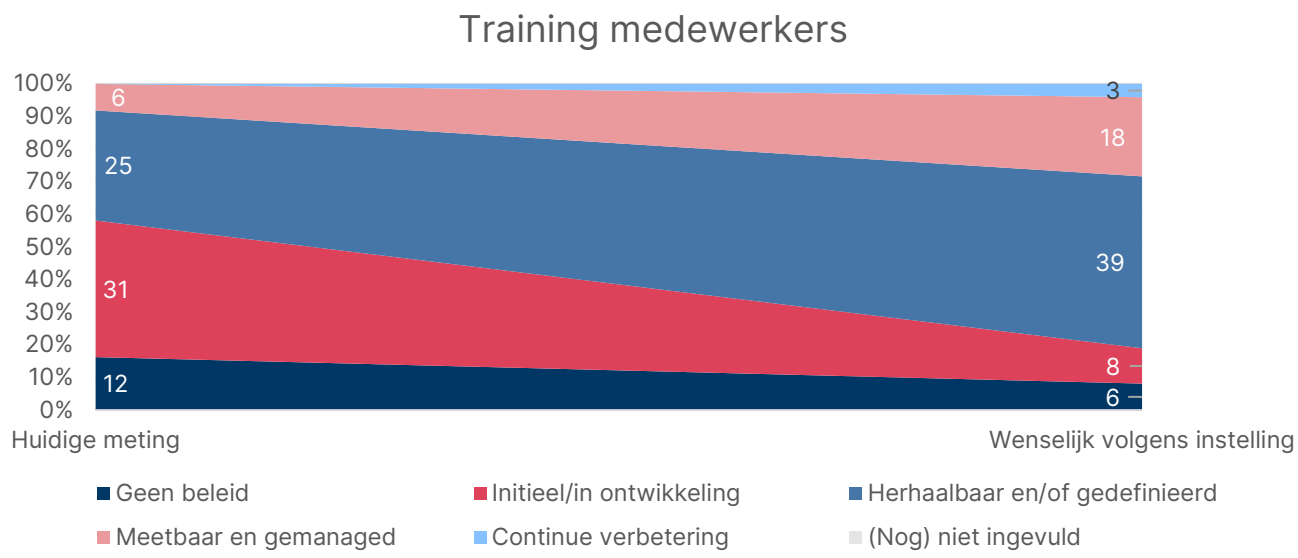
Samenvatting

- Stand 2026: De meerderheid van de instellingen geeft aan dat HR-personeel op de hoogte is van kennisveiligheidsrisico's, toegang heeft tot bronnen om risico's te herkennen en zo nodig samenwerkt met het adviesteam kennisveiligheid om risico's te mitigeren. Meer dan 70% van de instellingen geeft aan (nieuwe) medewerkers informatie en training te geven om hen meer veiligheidsbewust te maken. De nadruk ligt hierbij wel sterker bij (online) informatievoorziening dan bij het verzorgen van trainingen. Bijna alle instellingen hebben beleid voor buitenlandse dienstreizen en meer dan een derde van de instellingen heeft hiervoor een protocol.
- Stappen ten opzichte van de nulmeting: In vergelijking met de nulmeting is het personeelsbeleid m.b.t. kennisveiligheid verder ontwikkeld tijdens de huidige meting. Er worden o.a. meer activiteiten voor personeel georganiseerd in de vorm van bewustwording en training m.b.t. kennisveiligheid.
- Vinden instellingen zichzelf ver genoeg gegeven hun risicoprofiel? Instellingen hebben hun ambitieniveau wat betreft training van personeel nog niet behaald. Wat betreft kennisveiligheidsbeleid ten aanzien van werving van nieuwe medewerkers, is het verschil tussen het behaalde niveau en het wenselijke niveau relatief klein. Instellingen geven aan in afwachting te zijn van de wet screening kennisveiligheid.
- Keuzes en dilemma's. In zowel de self-assessment en casestudy komt terug dat bewustwording een belangrijk onderdeel is van de training van personeel. Dit draagt er eveneens aan bij dat het kennisveiligheidsbeleid sneller wordt aanvaard. Ongeveer een derde van de instellingen heeft aandacht voor aantasting van sociale veiligheid die voortvloeit uit (heimelijke) beïnvloeding door statelijke actoren. Dit is meestal belegd bij vertrouwenspersonen, al hebben drie instellingen hiervoor een eigen loket/meldpunt. Als dilemma's komt o.a. naar voren dat screening van personeel op kennisveiligheid risico's op discriminatie en stigmatisering kan geven. Als laatste worden er zorgen geuit over de wet screening kennisveiligheid. Hierbij wordt o.a. de doorlooptijd van screening als risico gezien.

In dit hoofdstuk bespreken we het personeelsbeleid m.b.t kennisveiligheid op drie verschillende thema's: de training van medewerkers, de werving van medewerkers en buitenlandse dienstreizen. De rubrics over personeelsbeleid waren in de huidige meting uitgesplitst in de bovenstaande drie thema's aan bod gekomen, terwijl er in de nulmeting enkel een algemene rubric over personeelsbeleid in relatie tot kennisveiligheid is gesteld. Daarom kan de nulmeting op dit onderwerp niet één op één worden vergeleken met de huidige meting.

8.1.1 Training van medewerkers

De meeste instellingen hebben een initieel (42%) of herhaalbaar (34%) beleid voor training van medewerkers op gebied van kennisveiligheid. Meer dan de helft van de instellingen vindt een herhaalbaar en/of gedefinieerd beleid voor de training van nieuwe medewerkers wenselijk. Instellingen hebben hun ambitieniveau nog niet bereikt. De onderstaande figuur illustreert dit: hierin is te zien hoe instellingen het kennisveiligheidsbeleid ten aanzien van training van nieuwe medewerkers beoordelen.



Figuur 17: Ontwikkeling van instellingen: beleid omtrent training van medewerkers

Van de 12 instellingen die geen beleid hebben voor de training van medewerkers m.b.t. kennisveiligheid, vinden 6 instellingen dat niveau ook wenselijk. Ongeveer een kwart van de totale hoeveelheid instellingen vindt een meetbaar en gemanaged niveau wenselijk.

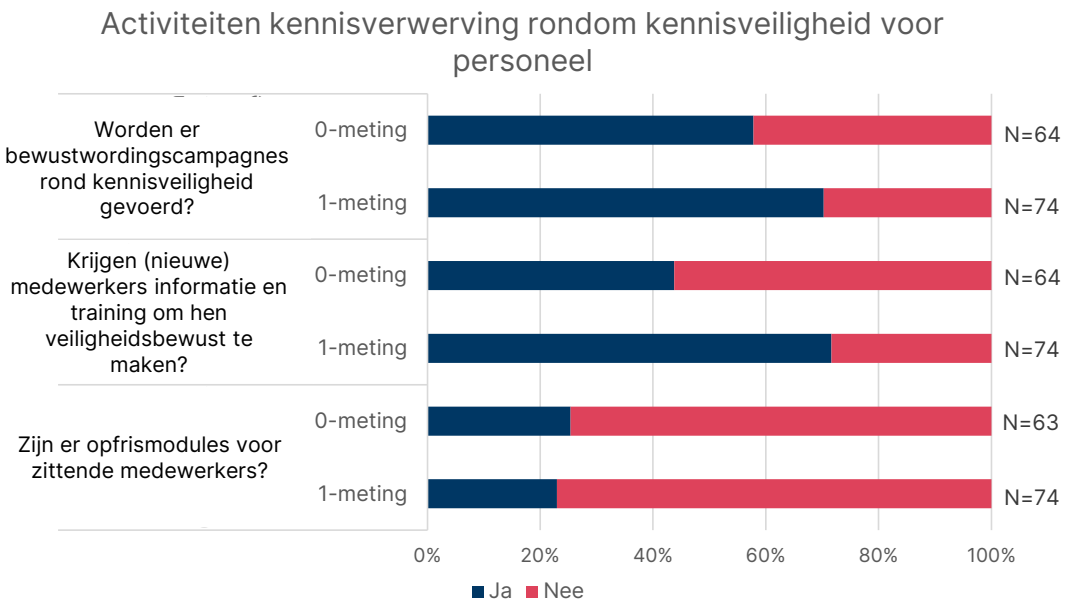
Tijdens de nulmeting had ongeveer een derde van de instellingen geen personeelsbeleid m.b.t. kennisveiligheid, en bij nog eens een derde van de instellingen was het beleid initieel of in ontwikkeling. Uit de huidige meting blijkt dat er voortuitgang is ten opzichte van de nulmeting. Ook al kunnen de vragen niet één op één vergeleken worden, is het wat ons betreft wel zichtbaar dat er tijdens de huidige meting meer instellingen beleid hebben voor de training van medewerkers op gebied van kennisveiligheid.

Ongeveer een vijfde van de kennisinstellingen geeft als toelichting aan trainingen over kennisveiligheid of gerelateerde thema's (zij noemen hier bijvoorbeeld sociale veiligheid of cyberveiligheid) te verzorgen. Deze trainingen zijn veelal op ad hoc basis georganiseerd, en vaak gericht op de personen waarvoor ze het meest van toepassing zijn. Enkele kennisinstellingen geven periodiek presentaties, sessies of verplichte trainingen. Daarnaast geven ook enkele kennisinstellingen aan dat er gewerkt wordt om trainingen meer systematisch in het beleid te integreren, bijvoorbeeld door kennisveiligheidschecks in reguliere onderzoeksprocessen in te bouwen.

Niet alle kennisinstellingen hebben beleid op kennisveiligheidstrainingen voor medewerkers. Dit hangt samen met het risicoprofiel van instellingen. Sommige instellingen hebben alleen trainingen voor relevant personeel.

Verder geven veel instellingen aan dat er gewerkt wordt aan het creëren van bewustwording en kennisopbouw over kennisveiligheid. Dat wordt bijvoorbeeld gedaan door online informatie voor medewerkers beschikbaar te stellen, bijvoorbeeld via intranet of een website. Deze informatie bestaat onder andere uit algemene voorlichting, *e-learnings* en factsheets. In bijna alle cases komt ter sprake dat bewustwording een essentieel onderdeel is van het personeelsbeleid rondom kennisveiligheid. Zo wordt er uitgelegd dat het helpt om risicovolle cases (anoniem) te benoemen bij personeel, deskundigen te vragen om uitleg te geven en kennisveiligheidsrisico's vanuit verschillende perspectieven (zoals IT, HR, onderzoekers, etc.) onder de aandacht te brengen. Daarnaast wordt er ook benoemd dat men zorgvuldig om moet gaan met het ontwerp van algemene bewustwordingscampagnes, omdat het ook stigmatisering in de hand kan werken.

In de onderstaande figuur is van enkele activiteiten m.b.t. kennisveiligheid aangegeven of instellingen deze activiteiten uitvoeren.



Figuur 18. De activiteiten door instellingen over kenniswerving rondom kennisveiligheid voor personeel

Inmiddels voert 70% van de instellingen bewustwordingscampagnes rond kennisveiligheid uit, dit is een hoger percentage dan tijdens de nulmeting. We zien zowel brede activiteiten met als doelgroep alle medewerkers of al het wetenschappelijk- en ondersteunend personeel, als gerichte inzet voor specifiek personeel, zoals leidinggevenden, juridische medewerkers of onderzoekers die werken in risicodomeinen. Een deel van de instellingen zet beide vormen bewust naast elkaar in.

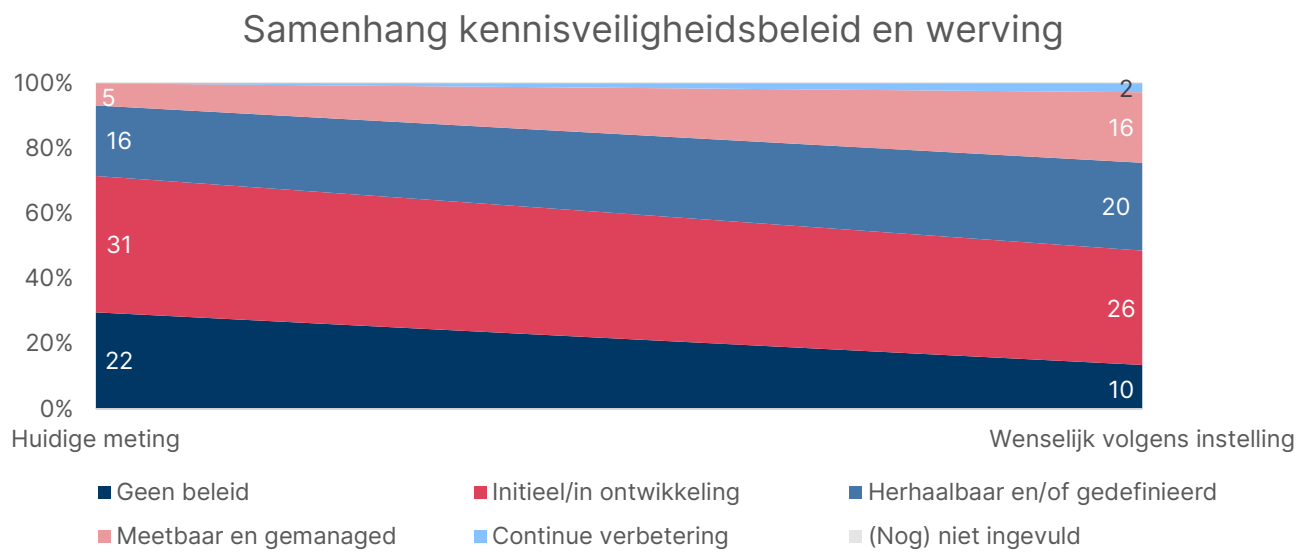
Ruim 70% van de instellingen geeft aan dat (nieuwe) medewerkers informatie en training krijgen om hen veiligheidsbewust te maken. Hierbij ligt de nadruk sterker bij informatievoorziening dan bij het geven van trainingen. Er wordt vaak aangegeven dat veiligheidsbewustheid onderdeel is van de *onboarding* van nieuwe medewerkers, bijvoorbeeld door middel van (verplichte) online modules, presentaties of een startcursus. Een deel van de instellingen geeft aan dat kennisveiligheid voor hen niet relevant is, maar dat er wel voorlichting is op gebied van algemene veiligheid, informatieveiligheid en/of cyberveiligheid.

Instellingen die geen bewustwordingscampagnes of training voor medewerkers te hebben, geven hiervoor verschillende redenen. Een deel van de instellingen vindt het vanwege hun risicoprofiel niet relevant. Een ander deel van de instellingen geeft aan dat campagnes of trainingen in ontwikkeling zijn. En een laatste deel van de instellingen heeft geen brede campagne of trainingen, maar geeft aandacht aan kennisveiligheid bij relevante interne overleggen.

Als laatste zijn opfrismodules voor zittende medewerkers beperkt aanwezig: ongeveer 20% van de instellingen verzorgt opfrismodules. Instellingen geven regelmatig aan dat er geen modules specifiek gericht op kennisveiligheid zijn, maar wel voor algemene veiligheid of cyberveiligheid. De meeste instellingen geven eerder projectmatig, op ad hoc basis of voor alleen relevante medewerkers (al dan niet verplichte) training over kennisveiligheid.

8.1.2 Samenhang kennisveiligheidsbeleid en werving medewerkers

Wat betreft samenhang tussen kennisveiligheidsbeleid en werving, is het verschil tussen het behaalde niveau en het wenselijke niveau relatief klein. Binnen het niveau 'geen beleid' kunnen nog stappen gezet worden: 22 instellingen hebben geen kennisveiligheidsbeleid ten aanzien van nieuwe medewerkers, terwijl er maar 10 instellingen het ook wenselijk achten dat hier geen beleid voor is. Bij universiteiten ligt het wenselijke niveau gemiddeld een niveau hoger dan bij hogescholen. De meeste instellingen geven op dit thema aan in afwachting te zijn van de wet screening kennisveiligheid, in hoofdstuk 9.1.3 gaan we hier in meer detail op in.



Figuur 19. Ontwikkeling van instellingen: beleid omtrent werving van nieuw personeel

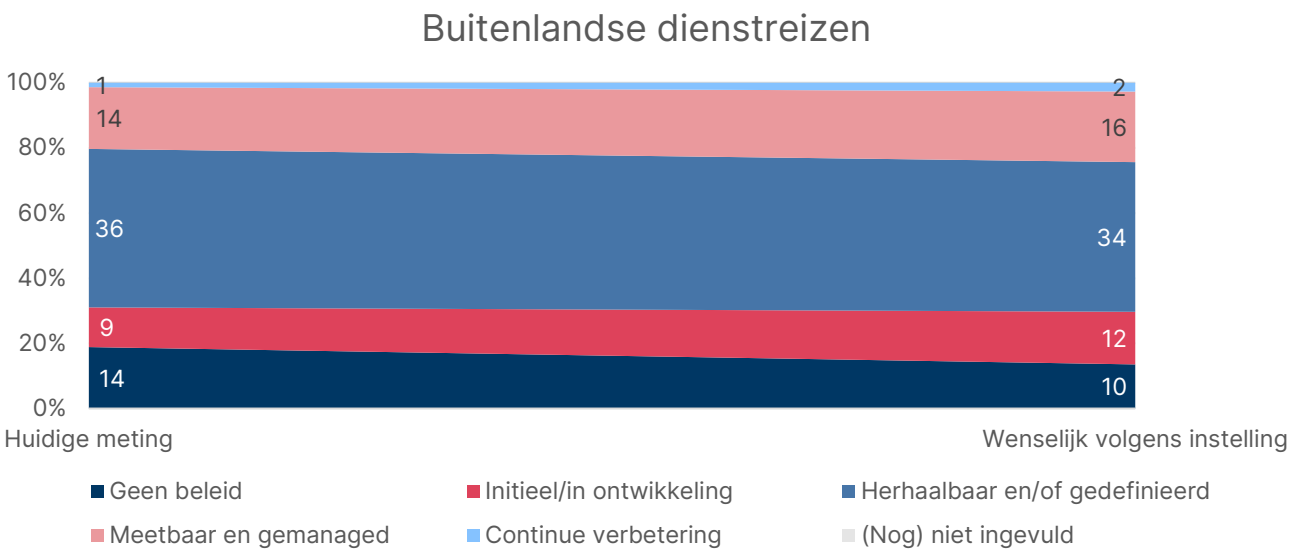
De meerderheid van de instellingen geeft aan dat HR-personeel op de hoogte is van kennisveiligheidsrisico's, toegang heeft tot bronnen om risico's te herkennen en zo nodig samenwerkt met het adviesteam kennisveiligheid. Ook geven sommige instellingen aan dat er (extra) trainingen rond veiligheidsbewustzijn beschikbaar zijn voor HR-personeel. Sommige instellingen hebben vanwege hun risicoprofiel geen actief beleid voor veiligheidsbewustzijn van HR-medewerkers.

De meeste universiteiten geven aan dat ze eraan werken om kennisveiligheid formeel onderdeel te maken van het wervingsproces en/of de selectieprocedure. Enkele universiteiten benoemen expliciet een afwegingskader kennisveiligheid: dat is een document wat helpt bij het signaleren van mogelijke risico's bij personen (of organisaties). Ook wordt er in een case benoemd dat screening op kennisveiligheidsaspecten al onderdeel is van vacatureteksten. Hogescholen refereren meestal naar de VOG. Zij geven aan dat op basis van de rol of functie binnen de organisatie een risicoschatting gemaakt wordt. Bij functies die betrokken zijn bij onderzoek met internationale samenwerking, kan er bijvoorbeeld extra screening plaatsvinden.

Als laatste worden in de cases twee dilemma's rondom werving benoemd. De meeste instellingen benoemen het risico op discriminatie en stigmatisering bij screening van nieuwe en zittende medewerkers. Instellingen geven aan dat strenge veiligheidschecks op gespannen voet kunnen staan met de kernwaarde van openheid en inclusiviteit die de instellingen hebben. Een tweede dilemma waar instellingen voor staan is dat het maken van een risicoafweging voor zittende medewerkers lastiger is dan voor nieuwe medewerkers. Om dit te illustreren: (potentiële) nieuwe medewerkers kunnen worden voorbereid dat een screening in het wervings- en selectieproces plaatsvindt. Als voor zittende medewerkers regels veranderen, kunnen daar niet zomaar arbeidsvoorwaarden worden veranderd. Ook signaleren instellingen dat een case-by-case afweging op de werkvloer soms als een generieke richtlijn wordt ervaren. Concreet: als een adviesteam adviseert een individuele kandidaat uit een risicoland niet aan te nemen interpreteert de werkvloer dit soms als een grondslag om uit dat risicoland helemaal geen kandidaten meer aan te nemen, terwijl dit niet de bedoeling van het adviesteam is.

8.1.3 Buitenlandse dienstreizen

Het onderstaande figuur geeft weer wat instellingen rapporteren over hun kennisveiligheidsbeleid m.b.t. buitenlandse dienstreizen. In het figuur is te zien dat instellingen op gebied van buitenlandse dienstreizen met het behaalde niveau dicht aan liggen tegen het wenselijke niveau.

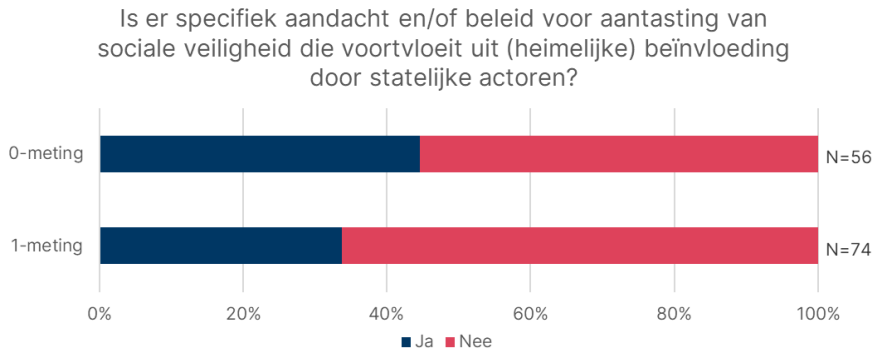


Figuur 20. Ontwikkeling van instellingen: beleid omtrent buitenlandse dienstreizen

Bijna alle instellingen geven aan beleid te hebben voor buitenlandse dienstreizen. Meer dan een derde van de instellingen geeft ook expliciet aan hiervoor een protocol te hebben. Soms is kennisveiligheid een specifiek onderdeel van het beleid omtrent buitenlandse dienstreizen, in andere gevallen is het beleid niet specifiek op kennisveiligheid gericht, maar wel op digitaal veilig werken en informatieveiligheid. Uit de casestudy blijkt dat ook instellingen met een laag risicoprofiel een protocol voor dienstreizen kunnen hebben.

De meeste instellingen geven aan dat er richtlijnen of protocollen gelden voor reizen naar landen met een verhoogd risicoprofiel, zoals bijvoorbeeld het meenemen van lege laptops/telefoons en/of het blokkeren van een account tijdens de reis. Er wordt vaak verwezen naar het (reis)advies van het ministerie van Buitenlandse Zaken. Voor landen met een oranje of rood reisadvies gelden er speciale regels, zoals overleg met de *International Office.* Bijna altijd worden landen met een rood reisadvies uitgesloten van buitenlandse dienstreizen.

Ongeveer een derde van de instellingen (N=25) geeft aan dat er specifieke aandacht en/of beleid is voor aantasting van sociale veiligheid die voortvloeit uit (heimelijke) beïnvloeding door statelijke actoren. Het aantal instellingen met deze specifiek(e) aandacht/beleid is hetzelfde als tijdens de nulmeting (toen was het aantal ook N=25), alleen lag het percentage van het geheel toen wat hoger (zie onderstaande figuur).



Figuur 21. Beleid van instellingen op aantasting van sociale veiligheid door beïnvloeding van statelijke actoren

De instellingen die in de huidige meting aangaven specifiek aandacht/beleid te hebben, lichten toe dat er o.a. aandacht voor dit thema is onder vertrouwenspersonen en in voorlichting en/of bewustwordingscampagnes. Drie instellingen hebben voor dit thema een speciaal loket of meldpunt. Wel zien we dat ook instellingen die rapporteren geen specifiek beleid of aandacht te hebben voor dit thema, ook benoemen dat beïnvloeding door statelijke actoren wel wordt opgevangen door vertrouwenspersonen, contactpersonen kennisveiligheid of (kennis)veiligheidsregels en gedragscodes.

9 Doorontwikkeling van beleid

Samenvatting

- De meeste instellingen willen hun kennisveiligheidsbeleid nog doorontwikkelen. Enkele kleinere, monosectorale hogescholen vinden zichzelf uitontwikkeld.
- Voornemens tot doorontwikkeling zitten vooral in verdere bewustwording, centrale en betere registratie van internationale samenwerking en het evalueren van bestaand beleid.
- De actualisatie van de Leidraad Kennisveiligheid en de wet screening kennisveiligheid zijn van invloed op de doorontwikkeling van beleid bij instellingen.
- De sector is overwegend positief over de huidige beleidsinzet van de Rijksoverheid. Richting de toekomst spreken instellingen vooral behoefte uit aan handzame tools en bronnen, een duidelijker handelingskader en financiële ondersteuning.

In dit hoofdstuk kijken we vooruit naar de verwachte en gewenste doorontwikkeling van het kennisveiligheidsbeleid op Nederlandse kennisinstellingen. We doen dat in twee stappen. Eerst bespreken we hoe instellingen hun beleid in de komende jaren willen doorontwikkelen en welke landelijke beleidsontwikkelingen hierop invloed hebben. Daarna bespreken we welke ondersteuning vanuit de Rijksoverheid instellingen aangeven nodig te hebben.

9.1 Voornemens instellingen doorontwikkeling van beleid

De meeste instellingen hebben nog voornemens tot doorontwikkeling. Elf instellingen hebben dit niet, dit zijn voornamelijk kleinere, monosectorale hogescholen die afgelopen periode hebben geconcludeerd dat ze geen risico's lopen en daarom bewust geen (verder) beleid nodig hebben. De instellingen die nog wel verder willen ontwikkelen hebben twee typen voornemens: (1) het verder implementeren van beleid en (2) het evalueren van beleid.

9.1.1 Verder implementeren van beleid

Voor verreweg de meeste instellingen liggen hun ambities in het verder implementeren van beleid op een of meer van de terreinen zoals in voorgaande hoofdstukken besproken. Twee beleidsterreinen worden hier relatief vaak genoemd: bewustwording en *real-time* registratie van internationale samenwerking.

Veel instellingen noemen bewustwording als een thema dat blijvende aandacht en doorontwikkeling nodig heeft. Kennisveiligheidsbeleid is veelal vastgesteld en wordt nu geïmplementeerd of gaat dat binnenkort worden. Dat moet leiden tot bewustwording bij medewerkers van risico's en de manier waarop daarmee omgegaan kan worden. Veel instellingen hebben dan ook het voornemen te hebben om trainingen en campagnes uit te gaan voeren of uit te blijven voeren die aan dat bewustzijn moeten bijdragen.

Verder hebben veel instellingen het plan om hun registratie van risicovolle internationale samenwerkingen te professionaliseren. Hoe dit er concreet uitziet levert een divers beeld op: sommige instellingen zijn bezig met het vervolmaken van hun huidige lijst, andere willen extern onderzoek laten uitvoeren om risico's rondom internationale samenwerking in beeld te brengen, terwijl sommige instellingen de ambitie hebben om een volledig (contract)managementsysteem te ontwikkelen waarmee *real-time* overzicht is bij te houden van risicovolle internationale samenwerkingen. Een paar instellingen zijn voornemens om tools te gaan inkopen of ontwikkelen die het maken van een risicoanalyse bij internationale samenwerkingen makkelijker moeten maken.

Ook op andere thema's zoals reisbeleid, gastonderzoekers en fysieke toegang hebben instellingen ambities, maar deze worden beduidend minder vaak genoemd en lijken – in vergelijking met bovengenoemde thema's - minder sterke ontwikkelgebieden te zijn.

9.1.2 Evalueren van beleid

Een aantal instellingen zijn op een of meer thema's in de evaluatiefase. Zij hebben op die terreinen vastgesteld beleid dat in uitvoering is. De laatste stap is dan het vervolmaken van de PDCA-cyclus door het kennisveiligheidsbeleid actief te monitoren, evalueren, en mogelijk aanpassen. Ten slotte heeft een aantal instellingen de ambitie uitgesproken in de komende tijd eerder uitgevoerde risicoanalyses en kroonjuwelenanalyses te herhalen.

9.1.3 Landelijke beleidsontwikkelingen

Meerdere instellingen geven aan landelijke beleidsontwikkelingen in de gaten te houden voor hun eigen beleidsontwikkeling. Het gaat hier om de wet screening kennisveiligheid en de actualisatie van de Leidraad Kennisveiligheid.

Sommige instellingen geven aan te wachten met hun personeelsbeleid tot het wetsproces rondom de wet screening kennisveiligheid is afgerond. Hun redenatie hierbij is dat instellingen niet teveel middelen willen steken in beleid dat vanwege de wet screening mogelijk op korte termijn weer achterhaald is. De wet screening gaat immers van invloed zijn op het personeelsbeleid van instellingen, met name als het gaat om pre-screening. Ook in de cases komt dit bij alle type instellingen duidelijk

naar voren. Er zijn vaak al wel gesprekken opgestart over screening, maar er is hierover nog geen beleid gevormd. Instellingen wijzen erop dat bij doorvoering van de wet screening kennisveiligheid, screening bij de Rijksoverheid wordt belegd en niet bij instellingen zelf. Hierdoor zou de screening beperkter onderdeel worden van interne processen. Aan de andere kant bestaat ook de kans dat instellingen vanwege de wet meer pre-screening gaan doen, om zeker(der) te weten dat hun kandidaat door de screening komt. In de cases worden ook specifieke zorgen geuit over de wet screening kennisveiligheid. Hierbij wordt o.a. de doorlooptijd van screening en schijnzekerheid als risico's gezien. Ook wordt benoemd dat voorbereiding op de wet screening kennisveiligheid veel tijd kost.

Ook geven meerdere instellingen aan hun beleid aan te passen op basis van de actualisatie van de Leidraad. Zij kijken reikhalzend naar de herziene versie uit, omdat hij voor veel instellingen de basis van hun beleid vormt. Daarbij helpt de (nieuwe) Leidraad kennisveiligheidscoördinatoren in het bijzonder met het agenderen van kennisveiligheid binnen de instellingen, zowel onder bestuurders als onder onderzoekers. Instellingen ervaren de huidige Leidraad dus als nuttig, maar soms wel als lang en breed. We horen veel geluiden dat instellingen behoefte hebben aan een Leidraad waarin minder beleidsthema's aan bod komen, maar op de belangrijke thema's meer diepgang wordt gegeven. Informatiebeveiliging wordt vaak genoemd als thema dat instellingen minder nodig vinden in de Leidraad.

9.2 Behoeften van instellingen richting de Rijksoverheid

De kennisinstellingen zijn in deze meting overwegend positief over de beleidsaanpak en ondersteuning vanuit de Rijksoverheid. De Leidraad heeft wat instellingen betreft bijgedragen aan de voortgang van hun beleid. Ook wordt waardering uitgesproken voor de oprichting en activiteiten van het Loket Kennisveiligheid, omdat het instellingen ondersteuning biedt en liet zien dat de Rijksoverheid zelf bereid is middelen beschikbaar te maken voor het versterken van de kennisveiligheid in Nederland. Instellingen waarderen dat de Rijksoverheid gekozen heeft voor een lerende aanpak met veel institutionele autonomie. Daarbij is de vorm van een bestuursakkoord positief ervaren, omdat het voor duidelijke afspraken en verwachtingen (inclusief middelen) zorgde, zonder direct naar wetgeving te grijpen.

Tegelijkertijd kijken instellingen voor de ontwikkeling van hun kennisveiligheidsbeleid voor een aantal punten naar de Rijksoverheid. Instellingen spreken de behoefte uit voor:

- Financiële houdbaarheid. Instellingen spreken zorgen uit over de financiële houdbaarheid van hun kennisveiligheidsbeleid. Het huidige bestuursakkoord met bijbehorende financiële middelen loopt binnenkort af en instellingen ervaren de incidentele financiële impuls van

OCW (hoewel gewaardeerd) niet als voldoende om kosten te dekken. Met name het implementeren van mitigerende maatregelen, in het bijzonder compartimentalisering van digitale en fysieke infrastructuur, zien instellingen als een significante kostenpost waarvoor nu geoormerkte middelen ontbreken.

- Handzame bronnen voor het uitvoeren van een risicoanalyse en maken van bijbehorende afweging. Instellingen maken hun afweging vaak op basis van twee aspecten: de affiliatie(s) van de samenwerkingspartners/mogelijk werknemer en het onderzoeksonderwerp. Op beide aspecten formuleren instellingen behoeften.
    - Affiliatie. Instellingen zoeken naar bronnen die hen helpen bepalen welke affiliaties risico's met zich meebrengen. Hoewel de wens voor een generieke bron bestaat, komt met name de wens voor een Europees of Nederlands alternatief voor de ASPI-tracker – een bron specifiek gericht op Chinese instellingen - vaak terug. Instellingen maakten hier massaal gebruik van zolang deze gratis te gebruiken was. Nu dat niet meer het geval is, zijn instellingen zelf bronnen gaan ontwikkelen of inkopen, maar een Nederlands of Europees alternatief is alsnog gewenst. Ook een gezamenlijke licentie voor de ASPI-tracker is voor sommige instellingen een optie, andere instellingen zijn liever niet afhankelijk van een lijst van een Australische denktank. De reden dat een alternatief voor ASPI vaak gevraagd wordt, komt doordat instellingen vaak met Chinese partners te maken hebben, en dat zij de affiliatie-afweging hier complexer vinden dan bij risicolanden die op een sanctielijst staan. Het zou de uniformiteit van het kennisveiligheidsbeleid ten goede komen als alle instellingen met dezelfde bronnen werken.
    - Onderzoeksonderwerp. Instellingen zijn kritisch op de bruikbaarheid van bestaande lijsten met sensitieve onderzoeksgebieden omdat ze in hun ogen te ongenuanceerd zijn. Bijlage 2 van het wetsvoorstel screening kennisveiligheid wordt hierbij vaak genoemd. Instellingen zijn kritisch op brede lijsten omdat sommige specifieke onderzoeksgebieden binnen een breed thema niet per sé sensitief hoeven te zijn. Volgens respondenten zijn sommige onderzoeksgebieden die nu onder bijlage 2 vallen evident niet sensitief. Hierdoor merken kennisveiligheidscoördinatoren dat kennisveiligheidsbeleid op weerstand en onbegrip stuit binnen hun instelling. Tegelijkertijd heeft een te specifieke lijst ook nadelen. Een zeer gedetailleerde lijst creëert mogelijk schijnzekerheid (alsof dingen buiten de lijst totaal niet sensitief zijn) en vereist ook regelmatige actualisatie. Ongeacht de breedte van de lijst blijft het lastig om te bepalen wanneer een onderzoeksonderwerp sensitief is, zeker bij onderzoek op lage TRL-niveaus.
- Een duidelijk(er) en concreet(er) handelingskader. We merken uit de vragenlijst en de gesprekken dat het gezamenlijk ontwikkelde document met Indicatoren voor Risicoinschatting Internationale Samenwerkingen Kennisveiligheid (2025) breed in de sector

gebruikt wordt en instellingen houvast geeft bij het bepalen van de vraag of sprake is van risico's voor kennisveiligheid. Aanvullend heeft een deel van de Kennisveiligheidscoördinatoren behoefte aan meer richting bij het maken van afwegingen wanneer sprake is van risico's. Veel instellingen hebben behoefte aan meer concrete tips en voorbeelden vanuit de Rijksoverheid. Om dat passend te krijgen, is het voor de sector belangrijk dat zo'n nadere invulling voldoende specifiek per onderzoeksgebied is, en ook rekening houdt met de diversiteit aan risicoprofielen binnen de sector. Belangrijk voor instellingen is dat ze zelf afwegingen kunnen blijven maken, maar daar verder en beter bij ondersteund worden. Instellingen benadrukken dat ook een duidelijk handelingskader geen uitsluitsel kan geven bij complexe casuïstiek, en dat een maatwerk-oordeel altijd nodig zal blijven.

- Tools voor naleving exportwetgeving en technische bijstand bij sanctieregels. Instellingen worstelen met de naleving van complexe exportwetgeving en technische bijstand bij sanctieregels omdat het specifieke juridische expertise vereist. Er is duidelijke vraag naar een handzaam document, of een concrete tool waarmee zelf kunnen nagaan of zij voldoen aan deze wetgeving.

10 Conclusies

In dit hoofdstuk vatten we de uitkomsten uit dit sectorbeeld kennisveiligheid samen in een aantal conclusies waarmee we de onderzoeksvragen 1 tot en met 4 beantwoorden.

Conclusie 1. De Leidraad Kennisveiligheid is breed geïmplementeerd. We zien dat op alle thema's van de Leidraad de meeste instellingen beleid hebben geïmplementeerd. Nagenoeg alle instellingen bereiken minimaal een initieel niveau bij de vertaalslag van juridische kaders (zoals sanctie- en exportwetgeving) naar interne procedures. De grootste groep instellingen beschikt over vastgestelde toetsingskaders en procedures voor risico-inschatting en verantwoordelijkheden zijn bij bijna alle instellingen formeel belegd. Veel instellingen hebben wel een centraal overzicht van internationale samenwerkingen die periodiek handmatig geactualiseerd dient te worden.

De meerderheid van de instellingen geeft aan dat HR-personeel op de hoogte is van kennisveiligheidsrisico's, toegang heeft tot bronnen om risico's te herkennen en zo nodig samenwerkt met het adviesteam kennisveiligheid om risico's te mitigeren. Meer dan 70% van de instellingen geeft aan (nieuwe) medewerkers informatie en training te geven om hen meer veiligheidsbewust te maken. De nadruk ligt hierbij sterker bij (online) informatievoorziening dan bij het verzorgen van trainingen. Bijna alle instellingen hebben beleid voor buitenlandse dienstreizen, meer dan een derde van de instellingen heeft hiervoor een protocol. De meeste instellingen hebben initieel beleid rondom fysieke beschermingsmaatregelen, ook de samenhang met het digitale beschermingsmaatregelen is meestal nog in ontwikkeling.

Conclusie 2. De Nederlandse kennissector heeft breed vooruitgang geboekt ten opzichte van de vorige sectorbeelden. Op vrijwel alle thema's vinden de meeste instellingen zichzelf volwassener geworden. Dit beeld wordt bevestigd in de casestudy. Die vooruitgang zien we gemiddeld over alle type instellingen heen, al is de ontwikkeling verschillend per thema, instelling en ook subsector. Hoewel veranderingen in de vragenlijst kunnen meespelen in de interpretatie van individuele scores, heeft ten opzichte van de nulmeting een duidelijke verschuiving plaatsgevonden: waar instellingen toen nog veelal beleid aan het vormgeven en vaststellen waren, zijn ze dat nu aan het uitvoeren en soms al aan het evalueren. Kennisveiligheidsbeleid is meer geïnstitutionaliseerd geworden. Bewustzijn van kennisveiligheid is zowel verbreed (meer mensen binnen instellingen hebben het op hun radar) als verdiept (bij mensen die al met kennisveiligheid bezig waren is expertise vergroot).

Conclusie 3a. De sector is nog niet volledig uitontwikkeld. Meer dan de helft van de instellingen – voornamelijk instellingen met een hoger zelf ingeschat risicoprofiel – willen nog stappen in volwassenheid zetten. Sommige van deze instellingen hebben hier al concrete plannen voor, andere nog niet. De plannen voor doorontwikkeling richten zich voornamelijk op het verder uitvoeren,

evalueren en borgen van beleid, en het evalueren van eerder gemaakte risicoanalyses. Binnen de thema's van de Leidraad zien instellingen *real-time* registratie van internationale partnerschappen en bewustzijn onder medewerkers als grootste ontwikkelpunten.

Conclusie 3b. We zien wel duidelijke differentiatie binnen de sector. Het gewenste volwassenheidsniveau verschilt tussen instellingen, tussen en binnen subsector, en tussen thema's. Waar instellingen met een hoger zelf ingeschat risicoprofiel nog duidelijke ambities hebben, vindt een groep instellingen met een zelf ingeschat laag risicoprofiel zich uitontwikkeld. Deze groep bestaat uit kleine, monosectorale hogescholen die de onderbouwde keuze gemaakt hebben om vanwege het weinig risico's geen of beperkt beleid ten aanzien van kennisveiligheid te voeren. Dit zijn echter niet alle kleine, monosectorale hogescholen: sommigen van hen hebben wel een uitgewerkt beleid en/of willen nog verder ontwikkelen.

Conclusie 3c: De voornaamste verklaringen voor nog niet gerealiseerde ambities zijn beperkte tijd en capaciteit. Instellingen vinden bewustzijn en draagvlak op de werkvloer essentieel voor hun kennisveiligheidsbeleid. Ze geven aan dit tijd kost en enkel kan door in dialoog te blijven. Tevens is het vrijmaken van tijd of vinden van de juiste kennisveiligheidsmedewerkers soms een uitdaging. Het is bij sommige instellingen pas later is gelukt om de juiste inhoudelijke expertise, kennis van de instelling en procesmatige vaardigheden bij elkaar te brengen, wat heeft geleid tot vertraging in hun kennisveiligheidsbeleid. Ook geven sommige instellingen aan te wachten op landelijke beleidsontwikkelingen – de actualisatie van de Leidraad en de wet screening kennisveiligheid – voor ze hun eigen beleid verder ontwikkelen. Inhoudelijk lopen instellingen op specifieke onderwerpen tegen praktische obstakels aan zoals een gebrek aan concrete en hanteerbare bronnen, tools en adviezen, vooral voor het maken van gerichte risico-afwegingen van affiliaties en de sensitiviteit van onderzoeksthema's of technologieën.

Conclusie 4. De onderliggende dilemma's zijn dezelfde als in de nulmeting, er zijn wel stappen op gezet. Instellingen lopen net als in de nulmeting tegen onderstaande onderliggende dilemma's aan bij het uitwerken van hun kennisveiligheidsbeleid. De eerste twee dilemma's weten instellingen beter mee om te gaan de afgelopen jaren, voor de laatste drie dilemma's zien we, op basis van de toelichtingen in de vragenlijst en de gesprekken, dat het denken hierover breder en verder ontwikkeld is:

a) **Kennisveiligheid en academische kernwaarden**. Instellingen ervaren dilemma's tussen kennisveiligheidsbeleid en open science, academische vrijheid, non-discriminatie en inclusiviteit. Dit dilemma komt in deze meting echter minder sterk naar voren dan tijdens de nulmeting. Een aantal instellingen geeft ook aan dat zij kennisveiligheid juist zien als mogelijkheid om academische kernwaarden te beschermen.

b) **Proportionaliteit**. Instellingen hebben afgelopen jaren hun risico's geanalyseerd en deze met samenhangend beleid proberen te mitigeren, soms met inzet van specialistische expertise. Zeker voor instellingen met een lager risicoprofiel is het de vraag wat een passende en proportionele inzet moet zijn voor registratie, processen en functies voor risicomanagement. In de nulmeting was dit vaak een argument om geen beleid te hebben, nu zien we het vaker als een onderbouwing van een beperkte beleidsinzet.
c) **Maatwerk versus duidelijk kaders en richtlijnen**. Instellingen zoeken naar een optimum tussen maatwerk en generieke richtlijnen. Instellingen maken vaak tijdrovende case-by-case afwegingen. Met duidelijke kaders wordt het maken van een beslissing efficiënter maar ligt het risico op schijnzekerheid op de loer. Ook bestaat het risico dat een duidelijk kader samenwerkingen uitsluit die met een case-by-case benadering wel zouden kunnen. Instellingen worstelen met – in hun ogen – te generieke lijsten over sensitiviteit van onderzoek, bepaling of iets dual-use is (zeker bij laag TRL onderzoek) en een gebrek aan handzame tools.
d) **Voorkomen stigmatisering en discriminatie**. Screening van personeel en focus op risicolanden brengt risico's op stigmatisering en discriminatie met zich mee. Bewustzijn van kennisveiligheid is voor instellingen essentieel, maar overbewustzijn of het willen uitsluiten van elk risico kan stigmatisering in de hand werken. Ook signaleren instellingen dat uitkomsten van een case-by-case afweging door een adviesteam, op de werkvloer soms als een generieke richtlijn wordt ervaren.
e) **Gelijk speelveld**. Instellingen benoemen meermaals dat andere landen vrijblijvender of juist dwingender kennisveiligheidsbeleid voeren. Dit leidt tot waterbedeffecten en bemoeilijkt internationale samenwerkingen. Met name bij grote internationale partnerschappen zorgt dit voor wrijving. Men pleit in ieder geval voor een zoveel mogelijk gezamenlijke Europese aanpak.

Conclusie 5a. De sector is overwegend positief over de lerende aanpak van de Rijksoverheid. Instellingen waarderen dat de Rijksoverheid gekozen heeft voor een lerende aanpak waar de institutionele autonomie gerespecteerd is. Wat instellingen betreft moet de verantwoordelijkheid voor het maken van keuzes ook bij henzelf blijven liggen. De Leidraadheeft wat instellingen betreft bijgedragen aan de voortgang en de oprichting en activiteiten van het Loket Kennisveiligheid worden breed gewaardeerd.

Conclusie 5b. De sector heeft behoefte aan meer proactieve ondersteuning en richting van de Rijksoverheid. Binnen hun institutionele autonomie zoeken instellingen meer specifieke ondersteuning en richting vanuit de Rijksoverheid. Zij spreken specifiek de behoefte uit voor:

a) **Financiële ondersteuning**. Instellingen spreken zorgen uit over de financiële houdbaarheid van hun kennisveiligheidsbeleid, omdat het implementeren van beleid en mitigerende maatregelen kostbaar is maar niet is opgenomen in de structurele bekostiging.
b) **Handzame bronnen** voor het uitvoeren van een risicoanalyse en maken van bijbehorende afwegingen. Op drie aspecten hebben instellingen behoeften:
    1. Affiliatie. Instellingen zoeken een betere en meer uniforme bron die helpt met bepalen welke risico's met een affiliatie gemoeid zijn.
    2. Onderzoeksonderwerp. Instellingen zijn kritisch op de bruikbaarheid van bestaande lijsten met sensitieve onderzoeksgebieden omdat ze in hun ogen te ongenuanceerd zijn. Dilemma C (hierboven benoemd) speelt hier: instellingen zijn kritisch op brede lijsten omdat sommige specifieke onderzoeksgebieden binnen een breed thema niet per sé sensitief hoeven te zijn maar een zeer gedetailleerde lijst creëert mogelijk schijnzekerheid (alsof dingen buiten de lijst totaal niet sensitief zijn) en vereist ook regelmatige actualisatie. Het is de vraag in hoeverre hier een goede middenweg tussen gevonden kan worden.
    3. Tools voor naleving exportwetgeving en sanctieregels. Instellingen worstelen met de naleving van complexe exportwetgeving en technische bijstand bij sanctieregels omdat het specifieke juridische expertise vereist. Er is duidelijke vraag naar handzaam document, of een concrete tool waarmee zelf kunnen nagaan of zij voldoen aan deze wetgeving.
c) **Een duidelijk(er) en concreet(er) handelingskader**. Kennisveiligheidscoördinatoren hebben aanvullend aan de set uniforme risico-indicatoren behoefte aan meer richting en ondersteuning vanuit de Rijksoverheid bij het maken van afwegingen in het geval van (potentiële) risico's. Om dat passend te krijgen, is het voor de sector belangrijk dat zo'n nadere invulling voldoende specifiek per onderzoeksgebied is, en ook rekening houdt met de diversiteit aan risicoprofielen binnen de sector. Belangrijk voor instellingen is dat ze zelf afwegingen kunnen blijven maken, maar daar verder en beter bij ondersteund worden.

Bijlage 1. Samenstelling klankbordgroep

Naam	Affiliatie
Han Boter	Universitair Medisch Centrum Groningen
Hanna van Lee	Technische Universiteit Delft
Johannes Versluijs	Fontys Hogeschool
Maaike Wagenaar	Rijksuniversiteit Groningen
Mirelle van Emmerik	Maastricht University
Miriam Roelofs / Ella Bosch	NWO-I
Wietske Hurrelbrinck	KNAW

Bijlage 2. Vragenlijst self-assessment

Welkom!

Context en doel van de meting

Het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) heeft onderzoeksbureaus Dialogic en Oberon gevraagd een vervolgmeting uit te voeren naar kennisveiligheidsbeleid onder universiteiten, hogescholen, KNAW- en NWO-instituten. Deze meting is een vervolg op de 0-metingen die in 2023-2024 zijn uitgevoerd, en is door de minister toegezegd aan de Tweede Kamer. In tegenstelling tot de vorige meting waar verschillende sectorbeelden werden opgeleverd, wordt er bij deze meting een sectorbeeld opgeleverd. De antwoorden op deze vragenlijst zijn anoniem. In het sectorbeeld zijn antwoorden niet herleidbaar naar instellingen.

We onderzoeken in de vervolgmeting de stand van implementatie van **de Nationale Leidraad Kennisveiligheid 2022[1].** Hierbij brengen we veranderingen ten opzichte van de nulmeting in kaart en onderzoeken we ontwikkelingen, dilemma's en good practices. We zijn geïnteresseerd in de mate waarin kennisinstellingen vinden dat de stand van hun beleid aansluit bij hun zelf-ingeschatte risicoprofiel.

Deze vragenlijst is opgesteld door Dialogic en Oberon in afstemming met het ministerie van OCW ende klankbordgroep van het onderzoek - met daarin betrokkenen en vertegenwoordigers vanuit de sector. U ontvangt deze vragenlijst omdat u door uw instelling als contactpersoon bent voorgedragen bij het ministerie van OCW.

Indien gewenst kunt u de link naar de vragenlijst of de bijgevoegde pdf intern verspreiden; we verzoeken u de vragenlijst niet buiten uw instelling te verspreiden. We vragen u de afhandeling van de vragenlijst ook af te stemmen met de bestuurlijk portefeuillehouder kennisveiligheid van uw instelling.

Toelichting op de vragenlijst

Voor de beantwoording van vragen hanteren we de volgende uitgangspunten:

- Vragen hebben betrekking op de ***aanwezigheid*** *van* beleid en processen om afwegingen te maken. We vragen nadrukkelijk niet naar concrete uitkomsten of uitvoering ervan. Bijvoorbeeld: wij vragen of uw instelling beleid heeft om te bepalen of voor bepaalde ruimtes restrictief toegangsbeleid nodig is. Daarbij zijn we vooral geïnteresseerd in hoe u tot zulke besluiten komt - bijvoorbeeld welke stappen u volgt of wie erbij betrokken zijn - en niet in een overzicht van specifieke ruimtes of de afzonderlijke afwegingen per ruimte.
- Met vragen over het bestaan van beleid, processen of verantwoordelijken bedoelen we niet dat er altijd sprake zou m6eten zijn van beleid of procedures. De wenselijkheid of noodzakelijkheid van beleid is afhankelijk van de context van uw instelling. Daarom kunt u in alle vragen aangeven welk niveau past bij het risicoprofiel van uw instelling, waar uw beleid nu staat, en waarom.
- Net als in de nulmeting hanteren we rubrics. Ten opzichte van de nulmeting zijn de niveaus specifieker omschreven en kunt u telkens ook aangeven waar u vindt dat het beleid van uw instelling zou moeten staan.
- Omdat de vragenlijst zien richt op beleid, verwachten we dat deze grotendeels kan worden ingevuld door de coördinator kennisveiligheid. We realiseren ons echter dat kennisveiligheid verschillende afdelingen raakt. Waar nodig kan daarom afstemming worden gezocht met collega's, bijvoorbeeld als het beleid wordt ontwikkeld of beheerd door andere onderdelen van de organisatie. We verwachten echter niet dat u intensief afstemming hoeft te zoeken met collega's betrokken bij de uitvoering van beleid.
- In overleg tussen OCW en NFU is besloten dat net als in de nulmeting de UMC's niet als afzonderlijke instellingen in het onderzoek worden betrokken. Het wetenschappelijk onderzoek en onderwijs bij UMC's wordt meegenomen in het onderzoek bij de universiteiten. Daarom is de vraag aan universiteiten met een UMC om deze te betrekken bij het invullen van de vragenlijst.
- Terminologie in deze vragenlijst is gebaseerd op de oorspronkelijke Leidraad Kennisveiligheid uit 2022. Waar de Leidraad een term niet definieert, hebben we ervoor gekozen niet zelf een definitie in te vullen.

Vertrouwelijkheid van de vragenlijst

De antwoorden worden vertrouwelijk behandeld en leiden na analyse tot een geanonimiseerd sectorbeeld voor de gehele kennissector (dus universiteiten, hogescholen, **KNAW-** en NWO-instituten samen) waarin individuele instellingen niet herkenbaar zullen zijn. In het sectorbeeld worden geen antwoorden uit de vragenlijsten geciteerd of op een naar instellingen herleidbare wijze beschreven. Waar relevant worden in het sectorbeeld verschillen tussen typen instellingen op een anonieme manier beschreven.

Het brede beeld uit de vragenlijst vullen we later aan met verdiepende casestudies bij een selectie van instellingen. De case studies dienen om inhoudelijk interessante praktijken, dilemma's en knelpunten beter te begrijpen. Het sectorbeeld wordt door OCW aan de Tweede Kamer aangeboden.

Daarnaast ontvangt iedere deelnemende instelling een eigen instellingsbeeld waarin de gegeven antwoorden worden geplaatst in de context van het algemene sectorbeeld. Op deze manier draagt de vervolgmeting bij aan een lerende aanpak. Dit instellingsbeeld wordt **niet gedeeld** met OCW, de Tweede Kamer of derden.

Alleen projectmedewerkers van Dialogic en Oberon hebben toegang tot de omgeving waarin de (ingevulde) vragenlijst beschikbaar is. Uiterlijk een maand na afloop van het onderzoek verwijderen wij de ingevulde vragenlijsten (en eventueel gedeelde bijlagen).

Onderwerpen in de vragenlijst

In de vragenlijst kamen achtereenvolgens kennisveiligheid en academische kernwaarden, juridische kaders en gedragscodes, het inschatten van risico's, risicomanagement, internationale partnerschappen, personeelsbeleid, en de doorontwikkeling van kennisveiligheidsbeleid aan bod. Ter afsluiting vragen we u om een reflectie op deze vervolgmeting.

Praktische zaken

We verzoeken u de vragenlijst uiterlijk **17 oktober** volledig ingevuld te retourneren.

Macht u vragen hebben over het onderzoek, de vragenlijst, of de vragen op een andere manier willen beantwoorden, dan kunt u contact opnemen met uw eigen contactpersoon, deze persoon staat vermeid in de e-mail die u met de vragenlijst heeft ontvangen.

---

[1] Deze is opgesteld door UNL, KNAW, de VH, NFU, de T02 federatie, NWO en OCW. Zie: Nationale Leidraad kennisveiligheid - Veilig internationaal samenwerken /Rapport/ Rijksoverheid.nl

1.2 Kennisveiligheid en het beschermen van academische kernwaarden

De volgende vragen gaan over uw definitie van kennisveiligheid en de verhouding tussen kennisveiligheidsbeleid en academische kernwaarden. Binnen de kennissector vormen academische kernwaarden zoals academische vrijheid en wetenschappelijke integriteit de toetsstenen van het handelen van instellingen.

1. Is de manier waarop uw instelling het begrip kennisveiligheid hanteert of definieert in de afgelopen twee jaar veranderd? *

- ◯ Ja*
- ◯ Nee*

1a. Zo ja, kunt u kort toelichten wat er precies is veranderd en waarom? *

Bovenstaande vraag alleen invullen indien de vraag *"1. Is de manier waarop uw instelling het begrip kennisveiligheid hanteert of definieert in de afgelopen twee jaar veranderd?* "is beantwoord met "Ja".

1b. Zo nee, kunt u toelichten waarom niet?*

Bovenstaande vraag alleen invullen indien de vraag *"1. Is de manier waarop uw instelling het begrip kennisveiligheid hanteert of definieert in de afgelopen twee jaar veranderd?* "is beantwoord met "Nee".

2. Op welke manier is er in uw kennisveiligheidsbeleid aandacht voor academische kernwaarden en Open Science? *

Bij internationale samenwerkingen kunnen ook ethische dilemma's een rol spelen.

3. Hoe wordt binnen uw instelling aan ethische oordeelsvorming over kennisveiligheidsvraagstukken gedaan? *

4. Heeft uw instelling een of meer commissie(s) waar onderzoekers internationale samenwerkingen waarbij

ethische dilemma's spelen kunnen melden en bespreken? *

- ◯ Ja*
- ◯ Nee*

4a. Zo ja, wat is de positie en rol van deze commissie binnen uw instelling?*

Bovenstaande vraag alleen invullen indien de vraag *"4. Heeft uw instelling een of meer commissie(s) waar onderzoekers internationale samenwerkingen waarbij ethische dilemma's spelen kunnen melden en bespreken?* "is beantwoord met “Ja".

4b. Zo ja, heeft deze commissie ook de taak om andere ethische vraagstukken te behandelen?*

Bovenstaande vraag alleen invullen indien de vraag *"4. Heeft uw instelling een of meer commissie(s) waar onderzoekers internationale samenwerkingen waarbij ethische dilemma's spelen kunnen melden en bespreken?* "is beantwoord met “Ja".

4c. Hoe wordt omgegaan met de adviezen van de commissie(s) *

Bovenstaande vraag alleen invullen indien de vraag *"4. Heeft uw instelling een of meer commissie(s) waar onderzoekers internationale samenwerkingen waarbij ethische dilemma's spelen kunnen melden en bespreken?* "is beantwoord met “Ja".

4d. Zo nee, kunt u toelichten waarom niet?*

Bovenstaande vraag alleen invullen indien de vraag *"4. Heeft uw instelling een of meer commissie(s) waar onderzoekers internationale samenwerkingen waarbij ethische dilemma's spelen kunnen melden en bespreken?* "is beantwoord met "Nee".

5. Kunt u in onderstaande rubric aangeven in hoeverre uw kennisveiligheidsbeleid rekening houdt met inclusiviteit en non-discriminatie?*

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Het kennisveiligheidsbeleid neemt geen directe maatregelen om inclusiviteit en non-discriminatie te garanderen.
Initieel/in ontwikkeling	Er wordt gewerkt aan het opnemen van principes om inclusiviteit en non-discriminatie in het kennisveiligheidsbeleid te garanderen.
Herhaalbaar en/of gedefinieerd	In het beleid voor kennisveiligheid zijn expliciet principes opgenomen om inclusiviteit en non-discriminatie te garanderen.
Meetbaar en gemanaged	De instelling evalueert periodiek of kennisveiligheidsmaatregelen kunnen leiden tot uitsluiting, stigmatisering of discriminatie en hoe dit te mitigeren.
Continue verbetering	De instelling heeft een structureel proces ingericht waarin de impact van kennisveiligheidsmaatregelen op inclusiviteit en non-discriminatie wordt gemonitord, besproken met betrokkenen, en (indien nodig) aangepast.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

6. Wat is uw inhoudelijke toelichting bij deze scores? *

7. Heeft u verder nog opmerkingen of een toelichting ten aanzien van kennisveiligheid en het beschermen van academische kernwaarden?

1.3 Juridische kaders en gedragscodes

Voor sommige onderdelen van het kennisveiligheidsbeleid gelden een aantal bestaande juridische kaders en gedragscodes, zoals sanctie- en exportcontroleregelgeving. U kunt aan de hand van onderstaande vragen aangeven in hoeverre uw instelling hier mee te maken heeft en hoe uw instelling hiermee omgaat.

8. Kunt u in onderstaande rubric aangeven waar uw kennisveiligheidsbeleid staat ten aanzien van de naleving van juridische kaders en gedragscodes?*

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Medewerkers zijn zien niet bewust van sanctie- en exportcontroleregelgeving bij internationale samenwerking en werving.
Initieel/in ontwikkeling	Medewerkers beoordelen de relevantie van wettelijke kaders ad hoc. Er is geen *structureel* bewustzijn van sanctie- en exportcontroleregelgeving bij internationale samenwerking en werving.
Herhaalbaar en/of gedefinieerd	Medewerkers zijn zien enigszins bewust van sanctie- en exportcontroleregelgeving van toepassing op internationale samenwerkingen. Relevant personeel heeft werkwijzen ontwikkeld om te voldoen aan deze regels en communiceert deze per geval. De instelling heeft maatregelen voor interne naleving. Er zijn medewerkers verantwoordelijk voor deze naleving.
Meetbaar en gemanaged	Er is een periodieke evaluatie en verbetering van de naleving van wettelijke kaders.
Continue verbetering	De naleving van de wettelijke kaders ondergaat een voortdurende evaluatie- en verbetercyclus.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

9. Wat is uw inhoudelijke toelichting bij deze scores? *

10. Hoe is compliance met EU-exportcontrole van dual-use-technologie [2] geborgd binnen uw instelling? In hoeverre zijn dit soort exportregels voor uw instelling - gegeven het risicoprofiel - relevant en hoe bent u tot die afweging gekomen?*

[2] Voor *dual-use* technologieën zijn gedetailleerde Europese exportregels opgesteld. De kennisvelden die mogelijk onder deze regels vallen zijn opgedeeld in 10 categorieën, te weten: nucleaire goederen, speciale materialen en aanverwanten apparatuur, materiaalverwerking, elektronica, computers, telecommunicatie en informatiebeveiliging, sensoren en lasers, navigatie en vliegtuigelektronica, zeewezen en schepen & ruimtevaart en voortstuwing.

10a. Heeft u bij het implementeren/interpreteren behoefte aan ondersteuning vanuit het rijk?*

11. Hoe wordt binnen uw instelling bepaald of een technologie dual-use is?*

12. Hoe is compliance met niet-EU import- en exportregels geborgd? In hoeverre zijn dit soort exportregels voor uw instelling - gegeven het risicoprofiel – relevant en hoe bent u tot die afweging gekomen?*

U kunt hierbij denken aan het in- en doorverkopen van Amerikaanse apparatuur.

12a. Heeft u bij het implementeren/interpreteren behoefte aan ondersteuning vanuit het rijk?*

13. Hoe is compliance met internationale en EU-sanctieregimes geborgd binnen uw instelling? In hoeverre zijn dit soort regels voor uw instelling - gegeven het risicoprofiel – relevant en hoe bent u tot die afweging gekomen?*

U kunt hier denken aan sanctieregimes ten aanzien van Rusland of Iran.

13a. Heeft u bij het implementeren/interpreteren behoefte aan ondersteuning vanuit het rijk?*

14. Hoe worden gedragscodes zoals het kader kennisveiligheid Instellingen, de EU guidelines on Tackling R&I foreign interference, of andere gedragscodes, binnen uw instelling toegepast?*

15. Heeft u verder nog opmerkingen of een toelichting ten aanzien van juridische kaders en gedragscodes?

1.4 Het inschatten van risico's

De volgende vragen gaan in op de risico-inschattingen die uw instelling maakt als onderdeel van het eigen kennisveiligheidsbeleid.

14. Kunt u in onderstaande rubric aangeven waar uw kennisveiligheidsbeleid staat ten aanzien van een toetsingskader voor kennisveiligheidsrisico's?*

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen beleid voor de beoordeling van kennisveiligheidsrisico's.
Initieel/in ontwikkeling	Risico's worden ad hoc geïdentificeerd. Er is geen formele risicobeoordeling die eventuele vervolgstappen beschrijft.
Herhaalbaar en/of gedefinieerd	Er is een gedefinieerde risicobeoordelingsprocedure of een toetsingskader.
Meetbaar en gemanaged	Er is een periodieke evaluatie en de risicobeoordelingsmethodologie wordt periodiek verbeterd.
Continue verbetering	Er is ondersteuning en advies voor medewerkers, en een evaluatie- en verbetercyclus is aanwezig.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

15. Wat is uw inhoudelijke toelichting bij deze scores? *

We zijn benieuwd op welke manier uw instelling risicoanalyses voor kennisgebieden maakt. Kunt u dit aan de hand van onderstaande vragen beschrijven?

16. Worden sensitieve kennisgebieden binnen uw instelling geïdentificeerd? *

- ○ Ja*
- ○ Nee*

18a. Zo ja, wie doet dat precies en op welk moment vindt die analyse plaats? *

Bovenstaande vraag alleen invullen indien de vraag *"18. Worden sensitieve kennisgebieden binnen uw instelling geïdentificeerd?* "is beantwoord met "Ja".

18b. Zo nee, hoe is de afweging om dit niet te doen tot stand gekomen? *

Bovenstaande vraag alleen invullen indien de vraag *"18. Worden sensitieve kennisgebieden binnen uw instelling geïdentificeerd?* "is beantwoord met "Nee".

17. Hanteert uw instelling een (eigen) lijst met sensitieve kennisgebieden? *

- Ja*
- Nee*

Bovenstaande vraag alleen invullen indien de vraag *"18. Worden sensitieve kennisgebieden binnen uw instelling geïdentificeerd?* "is beantwoord met ".Ja".

19a. Zo ja, kunt u toelichten hoe deze tot stand komt en hoe uw instelling zorgt dat deze actueel blijft? *

Bovenstaande vraag alleen invullen indien de vraag *"19. Hanteert uw instelling een (eigen) lijst met sensitieve kennisgebieden?* "is beantwoord met ".Ja".

19b. Op welke manier bepaalt uw instelling of onderwijs of onderzoek onder deze kennisgebieden valt?*

Bovenstaande vraag alleen invullen indien de vraag *"19. Hanteert uw instelling een (eigen) lijst met sensitieve kennisgebieden?* "is beantwoord met ".Ja".

19c. Zo nee, hoe is de afweging om dit niet te doen tot stand gekomen? *

Bovenstaande vraag alleen invullen indien de vraag *"19. Hanteert uw instelling een (eigen) lijst met sensitieve kennisgebieden?* "is beantwoord met "Nee".

18. Brengt uw instelling de 'kroonjuwelen' in kaart? *

In de Leidraad wordt dit gedefinieerd als kennisgebieden waarbij kennisveiligheidsrisico's zijn verbanden aan kennisoverdracht en waarop uw instelling internationaal toonaangevend is.

- Ja*
- Nee*

20a. Zo ja, kunt u toelichten hoe dit wordt gedaan?*

Bovenstaande vraag alleen invullen indien de vraag *"20. Brengt uw instelling de 'kroonjuwelen' in kaart?* "is beantwoord met ':Ja".

20b. Zo nee, kunt u toelichten waarom niet? *

Bovenstaande vraag alleen invullen indien de vraag *"20. Brengt uw instelling de 'kroonjuwelen' in kaart?* "is beantwoord met "Nee".

19. We zijn benieuwd op welke manier uw instelling risicoanalyses maakt voor samenwerkingen met internationale partnerorganisaties en personen. Maakt uw instelling dit soort risicoanalyses?*

- Ja*
- Nee*

21a. Zo ja, wanneer kiest uw instelling ervoor om zo'n risicoanalyse te maken? *

Bovenstaande vraag alleen invullen indien de vraag *"21. We zijn benieuwd op welke manier uw instelling risicoanalyses maakt voor samenwerkingen met internationale partnerorganisaties en personen. Maakt uw instelling dit soort*

risicoanalyses?" is beantwoord met “Ja".

21b. Zo ja, hoe doet uw instelling dat en van welke informatiebronnen wordt daarbij gebruik gemaakt? *

Bovenstaande vraag alleen invullen indien de vraag *"27. We zijn benieuwd op welke manier uw instelling risicoanalyses maakt voor samenwerkingen met internationale partnerorganisaties en personen. Maakt uw instelling dit soort risicoanalyses?" is* beantwoord met 'Ja".

21c. Zijn er de afgelopen twee jaar veranderingen in kennisveiligheidsbeleid doorgevoerd in de manier waarop uw instelling, instituten, onderzoekers of projectleiders de samenwerking met buitenlandse partnerorganisaties of opdrachtgevers beoordelen? *

Zo ja, wat is hierin veranderd en wat was hiervoor de aanleiding?

Bovenstaande vraag alleen invullen indien de vraag *"27. We zijn benieuwd op welke manier uw instelling risicoanalyses maakt voor samenwerkingen met internationale partnerorganisaties en personen. Maakt uw instelling dit soort risicoanalyses?" is* beantwoord met "Ja".

21d. Zo nee, kunt u toelichten waarom niet?*

Bovenstaande vraag alleen invullen indien de vraag *"27. We zijn benieuwd op welke manier uw instelling risicoanalyses maakt voor samenwerkingen met internationale partnerorganisaties en personen. Maakt uw instelling dit soort risicoanalyses?" is* beantwoord met "Nee".

22. Zijn er binnen uw instelling standaardprocessen die in werking treden bij een bepaald risiconiveau van het kennisgebied en/of de achtergrond van de partnerorganisatie of persoon? *

- ○ Ja*
- ○ Nee*

22a. Zo ja, hoe zien deze standaardprocessen eruit?*

Bijvoorbeeld, worden de benodigde risicoanalyses en controles strikter? Komt de beslisbevoegdheid op een hoger, centraler niveau te liggen?

Bovenstaande vraag alleen invullen indien de vraag *"22. Zijn er binnen uw instelling standaardprocessen die in werking treden bij een bepaald risiconiveau van het kennisgebied en/of de achtergrond van de partnerorganisatie of persoon?* " is beantwoord met “Ja".

22b. Zo nee, kunt u toelichten hoe uw instelling hier dan mee omgaat? *

Bovenstaande vraag alleen invullen indien de vraag *"22. Zijn er binnen uw instelling standaardprocessen die in werking treden bij een bepaald risiconiveau van het kennisgebied en/of de achtergrond van de partnerorganisatie of persoon?* " is beantwoord met "Nee".

23. Heeft u verder nog opmerkingen of een toelichting ten aanzien van het inschatten van risico's?

1.5 Risicomanagement

De volgende vragen gaan in op de organisatie van risicomanagement op het gebied van kennisveiligheid binnen uw instelling. Kennisveiligheid kan belegd zijn bij verschillende afdelingen of bij verschillende verantwoordelijken. Om een beeld te krijgen hoe instellingen dit organiseren vragen we graag voor verschillende afdelingen of zij een rol spelen in het kennisveiligheidsbeleid van uw instelling.

24. Kunt u in onderstaande rubric aangeven waar uw kennisveiligheidsbeleidsbeleid staat als het gaat om registratie en overzicht van internationale overeenkomsten?*

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen beleid voor registratie van partnerschappen om relevante informatie vanuit het perspectief van kennisveiligheid te documenteren.
Initieel/in ontwikkeling	Internationale overeenkomsten en financiële transacties worden gedocumenteerd en bewaard. Toegang is toegewezen aan relevant personeel.
Herhaalbaar en/of gedefinieerd	Een overzicht van afspraken, financiering, werknemers is geregistreerd, centraal beschikbaar en wordt periodiek aan het hoger management gerapporteerd. Er wordt verantwoordelijkheid genomen voor archivering en toegang is toegewezen aan relevant personeel.
Meetbaar en gemanaged	Gemaakte overzichten van partnerschappen worden gebruikt voor analytische doeleinden en strategische besluitvorming. Procedures rondom het maken van deze overzichten worden periodiek geëvalueerd en aangepast.
Continue verbetering	Overzichten worden opgenomen in het managementinformatiesysteem, resultaten worden gebruikt voor training en bewustwording over kennisveiligheidsrisico's. De procedures ondergaan een voortdurende evaluatie- en verbeter cyclus.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

25. Wat is uw inhoudelijke toelichting bij deze scores? *

26. Als uw instelling internationale partnerschappen registreert: welke informatie over internationale partnerschappen registreert uw instelling? *

Als u dit niet registreert kan 'n.v.t' ingevuld worden.

26a. Kunt u toelichten hoe u tot deze selectie van typen gegevens bent gekomen?*

Als u dit niet registreert kan 'n.v.t' ingevuld worden.

27. Kunt u in onderstaande rubric aangeven op welk niveau de verantwoordelijkheden en processen van uw kennisveiligheidsbeleid belegd zijn? *

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen beleid om processen en verantwoordelijkheden rondom kennisveiligheid vorm te geven.
Initieel/in ontwikkeling	Sommige medewerkers van de instelling houden zien op ad hoc en informele basis bezig met kennisveiligheid. Er wordt gewerkt aan het formaliseren van de verantwoordelijkheden omtrent kennisveiligheid.
Herhaalbaar en/of gedefinieerd	Er is een formeel advies- of programmateam kennisveiligheid, en/of de Raad van Bestuur of het College van Bestuur heeft een portefeuillehouder kennisveiligheid aangesteld. Verantwoordelijkheden zijn toegewezen aan rollen en niveaus en zijn gedocumenteerd.
Meetbaar en gemanaged	De verdeling van taken en verantwoordelijkheden wordt periodiek geëvalueerd, gerapporteerd en indien nodig verbeterd.
Continue verbetering	De verdeling van taken en verantwoordelijkheden over rollen en niveaus en het functioneren en de samenstelling van het advies- of programmateam kennisveiligheid wordt voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0

Welk niveau heeft uw instelling nu?	0	0	0	0	0

28. Wat is uw inhoudelijke toelichting bij deze scores? *

29. Is er binnen uw instelling op bestuurlijk niveau een portefeuillehouder kennisveiligheid? *

- Ja*
- Nee*

29a. Zo ja, wat is de verantwoordelijkheid van de bestuurlijk portefeuillehouder? *

Bovenstaande vraag alleen invullen indien de vraag *"29. Is er binnen uw instelling op bestuurlijk niveau een portefeuillehouder kennisveiligheid?* "is beantwoord met ".Ja".

29b. Zo nee, hoe is de afweging gemaakt deze niet te hebben? *

Bovenstaande vraag alleen invullen indien de vraag *"29. Is er binnen uw instelling op bestuurlijk niveau een portefeuillehouder kennisveiligheid?* "is beantwoord met "Nee".

30. Heeft uw instelling een Adviesteam Kennisveiligheid?*

- Ja - de instelling heeft een eigen Adviesteam Kennisveiligheid*
- Ja - de instelling heeft een Adviesteam kennisveiligheid die (deels) gebundeld is met een andere instelling(en)*
- Nee*

30a. Kunt u de achtergrond, deskundigheid en samenstelling van dit team beschrijven? *

Bovenstaande vraag alleen invullen indien de vraag *"30. Heeft uw instelling een Adviesteam Kennisveiligheid?" is* beantwoord met ".Ja - de instelling heeft een eigen Adviesteam Kennisveiligheid" of ".Ja - de instelling heeft een Adviesteam kennisveiligheid die (deels) gebundeld is met een andere instelling(en)".

30b. Waarom heeft uw instelling ervoor gekozen om het adviesteam (of onderdelen daarvan) te bundelen met een

andere instelling(en)? *

Bovenstaande vraag alleen invullen indien de vraag *"30. Heeft uw instelling een Adviesteam Kennisveiligheid?"* is beantwoord met ".Ja - de instelling heeft een Adviesteam kennisveiligheid die (deels) gebundeld is met een andere instelling(en)".

30c. Zo nee, hoe is deze afweging gemaakt?*

Bovenstaande vraag alleen invullen indien de vraag *"30. Heeft uw instelling een Adviesteam Kennisveiligheid?" is* beantwoord met "Nee".

31. Op welke wijze wordt beleidsmatige afstemming verkregen tussen het instellingsbrede kennisveiligheidsbeleid ende decentrale onderdelen (zoals faculteiten, instituten, academies)?*

32. Zijn er vertrouwenspersonen of kennisloketten binnen uw instelling waar medewerkers terechtkunnen met signalen en vragen over veiligheidsrisico's? *

- ◯ Ja*
- ◯ Nee*

32a. Waarom wel?*

Bovenstaande vraag alleen invullen indien de vraag *"32. Zijn er vertrouwenspersonen of kennisloketten binnen uw instelling waar medewerkers terechtkunnen met signalen en vragen over veiligheidsrisico's?* "is beantwoord met ".Ja".

32b. Waarom niet?*

Bovenstaande vraag alleen invullen indien de vraag *"32. Zijn er vertrouwenspersonen of kennisloketten binnen uw instelling waar medewerkers terechtkunnen met signalen en vragen over veiligheidsrisico's?* "is beantwoord met "Nee"

33. In hoeverre zijn vertrouwenspersonen op de hoogte van wat kennisveiligheid is en met welke risico's de studenten/onderzoekers/docenten te maken kunnen krijgen?*

Bovenstaande vraag alleen invullen indien de vraag *"32. Zijn er vertrouwenspersonen of kennisloketten binnen uw instelling waar medewerkers terechtkunnen met signalen en vragen over veiligheidsrisico's?* "is beantwoord met ".Ja".

34. In hoeverre hebben de kennistransferbureau(s) binnen uw instelling een rol in het beleid rondom kennisveiligheid? *

- Ja*
- Nee*
- N.v.t.*

34a. Waarom wel?*

Bovenstaande vraag alleen invullen indien de vraag *"34. In hoeverre hebben de kennistransferbureau(s) binnen uw instelling een rot in het beleid rondom kennisveiligheid?* "is beantwoord met ".Ja".

34b. Waarom niet?*

Bovenstaande vraag alleen invullen indien de vraag *"34. In hoeverre hebben de kennistransferbureau(s) binnen uw instelling een rot in het beleid rondom kennisveiligheid?* "is beantwoord met "Nee".

35. Zijn er nog andere functionarissen of organen binnen uw instelling betrokken bij het beleid op kennisveiligheid?

- Ja*
- Nee*

35a. Zo ja, om welke functies gaat dit en welke rol spelen zij? *

Bovenstaande vraag alleen invullen indien de vraag *"35. Zijn er nog andere functionarissen of organen binnen uw instelling betrokken bij het beleid op kennisveiligheid?* "is beantwoord met ".Ja".

36. Heeft u verder nog opmerkingen of een toelichting ten aanzien van de organisatie van risicomanagement op kennisveiligheid?

1.6 Fysieke en digitale veiligheidsmaatregelen

1.6 Fysieke en digitale veiligheidsmaatregelen

37. Kunt u in onderstaande rubric aangeven waar uw instelling staat met betrekking tot de kwetsbaarheid van gebouwen en fysieke onderzoeksfaciliteiten[3] als onderdeel van kennisveiligheidsbeleid? *

[3] Kwetsbaarheid van onderzoeksfaciliteiten verwijst naar de mate waarin ruimten, apparatuur, systemen of processen binnen een instelling gevoelig zijn voor misbruik, sabotage, diefstal of ongewenste kennisoverdracht - met name in relatie tot kennisveiligheidsrisico's.

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er worden geen kwetsbaarheidsbeoordelingen uitgevoerd van gebouwen en fysieke onderzoeksfaciliteiten.
Initieel/in ontwikkeling	Relevante medewerkers en afdelingen (zoals opleidingen, instituten, faculteiten of dienstverlenende afdelingen) zijn bekend met kennisveiligheidsrisico's met betrekking tot hun fysieke faciliteiten en houden hier rekening mee.
Herhaalbaar en/of gedefinieerd	Risico's voor kennisveiligheid zijn geïdentificeerd en beschreven voor relevante gebouwen en onderzoeksfaciliteiten en risicobeperkende maatregelen zijn beschreven.
Meetbaar en gemanaged	Kennisveiligheidsmedewerkers bespreken periodiek de kwetsbaarheden met managers van de faciliteiten en stellen gezamenlijk aanpassingen voor als dat nodig is. Er is een periodieke evaluatie en verbetering afstemming tussen kennisveiligheidsbeleid en het fysieke veiligheidsbeleid.
Continue verbetering	De overzichten en methoden van de interne kwetsbaarheidsbeoordelingen worden in een cyclisch proces geëvalueerd en (indien nodig) verbeterd.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0

Welk niveau heeft uw instelling nu?	0	0	0	0	0

38. Wat is uw inhoudelijke toelichting bij deze scores? *

39. Wat is de samenhang tussen cyberveiligheidsbeleid en digitale veiligheidsbeleid en het kennisveiligheidsbeleid op uw instelling?*

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen beleid voor cyberveiligheid m.b.t. kennisveiligheidsrisico's.
Initieel/in ontwikkeling	Beleid voor gevoelige gegevens (classificatie en autorisatie) houdt op ad-hoc basis rekening met kennisveiligheidsrisico's.
Herhaalbaar en/of gedefinieerd	De raakvlakken tussen kennisveiligheidsbeleid en cyberveiligheidsbeleid zijn beschreven en bekend bij betrokken medewerkers.
Meetbaar en gemanaged	De afstemming tussen het kennisveiligheidsbeleid en het cyberveiligheidsbeleid wordt periodiek geëvalueerd en verbeterd (indien nodig).
Continue verbetering	De afstemming tussen het kennisveiligheidsbeleid en het cyberbeveiligingsbeleid wordt continu geëvalueerd binnen de instelling en verbeterd (indien nodig) in een cyclisch proces.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

40. Wat is uw inhoudelijke toelichting bij deze scores? *

41. Geldt er voor bepaalde onderzoeksgegevens en documenten een restrictief toegangsbeleid? *

- ◯ Ja*
- ◯ Nee*

41a. Zo ja, hoe wordt deze afweging gemaakt? Op welk niveau gebeurt dit? *

Bovenstaande vraag alleen invullen indien de vraag *"41. Geldt er voor bepaalde onderzoeksgegevens en documenten een restrictief toegangsbeleid?* "is beantwoord met "Ja".

41b. Zo nee, kunt u toelichten waarom niet?*

Bovenstaande vraag alleen invullen indien de vraag *"41. Geldt er voor bepaalde onderzoeksgegevens en documenten een restrictief toegangsbeleid?* "is beantwoord met "Nee".

42. Indien uw instelling met zeer sensitieve gegevens werkt: werkt uw instelling met rubricering van documenten (zoals 'vertrouwelijk' of 'geheim')?*

- ◯ Ja*
- ◯ Nee*
- ◯ N.v.t.*
- ◯ Anders namelijk*

43. Hoe gaat uw instelling om met buitenlandse reisdelegaties die ruimtes met een restrictief toegangsbeleid op uw instelling bezoeken?*

44. Heeft u verder nog opmerkingen of een toelichting ten aanzien van fysieke en digitale beschermingsmaatregelen?

1.7 Internationale partnerschappen

Hieronder vragen we in welke mate uw instelling aan verschillende beleidsmaatregelen ten aanzien van internationale partnerschappen invulling geeft en wat daarbij de overwegingen zijn.

45. Kunt u in onderstaande rubric aangeven waar uw kennisveiligheidsbeleid staat ten aanzien van internationale, geformaliseerde samenwerking op gebied van onderwijs (denk aan trainingen, uitwisselingen en summer schools)?

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen kennisveiligheidsbeleid met betrekking tot internationale samenwerking in het onderwijs.
Initieel/in ontwikkeling	Er wordt gewerkt aan kennisveiligheidsbeleid met betrekking op internationale samenwerking in het onderwijs. Er zijn geen formele regels en/of verantwoordelijkheden.
Herhaalbaar en/of gedefinieerd	De voorbereiding van internationale samenwerkingsovereenkomsten in het onderwijs omvat kennisveiligheidsmaatregelen zoals *due diligence* en exportcontrole. Betrokken medewerkers zijn hiermee bekend.
Meetbaar en gemanaged	Kennisveiligheidsmaatregelen in de procedure voor het voorbereiden van internationale samenwerkingsovereenkomsten rondom onderwijs worden periodiek geëvalueerd en aangepast.
Continue verbetering	De afstemming tussen kennisveiligheidsbeleid en de onderwijs-internationaliseringsstrategie, en de procedures hier rondom, ondergaan een voortdurende evaluatie- en verbeter cyclus.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

46. Wat is uw inhoudelijke toelichting bij deze scores? *

47. Kunt u in onderstaande rubric aangeven waar uw kennisveiligheidsbeleid staat ten aanzien internationale samenwerking (zowel formeel als informeel) op gebied van onderzoek ?*

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen kennisveiligheidsbeleid met betrekking op internationale samenwerking op gebied van onderzoek.
Initieel/in ontwikkeling	Ondersteunend personeel dat betrokken is bij het opstellen van internationale samenwerkingsovereenkomsten op gebied van onderzoek is bekend met kennisveiligheidsrisico's en houden hier rekening mee.
Herhaalbaar en/of gedefinieerd	De procedure voor het voorbereiden van internationale samenwerkingsovereenkomsten op gebied van onderzoek omvat kennisveiligheidsmaatregelen, waaronder *due diligence* en exportcontrole. Medewerkers krijgen verantwoordelijkheden toegewezen voor het implementeren van kennisveiligheidsmaatregelen.
Meetbaar en gemanaged	Kennisveiligheidsmaatregelen in de procedure voor het voorbereiden van internationale samenwerkingsovereenkomsten rondom onderzoek worden periodiek geëvalueerd en aangepast.
Continue verbetering	Kennisveiligheidsmaatregelen in internationale onderzoekssamenwerking worden binnen de instelling voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

48. Wat is uw inhoudelijke toelichting bij deze scores? *

Wij zijn benieuwd hoe uw partneracceptatiebeleid (voor onderwijs en onderzoek) er uitziet. Kunt u dat toelichten aan de hand van onderstaande vragen?

49. Zijn er interne procedures waarbij in het kader van due diligence de achtergrond van een buitenlandse partner of opdrachtgever wordt nagegaan? *

49a. In hoeverre wordt daarbij juridische en veiligheidsexpertise ingeschakeld?*

49b. Wat voor afwegingen worden gemaakt bij het definitief aangaan van de samenwerking? *

49c. Waar ligt de verantwoordelijkheid voor het aangaan van partnerschappen?*

49d. Verschilt dit voor partners op onderwijs- of onderzoeksvlak?*

49e. In het geval dat uw instelling geen partneracceptatiebeleid heeft: hoe is deze afweging gemaakt?*

50. Heeft uw instelling beleid om te voorkomen dat (instituten binnen) uw instelling in een situatie van ongewenste (financiële) afhankelijkheid van statelijke actoren kan worden gebracht?*

- ◯ Ja*
- ◯ Nee*

50a. Zo ja, kunt u dit toelichten? Hoe ziet dit beleid eruit? *

Bovenstaande vraag alleen invullen indien de vraag *"50. Heeft uw instelling beleid om te voorkomen dat {instituten binnen) uw instelling in een situatie van ongewenste {financiële) afhankelijkheid van statelijke actoren kan worden gebracht?"* is beantwoord met ".Ja".

50b. Zo nee, kunt u toelichten waarom niet? *

Bovenstaande vraag alleen invullen indien de vraag *"50. Heeft uw instelling beleid om te voorkomen dat (instituten binnen) uw instelling in een situatie van ongewenste (financiële) afhankelijkheid van statelijke actoren kan worden gebracht?" is* beantwoord met "Nee".

51. Is er een interne procedure om ervoor te zorgen dat lopende samenwerkingen met buitenlandse partners regelmatig worden geëvalueerd en dat overeenkomsten niet stilzwijgend worden verlengd? *

- ◯ Ja*
- ◯ Nee*

51a. Zo ja, hoe ziet deze procedure eruit? *

Bovenstaande vraag alleen invullen indien de vraag *"51. Is er een interne procedure om ervoor te zorgen dat lopende samenwerkingen met buitenlandse partners regelmatig worden geëvalueerd en dat overeenkomsten niet stilzwijgend worden verlengd?* "is beantwoord met “Ja".

51b. Zo nee, waarom heeft uw instelling niet zo'n procedure? *

Bovenstaande vraag alleen invullen indien de vraag *"51. Is er een interne procedure om ervoor te zorgen dat lopende samenwerkingen met buitenlandse partners regelmatig worden geëvalueerd en dat overeenkomsten niet stilzwijgend worden verlengd?* "is beantwoord met "Nee".

52. Heeft u verder nog opmerkingen of een toelichting ten aanzien van internationale partnerschappen?

1.8 Personeelsbeleid

De Leidraad stelt dat het wenselijk is dat veiligheidsbewustzijn onderdeel wordt van het personeelsbeleid. In onderstaande vragen beschrijven we een aantal wijzen waarop dit bewustzijn kan worden geïmplementeerd in beleid om een beeld te krijgen hoe uw instelling hier invulling aan geeft.

53. Kunt u in onderstaande rubric aangeven waar uw kennisveiligheidsbeleid staat ten aanzien van training van medewerkers? *

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen beleid voor de training van personeel en management op gebied van kennisveiligheid.
Initieel/in ontwikkeling	Onderzoekers, management en relevant ondersteunend personeel worden af en toe geïnformeerd over risico's en maatregelen op het gebied van kennisveiligheid.
Herhaalbaar en/of gedefinieerd	Algemene informatie over kennisveiligheid is beschreven en beschikbaar gemaakt en/of er worden (informele) bijeenkomsten of cursussen over kennisveiligheid en relevante maatregelen gegeven.
Meetbaar en gemanaged	De opzet en deelname van bijeenkomsten en cursussen wordt periodiek geëvalueerd en (indien nodig) verbeterd.
Continue verbetering	Het ontwerp en de deelname aan bijeenkomsten en cursussen wordt binnen de instelling geëvalueerd en (indien nodig) verbeterd in cyclische processen.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

54. Wat is uw inhoudelijke toelichting bij deze scores? *

55. In hoeverre voert uw instelling actief beleid om een open veiligheidscultuur te creëren?*

56. Worden er bewustwordingscampagnes rond kennisveiligheid gevoerd? *

- ◯ Ja*
- ◯ Nee*

56a. Zo ja, op welke doelgroepen richten deze campagneactiviteiten zien specifiek? *

Bovenstaande vraag alleen invullen indien de vraag *"56. Worden er bewustwordingscampagnes rond kennisveiligheid gevoerd?* "is beantwoord met ".Ja".

56b. Zo nee, kunt u toelichten waarom niet? *

Bovenstaande vraag alleen invullen indien de vraag *"56. Worden er bewustwordingscampagnes rond kennisveiligheid gevoerd?* "is beantwoord met "Nee".

57. Krijgen (nieuwe} medewerkers informatie en training om hen veiligheidsbewust te maken?*

- ◯ Ja*
- ◯ Nee*

57a. Zo ja, kunt u dit toelichten?*

Bovenstaande vraag alleen invullen indien de vraag *"57. Krijgen (nieuwe) medewerkers informatie en training om hen veiligheidsbewust te maken?" is* beantwoord met ".Ja".

57b. Zo nee, kunt u toelichten waarom niet? *

Bovenstaande vraag alleen invullen indien de vraag *"57. Krijgen (nieuwe) medewerkers informatie en training om hen veiligheidsbewust te maken?" is* beantwoord met "Nee".

58. Zijn er opfrismodules voor zittende medewerkers? *

- Ja*
- Nee*

58a. Zo ja, kunt u dit toelichten?*

Bovenstaande vraag alleen invullen indien de vraag *"58. Zijn er opfrismodules voor zittende medewerkers?* "is beantwoord met “Ja".

58b. Zo nee, kunt u toelichten waarom niet? *

Bovenstaande vraag alleen invullen indien de vraag *"58. Zijn er opfrismodules voor zittende medewerkers?* "is beantwoord met "Nee".

59. Zijn er speciale trainingsprogramma's gericht op academische kernwaarden voor gastonderzoekers uit landen met een verhoogd risicoprofiel?*

- Ja*
- Nee*

59a. Zo ja, kunt u dit toelichten?*

Bovenstaande vraag alleen invullen indien de vraag *"59. Zijn er speciale trainingsprogramma's gericht op academische kernwaarden voor gastonderzoekers uit landen met een verhoogd risicoprofiel?"* is beantwoord met “Ja".

59b. Zo nee, kunt u toelichten waarom niet? *

Bovenstaande vraag alleen invullen indien de vraag *"59. Zijn er speciale trainingsprogramma's gericht op academische kernwaarden voor gastonderzoekers uit landen met een verhoogd risicoprofiel?"* is beantwoord met "Nee".

60. Kunt u in onderstaande rubric aangeven wat de relatie is tussen uw kennisveiligheidsbeleid en uw beleid ten aanzien van werving van medewerkers?*

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen beleid rond kennisveiligheid bij de werving van personeel.
Initieel/in ontwikkeling	(Opleidings-)Managers, vakgroepleiders, HR-medewerkers en ander relevant personeel is bekend met kennisveiligheidsrisico's en nemen dit mee in het wervingsproces. Er zijn geen formele regels en/of verantwoordelijkheden.
Herhaalbaar en/of gedefinieerd	Het wervingsproces omvat kennisveiligheidsmaatregelen zoals achtergrondonderzoeken, en HR-medewerkers zijn hiermee bekend. Risicovolle functies vereisen strengere achtergrondonderzoeken.
Meetbaar en gemanaged	Er is een periodieke evaluatie en verbetering van kennisveiligheidsmaatregelen binnen het wervingsproces.
Continue verbetering	Kennisveiligheidsmaatregelen binnen het wervingsproces ondergaan een voortdurende evaluatie- en verbeter cyclus.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0
Welk niveau heeft uw instelling nu?	0	0	0	0	0

61. Wat is uw inhoudelijke toelichting bij deze scores? *

62. Worden bij de werving en selectie van nieuwe medewerkers veiligheidsrisico's meegewogen? Zo ja, hoe? *

1s er bijvoorbeeld een interne procedure om potentiële risico's bij kandidaten tijdig te onderkennen?

63. Hoe wordt er binnen uw instelling voor gezorgd dat HR-medewerkers veiligheidsbewust zijn (en in staat zijn om signalen die wijzen op een verhoogd risico op te pikken)?*

64. Kunt u in onderstaande rubric aangeven waar uw kennisveiligheidsbeleid staat ten aanzien van buitenlandse dienstreizen? *

Onderstaande tabel geeft de omschrijving per niveau die in deze meting wordt aangehouden voor dit onderwerp.

Niveau	Omschrijving
Geen beleid	Er is geen beleid m.b.t. kennisveiligheidsrisiso's tijdens dienstreizen.
Initieel/in ontwikkeling	Onderzoekers en medewerkers die landen of bijeenkomsten met een verhoogd risicoprofiel bezoeken, beoordelen zelf de risico's en maatregelen voor kennisveiligheid.
Herhaalbaar en/of gedefinieerd	Een protocol voor dienstreizen voor dienstreizen naar landen of bijeenkomsten met een verhoogd risicoprofiel is beschreven.
Meetbaar en gemanaged	Het protocol voor dienstreizen naar landen of bijeenkomsten met een hoog risicoprofiel wordt regelmatig geëvalueerd en (indien nodig) verbeterd.
Continue verbetering	Het (gebruik van het) protocol voor zakenreizen naar landen of bijeenkomsten met een hoog risicoprofiel wordt voortdurend geëvalueerd binnen de instelling en verbeterd (indien nodig) in een cyclisch proces.

	Geen beleid	Initieel/in ontwikkeling	Herhaalbaar en/of gedefinieerd	Meetbaar en gemanaged	Continue verbetering
Welk niveau heeft uw instelling nu?	0	0	0	0	0
Welk ontwikkelingsniveau acht u wenselijk gezien het risicoprofiel van uw instelling?	0	0	0	0	0

65. Wat is uw inhoudelijke toelichting bij deze scores? *

66. Beschikt uw instelling over een specifiek beleid voor dienstreizen naar landen met een verhoogd risicoprofiel? Zo ja, kunt u dit kort beschrijven?*

67. Is er specifiek aandacht en/of beleid voor aantasting van sociale veiligheid die voortvloeit uit (heimelijke) beïnvloeding door statelijke actoren? *

Bijvoorbeeld: medewerkers afkomstig uit China die onder druk of invloed staan van de Chinese overheid.

- Ja*
- Nee*

67a. Zo ja, kunt u (in algemene termen) beschrijven hoe uw instelling hiermee omgaat en waar medewerkers terecht-kunnen als zij hiermee te maken krijgen?*

Bovenstaande vraag alleen invullen indien de vraag *"67. /s er specifiek aandacht en/of beleid voor aantasting van sociale veiligheid die voortvloeit uit (heimelijke) beïnvloeding door statelijke actoren?* "is beantwoord met ':.Ja".

67b. Zo ja, kunt u benoemen waar de instelling (mogelijk) tegenaanloopt bij het ontwikkelen van het beleid? *

Bovenstaande vraag alleen invullen indien de vraag *"67. Is er specifiek aandacht en/of beleid voor aantasting van sociale veiligheid die voortvloeit uit (heimelijke) beïnvloeding door statelijke actoren?* "is beantwoord met ':.Ja".

67c. Zo nee, kunt u toelichten waarom niet?*

Bovenstaande vraag alleen invullen indien de vraag *"67. /s er specifiek aandacht en/of beleid voor aantasting van sociale veiligheid die voortvloeit uit (heimelijke) beïnvloeding door statelijke actoren?* "is beantwoord met "Nee".

68. Heeft u verder nog opmerkingen of een toelichting ten aanzien van personeelsbeleid?

1.9 Doorontwikkeling

Kennisveiligheid is een relatief nieuw onderwerp dat nog sterk in ontwikkeling is. Met onderstaande vragen kunt u dit perspectief voor uw instelling schetsen.

69. Zijn er onderdelen van uw kennisveiligheidsbeleid die hierboven niet aan bod zijn gekomen? Zo ja, dan kunt u deze hier kort noemen.*

70. Wat zijn de belangrijkste dilemma's en vraagstukken voor uw instelling bij het vormgeven van kennisveiligheidsbeleid?*

71. Heeft uw instelling voor het komend jaar voornemens voor het (door)ontwikkelen van kennisveiligheidsbeleid in uw instelling? Zo ja, welke voornemens zijn dat?*

1.10 Reflectie op de vervolgmeting

1.10 Reflectie op vervolgmeting

72. Heeft de instelling gebruik gemaakt van het UNL volwassenheidsmodel om deze vragen te beantwoorden?*

73. In hoeverre vind u deze vervolgmeting een geschikte manier om de stand van kennisveiligheidsbeleid te onderzoeken? *

Wat ziet u als voor- en nadelen van de gekozen methode?

74. Welk advies zou u aan OCW willen meegeven als het gaat om kennisveiligheidsbeleid monitoren in de toekomst?

Afsluiting

We danken u zeer voor uw medewerking aan dit onderzoek. Als u de vragenlijst definitief hebt afgerond, kunt u deze versturen via onderstaande knop.

Bij vragen kunt u contact opnemen met uw contactpersoon zoals genoemd in het begin van deze vragenlijst.

dialogic

Onderzoek voor *onderbouwd* beleid.

Dialogic innovatie & interactie
Hooghiemstraplein 33
3514 AX Utrecht
030-2150580
www.dialogic.nl