Volwassenheids Model

Kennisveiligheid

19 april 2024

Universiteiten *van* Nederland

Colofon

Dit is een uitgave van
Universiteiten van Nederland
Postbus 13739
2501 ES Den Haag

www.universiteitenvannederland.nl

Vormgeving: Haagsblauw

Inhoudsopgave

Inleiding

Ondanks dat kennisveiligheid een relatief nieuw aandachtspunt is met een nationale aanpak die eind 2020 werd gepresenteerd, wordt het erkend als een relevant uitdaging voor de Nederlandse (en Europese) wetenschappelijke gemeenschap. Dit vereist het formuleren van nieuwe beleids-maatregelen die zowel precies als proportioneel zijn, zodat het Nederlandse wetenschappelijke systeem kan blijven functioneren volgens het uitgangspunt 'open waar mogelijk, beschermen waar nodig'.[1]

In januari 2022 publiceerde de Nederlandse overheid de Nationale Leidraad Kennisveiligheid (hierna: de Leidraad), met input van UNL, VH, NWO, KNAW, NFU en de TO2-federatie.[2] De Leidraad schetst de definitie en relevantie van kennisveiligheid, en legt de belangrijkste rollen, overwegingen en praktijken uit bij het opstellen van dergelijk beleid. De Nederlandse universiteiten/UNL hebben het initiatief genomen om een volwassenheidsmodel (ook wel 'Capability Maturity Model' of 'CMM') te ontwikkelen.

Het volwassenheidsmodel is binnen het samenwerkingsverband van Universiteiten van Nederland (UNL) door de universiteiten zelf ontwikkeld als instrument met als doelen:

a. ondersteuning van universiteiten bij het ontwerpen en implementeren van hun kennisveiligheidsbeleid;
b. intern beoordelen van het volwassenheidsniveau voor elk specifiek onderwerp en het gewenste volwassenheidsniveau;
c. het mogelijk maken van een interne strategie en planning naar het gewenste volwassenheidsniveau, en
d. verdere verbetering van de afstemming van kennisveiligheidsbeleid van universiteiten wat betreft de gebruikte concepten en het bieden van een overzicht van onderwerpen.

Het model is expliciet niet ontworpen als een instrument voor externe audits van kennisveiligheidsbeleid. Dergelijke audits zouden een andere invulling van de volwassenheidsniveaus vereisen, die zich meer richten op specifieke eisen met betrekking tot de inhoud van kennisveiligheidsbeleid. Dit specifieke aspect is niet opgenomen in dit model, het richt zich op het beleidsproces in plaats van de beleids-inhoud. Deze inleiding geeft een beknopt overzicht van hoe het model kan worden gebruikt. De tabel op de volgende pagina geeft een overzicht van de volwassenheidsniveaus.

Zoals de Leidraad adviseert, is het belangrijk om rekening te houden met de diversiteit en verschillen in risicoprofielen tussen instellingen. Bij het gebruik van het model is het belangrijk om voor de eigen universiteit per gebied te beoordelen welk niveau wenselijk is. Het model zelf schrijft niet voor wat het optimale niveau is voor een universiteit. Om deze reden moeten de volgende overwegingen in acht worden genomen bij het scoren van het volwassenheidsmodel:

- Het benodigde volwassenheidsniveau hangt af van het *risicoprofiel van de instelling*. Dit volwassenheids-model is bedoeld om interne discussies over de gewenste volwassenheidsniveaus te ondersteunen. Het uitvoeren van een interne risicoanalyse om het risicoprofiel te beoordelen kan helpen om dit te bepalen.
- De niveaus zijn op een algemeen niveau gedefinieerd. Dit impliceert dat gebruikers van het model moeten overwegen *hoe de niveaus kunnen worden geoperationaliseerd om bij hun individuele context te passen*. Het is mogelijk om gedeeltelijk aan de kenmerken van een bepaald niveau te voldoen. In een dergelijk geval kunt u uw instelling beoordelen als tussen twee niveaus.

1 Kamerbrief over maatregelen kennisveiligheid hoger onderwijs en wetenschap | Kamerstuk | Rijksoverheid.nl
2 Nationale leidraad kennisveiligheid - Veilig internationaal samenwerken | Rapport | Rijksoverheid.nl

Level	Label	Eigenschappen
1	**Initieel**	Maatregelen zijn niet of slechts gedeeltelijk gedefinieerd en/of worden uitgevoerd op een inconsistente manier en zijn sterk afhankelijk van individuen.
2	**Herhaalbaar**	Maatregelen zijn aanwezig en worden uitgevoerd op een gestructureerde en consistente, maar informele, manier.
3	**Gedefinieerd**	Maatregelen zijn gedocumenteerd en worden uitgevoerd op een gestructureerde en formele manier. De uitvoering van maatregelen kan worden aangetoond, wordt getest en is effectief. Periodieke rapportages (bijvoorbeeld in jaarverslagen of tijdens vergaderingen) levert input voor strategische beslissingen met betrekking tot kennisveiligheid.
4	**Meetbaar en gemanaged**	De effectiviteit van maatregelen wordt periodiek beoordeeld door de universiteit en indien nodig verbeterd. Dit wordt gedocumenteerd. Periodieke evaluaties (bijvoorbeeld in jaarverslagen of tijdens vergaderingen) rapporteren over de effectiviteit van het beleid en de implementatie van kennisveiligheid.
5	**Continue verbetering**	Een universiteitsbreed kennisveiligheidsprogramma biedt continue en effectieve strategische controle en behandeling van risico's, bijvoorbeeld via een PDCA-cyclus.

- *Periodieke rapportages* op niveaus 3 en 4 zijn een middel om te zorgen dat het management en andere belanghebbenden geïnformeerd blijven. Deze rapportages kunnen op verschillende manieren worden uitgevoerd, zoals rapportages tijdens vergaderingen, workshops, bijeenkomsten, (jaar)verslagen, infographics of dashboards. De verschillende onderwerpen van het volwassenheidsmodel kunnen tegelijkertijd worden gerapporteerd en impliceren geen aparte rapportagemechanismen per gebied.
- *Evaluatie en verbetering* op niveaus 4 en 5 zijn noodzakelijk voor een lerende aanpak.
  Net als bij periodieke rapportages kan het format voor dergelijke evaluaties divers zijn, variërend van een presentatie gevolgd door discussie en rapportage van deze discussie, tot een evaluatie die is gebaseerd op een reeks interviews of enquêtes.

Dit volwassenheidsmodel volgt de hoofdstukken van de Leidraad. Het recht om het model te wijzigen is uitsluitend voorbehouden aan UNL.

1. Bescherming van academische waarden

De Leidraad vat de adviezen in relatie tot academische waarden als volgt samen:

- Academische kernwaarden zoals **academische vrijheid** en **wetenschappelijke integriteit** vormen het fundament van hoger onderwijs en wetenschap in Nederland.
- Ook bij **activiteiten met buitenlandse partners** zijn de academische kernwaarden richtinggevend. Ze bieden houvast bij het aangaan van buitenlandse samenwerkingen. Buitenlandse **(gast)onderzoekers en docenten** dienen, net als hun Nederlandse collega's, de gedragscode te onderschrijven en na te leven.

Academische kernwaarden

Onderwerp	Bescherming van academische waarden
Omschrijving	Academische kernwaarden, zoals academische vrijheid en wetenschappelijke integriteit
Ambitie	Kennisveiligheidsmaatregelen zijn in balans met academische kernwaarden, zoals academische vrijheid en wetenschappelijke integriteit. Door academische waarden op te nemen in de kernwaarden van de universiteit geeft de universiteit uiting aan haar betrokkenheid en geeft ze richting.
1 Initieel	• Individuele medewerkers refereren ad hoc aan de balans tussen academische kernwaarden en kennisveiligheidsmaatregelen.
2 Herhaalbaar	• Betrokken medewerkers hebben (deels) enkele situaties beschreven waarin kennisveiligheidsmaatregelen een effect kunnen hebben op academische kernwaarden of vice versa.
3 Gedefinieerd	• De academische kernwaarden bieden extra houvast voor het betrokken personeel bij de implementatie van het beleid voor kennisveiligheid. • Complexe dilemma's waarbij kennisveiligheidsmaatregelen de academische kernwaarden kunnen beïnvloeden (of vice versa), worden besproken met het betrokken personeel.
4 Meetbaar en gemanaged	• De universiteit evalueert periodiek of haar kennisveiligheidsmaatregelen in balans zijn met de kernwaarden en verbetert haar maatregelen op basis van deze evaluatie. • 'Best practices' over kennisveiligheid in relatie tot de kernwaarden worden gedocumenteerd en gecommuniceerd.
5 Continue verbetering	• Complexe dilemma's (niveau 3) en best practices (niveau 4) leveren input voor training en bewustwordingsactiviteiten om een lerende aanpak en voortdurende verbetering te stimuleren. • De afstemming tussen kennisveiligheidsmaatregelen en kernwaarden wordt in een cyclisch proces geëvalueerd en (indien nodig) verbeterd.
Bron/referentie	Nationale Leidraad Kennisveiligheid (2022), Tackling R&I foreign interference (2022)

Open Science

De Leidraad vat de adviezen in relatie tot open science als volgt samen:

- **Open science** is binnen Europa de norm: het streven is om publiek gefinancierde onderzoeksresultaten voor iedereen toegankelijk te maken. Er kunnen echter legitieme redenen zijn om van openbaarmaking af te zien, zoals het beschermen van de **nationale veiligheid**. Maak vooraf goede afspraken om spanning tussen het streven naar maximale openheid en het treffen van legitieme beschermende maatregelen te voorkomen.

Onderwerp	Bescherming van academische waarden
Omschrijving	Open Science
Ambitie	Open Science en kennisveiligheid zijn op elkaar afgestemd en het personeel is toegerust om ervoor te zorgen dat onderzoek zo open als mogelijk is, en zo gesloten als nodig.
1 Initieel	• Sommige trekkers van Open Science, data stewards en andere relevante medewerkers zijn zich bewust van kennisveiligheidsrisico's in relatie tot open science praktijken. • Trekkers van Open Science, data stewards en andere relevante medewerkers hebben op ad-hoc basis informeel contact met kennisveiligheidsmedewerkers.
2 Herhaalbaar	• Open Science beleid en procedures beschrijven zowel de ambitie om zo open mogelijk te zijn, en om zo gesloten te zijn als nodig is. • Trekkers van Open Science, data stewards en ander relevant personeel zijn bekend met procedures en tools die gebruikt kunnen worden voor de bescherming van gegevens.
3 Gedefinieerd	• Procedures voor Open Science (zoals data management plannen) verwijzen naar kennisveiligheid, waar en wanneer dat relevant is. • Procedures voor kennisveiligheid verwijzen naar Open Science, waar en wanneer dat relevant is.
4 Meetbaar en gemanaged	• Er is technische, juridische en/of administratieve ondersteuning beschikbaar om de bescherming van gegevens en onderzoeksresultaten mogelijk te maken. • De balans tussen kennisveiligheid en Open Science wordt periodiek geëvalueerd, gerapporteerd en verbeterd (indien nodig). • Best practices met betrekking tot 'zo open als mogelijk, zo gesloten als nodig' worden gedocumenteerd en gecommuniceerd.
5 Continue verbetering	• De afstemming tussen kennisveiligheidsbeleid en Open Science procedures wordt in een cyclisch proces geëvalueerd, gerapporteerd en (indien nodig) verbeterd. • Best practices (van niveau 4) worden opgenomen in trainings- en bewustwordingsactiviteiten om een lerende aanpak voor voortdurende verbetering aan te moedigen.
Bron/referentie	Tackling R&I Foreign Interference (2021), hoofdstuk 1.5

Ethiek

De Leidraad vat de adviezen in relatie tot ethiek als volgt samen:

- **Ethische dilemma's** kunnen een rol spelen wanneer wordt samengewerkt met landen die de grondrechten niet respecteren. Hoe kan voorkomen worden dat onderzoeksresultaten daar worden gebruikt voor onderdrukking of schending van mensenrechten? Het is raadzaam om binnen uw instelling een **ethische commissie** te hebben die kan adviseren over ethisch gebruik van onderzoeksresultaten.

Onderwerp	Bescherming van academische waarden
Omschrijving	Ethiek
Ambitie	Reguliere ethische toetsing van onderzoek wordt afgestemd met kennisveiligheidrisico's, met name andere ethische kwesties dan wetenschappelijke integriteit.
1 Initieel	• Ethische commissies van universiteiten zijn zich ervan bewust dat er andere ethische kwesties kunnen ontstaan dan wetenschappelijke integriteit.
2 Herhaalbaar	• De ethische beoordelingen omvatten soms ook andere ethische dilemma's dan wetenschappelijke integriteit.
3 Gedefinieerd	• Het ethisch beleid maakt het mogelijk om andere ethische dilemma's dan wetenschappelijke integriteit te beoordelen. • De respectieve rollen van ethische commissie(s) en kennisveiligheidsmedewerkers worden besproken en wederzijds afgestemd.
4 Meetbaar en gemanaged	• De afstemming tussen kennisveiligheidsprocedures en de ethische toetsingsprocedures wordt periodiek geëvalueerd en (indien nodig) verbeterd. • Periodieke rapportage aan het hoger management omvat een evaluatie van de afstemming van kennisveiligheidsprocedures en ethische toetsingsprocedures.
5 Continue verbetering	• De afstemming tussen kennisveiligheid en ethische toetsingsprocedures wordt voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces. • Andere ethische dilemma's dan wetenschappelijke integriteit worden meegenomen in training en bewustwordingsactiviteiten.
Bron/referentie	Nationale Leidraad Kennisveiligheid (2022)

Inclusiviteit en non-discriminatie

- Vooral in een onderwerp als kennisveiligheid, waarbij dreigingsanalyses en risicoprofielen een belangrijke rol spelen, bestaat het gevaar dat de benadering 'te ver gaat' en leidt tot vormen van willekeurige uitsluiting, verdachtmaking en discriminatie. Dit moet ten alle tijde worden vermeden.
- Voer binnen uw instelling een open gesprek hierover en neem signalen hierover altijd serieus.
- Om uitsluiting, stigmatisering en discriminatie met betrekking tot kennisveiligheid te vermijden, zie het rapport *Tackling R&I foreign interference* (Europese Commissie, 2021).

Onderwerp	Bescherming van academische waarden
Omschrijving	Inclusiviteit en non-discriminatie
Ambitie	Maatregelen voor kennisveiligheid en exportcontrole zijn ontworpen om inclusiviteit en non-discriminatie te garanderen.
1 Initieel	• Kennisveiligheidsmedewerkers zijn zich ervan bewust dat er negatieve effecten van kennisveiligheidsmaatregelen kunnen optreden, zoals uitsluiting, stigmatisering of discriminatie.
2 Herhaalbaar	• Kennisveiligheidsmedewerkers hebben (gedeeltelijk) de risico's van uitsluiting, stigmatisering en discriminatie als gevolg van kennisveiligheidsmaatregelen beschreven en hoe deze risico's kunnen worden beperkt.
3 Gedefinieerd	• In het beleid voor kennisveiligheid zijn expliciet principes opgenomen om inclusiviteit en non-discriminatie te garanderen.
4 Meetbaar en gemanaged	• De universiteit evalueert periodiek of kennisveiligheidsmaatregelen kunnen leiden tot uitsluiting, stigmatisering of discriminatie en hoe dit te mitigeren. • Periodieke rapportages aan het hoger management over kennisveiligheid bevatten illustraties van uitsluiting of discriminatie indien en wanneer deze zich hebben voorgedaan.
5 Continue verbetering	• Wanneer er inderdaad maatregelen werden genomen om dergelijke effecten te verzachten, worden deze in een cyclisch proces geëvalueerd en (indien nodig) verbeterd. • Illustraties van discriminatie, stigmatisering en uitsluiting - en verzachtende maatregelen - worden opgenomen in opleidings- en bewustmakingsactiviteiten.
Bron/referentie	Oberon & Dialogic (2023). Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek. Sectorbeeld universiteiten. Rijksoverheid.

2. Bestuur en beleidskader

Hoewel sommige elementen van risicobeheer en de processen zijn opgenomen onder de titel 'risicobeheer' in de Leidraad, worden 'governance en beleidsimplementatie' niet apart behandeld in een afzonderlijk hoofdstuk. Gezien het belang ervan, wordt dit hier behandeld als een apart hoofdstuk, in lijn met de aanbevelingen uit het VSNU Kader Kennisveiligheid en de aanbevelingen van de EU (2021/1700).

Bestuur, verantwoordelijkheden en processen

De Leidraad vat de adviezen in relatie tot bestuur en beleidskaders als volgt samen:

- Het is raadzaam een aantal **standaardprocessen centraal in te regelen**. Afhankelijk van het risiconiveau zijn de benodigde risicoanalyses en controles strikter en ligt de beslisbevoegdheid op een hoger, centraler niveau.
- Het begint met het aanwijzen van een **portefeuillehouder op bestuurlijk niveau** en het instellen van een **Adviesteam Kennisveiligheid** van enkele deskundigen met relevante expertises om de portefeuillehouder bij te staan.

Onderwerp	Bestuur en beleidskader
Omschrijving	Bestuur, verantwoordelijkheden en processen
Ambitie	Verantwoordelijkheden voor kennisveiligheid zijn toegewezen aan rollen en niveaus binnen de universiteit op centraal en/of facultair niveau.
1 Initieel	• Sommige medewerkers van de universiteit houden zich op ad hoc en informele basis bezig met kennisveiligheid.
2 Herhaalbaar	• Betrokkenheid bij kennisveiligheid verspreid over verschillende rollen en niveaus is gedeeltelijk beschreven en wordt informeel uitgevoerd.
3 Gedefinieerd	• Het College van Bestuur heeft een portefeuillehouder kennisveiligheid aangesteld. • Er is formeel een Adviesteam Kennisveiligheid (of programmateam kennisveiligheid) ingesteld. • Verantwoordelijkheden zijn toegewezen aan rollen en niveaus en zijn gedocumenteerd.
4 Meetbaar en gemanaged	• De verdeling van taken en verantwoordelijkheden wordt periodiek geëvalueerd, gerapporteerd en indien nodig verbeterd. • De samenstelling en het functioneren van het Adviesteam Kennisveiligheid wordt periodiek geëvalueerd, gerapporteerd en waar nodig aangepast.
5 Continue verbetering	• De verdeling van taken en verantwoordelijkheden over rollen en niveaus en het functioneren en de samenstelling van het Adviesteam Kennisveiligheid wordt voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.
Bron/referentie	Nationale Leidraad Kennisveiligheid (2022), hoofdstuk 6

Beleid

Onderwerp	Bestuur en beleidskader
Omschrijving	Beleid
Ambitie	• Beleid, projecten en activiteiten op het gebied van kennisveiligheid zijn gebaseerd op de Nationale Leidraad Kennisveiligheid en andere relevante documenten.
1 Initieel	• Relevant personeel voert kennisveiligheidsactiviteiten op ad-hoc basis uit. • Er zijn enkele beleidsverklaringen voor kennisveiligheid opgesteld.
2 Herhaalbaar	• Activiteiten en processen met betrekking tot kennisveiligheid zijn gedeeltelijk beschreven en worden informeel uitgevoerd door medewerkers die betrokken zijn bij kennisveiligheid.
3 Gedefinieerd	• De universiteit heeft een kennisveiligheidsbeleid dat is goedgekeurd door het hoger management. Stakeholders worden geïnformeerd over relevante aspecten van het kennisveiligheidsbeleid. • Periodieke rapportages aan het hoger management bevatten een beschrijving van kennisveiligheidsactiviteiten en -processen.
4 Meetbaar en gemanaged	• Het kennisveiligheidsbeleid wordt periodiek geëvalueerd en bijgesteld. • Periodieke rapportage aan het hoger management omvat een evaluatie van kennisveiligheidsactiviteiten en –processen.
5 Continue verbetering	• Het kennisveiligheidsbeleid van de universiteit wordt voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.
Bron/referentie	

Implementatieprogramma

Onderwerp	Bestuur en beleidskader
Omschrijving	Implementatieprogramma
Ambitie	Het kennisveiligheidsbeleid wordt vertaald naar een implementatieprogramma of intern compliance programma met standaard operationele procedures. Betrokken medewerkers beschikken over voldoende expertise voor het implementeren en uitvoeren van kennisveiligheidsmaatregelen.
1 Initieel	• Medewerkers die betrokken zijn bij kennisveiligheidsprocedures voeren het kennisveiligheidsbeleid op ad-hoc basis uit. • Er zijn geen formele regels voor naleving of verantwoordelijkheden.
2 Herhaalbaar	• Sommige elementen van een implementatieprogramma zijn (gedeeltelijk) beschreven en worden informeel uitgevoerd door personeel dat betrokken is bij kennisveiligheid. • Alleen voor sommige aspecten van kennisveiligheid zijn de verantwoordelijkheden geformaliseerd.
3 Gedefinieerd	• Het implementatieprogramma is goedgekeurd door het hoger management en verantwoordelijkheden zijn toegewezen. • Betrokken medewerkers beschikken over voldoende expertise voor hun rol en verantwoordelijkheid bij de implementatie. • Periodieke rapportage aan het hoger management bevat een beschrijving van de voortgang van de implementatie.
4 Meetbaar en gemanaged	• Het implementatieprogramma en de voortgang worden periodiek geëvalueerd en bijgesteld. • De periodieke rapportage aan het hoger management omvat een evaluatie van het implementatieprogramma.
5 Continue verbetering	• Het implementatieprogramma wordt voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces. • De expertise van betrokken medewerkers die nodig is voor de implementatie wordt periodiek beoordeeld binnen de universiteit en, indien nodig, wordt aanvullende training verzorgd.
Bron/referentie	Commission Recommendation (EU) 2021/1700

3. Wettelijke kaders voor sancties en exportcontrole

De Leidraad vat de adviezen in relatie tot wettelijke kaders voor sancties en exportcontrole als volgt samen:[3]

- Er is wet- en regelgeving om de dreigingen het hoofd te bieden, waaraan uw instelling dient te voldoen (*compliance*). Zo gelden er binnen de Europese Unie strenge regels voor de uitvoer van **dual-use producten en technologie** die naast civiele ook militaire toepassingen hebben. Het gaat om alle vormen van overdracht, dus **ook via e-mail of een clouddienst**. Zuiver fundamenteel wetenschappelijk onderzoek en technologie die zich reeds in het publieke domein bevinden zijn uitgezonderd van exportcontrole. Twijfelt u of de exportregels van toepassing zijn, dan kunt u een indelingsverzoek doen bij de **Centrale Dienst voor In- en Uitvoer** (CDIU).
- Daarnaast zijn er **internationale sanctieregimes** van kracht tegen landen, organisaties en personen. Het actuele overzicht is te vinden op www.sanctionsmap.eu. De sancties tegen **Noord-Korea** en **Iran** zijn voor kennisinstellingen in het bijzonder relevant: deze vormen de basis voor het **verscherpt toezicht** dat voor een beperkt aantal vakgebieden geldt.

De Commission Recommendation (EU) 2021/1700 van 15 September 2021[4] betreffende interne nalevingsprogramma's voor controles op onderzoek met dual-use goederen onder Verordening (EU) 2021/821 heeft tot doel universiteiten en onderzoeksorganisaties te ondersteunen bij de interpretatie en implementatie van de Dual Use Verordening 2021/821.

De noodzaak van een apart programma / expertise op het gebied van exportcontrole hangt af van de aard van de universiteit, het internationale karakter van de universiteit en of de universiteit al dan niet een technische universiteit is, een algemene universiteit met een of meer technische afdelingen of een universiteit zonder onderzoeksgebieden die onder de dual-use-regelgeving vallen.

3 Andere relevante kaders, niet genoemd door de Leidraad, zijn: kennisembargo in relatie tot de EU - Iran Sanctieverordening 267/2012 en de Sanctieregeling Noord-Korea 2017. Wet Veiligheidstoets Investeringen, Fusies en Overnames (18 mei 2022); Regeling geavanceerde productieapparatuur voor halfgeleiders (MinBuza.2023.15246-27, 23 juni 2023), European Chips Act 2023, Wet screening kennisveiligheid (in voorbereideing). Andere relevante wetgeving zijn de GDPR and the EU Charter of Fundamental Rights, art. 21 over non-discriminatie and de EU Conventie over Mensenrechten. Het wordt verwacht dat het Europese regelgevingskader wordt uitgebreid gezien het pakket initiatieven onder de EU-economische veiligheidsstrategie (24 January 2024).

4 Commission Recommendation (EU) 2021/1700 van 15 September 2021

Juridische kaders

Onderwerp	Wettelijke kaders voor sancties en exportcontrole
Omschrijving	Juridische kaders
Ambitie	Er zijn processen en procedures voor naleving van sancties, exportcontrole en andere relevante regelgeving.
1 Initieel	• Er is geen structureel bewustzijn van wet- en regelgeving over sancties en exportcontrole die van toepassing zijn op internationale samenwerking of op het werven of ontvangen van internationale studenten, medewerkers of gastonderzoekers. • Medewerkers identificeren de relevantie van wettelijke kaders op een ad-hoc basis.
2 Herhaalbaar	• Er is enig bewustzijn van wet- en regelgeving op het gebied van sancties en exportcontrole die van toepassing zijn op internationale samenwerking. • Relevant personeel, zoals juridische adviseurs, kennisveiligheidsmedewerkers of contractfunctionarissen, hebben een manier van werken ontwikkeld om aan deze regels te voldoen en communiceren dit per geval aan relevante medewerkers of onderzoeksgroepen.
3 Gedefinieerd	• De universiteit heeft een uitgebreide reeks maatregelen ontwikkeld voor de interne naleving van sancties en exportcontrole. Aan het personeel zijn verantwoordelijkheden toegewezen om naleving te waarborgen. • Periodieke rapportage aan het hoger management bevat verwijzingen naar relevante wettelijke kaders en maatregelen voor naleving.
4 Meetbaar en gemanaged	• De universiteit evalueert periodiek de procedures om naleving van wettelijke kaders te waarborgen en verbetert deze indien nodig. • Periodieke rapportage omvat dilemma's en/of best practices met betrekking tot (niet-)naleving.
5 Continue verbetering	• De naleving van screening, sancties en exportcontrole wordt voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces. • Opleidings- en bewustmakingsactiviteiten omvatten een verduidelijking van de processen en procedures om sancties en/of exportcontrole na te leven.
Bron/referentie	Nationale Leidraad Kennisveiligheid (2022), hoofdstuk 4

4. Het inschatten van risico's

De Leidraad vat de adviezen in relatie tot het inschatten van risico's als volgt samen:

- Het is belangrijk om **sensitieve kennisgebieden** binnen uw instelling nauwkeurig te identificeren. Denk aan dual-use technologieën en kennis die onethisch ingezet kan worden. Breng ook uw '**kroon-juwelen**' in kaart; de gebieden waarop er risico's verbonden zijn aan kennisoverdracht en uw instelling internationaal toonaangevend is. Voer voor elk sensitief kennisgebied een korte risicoanalyse uit.
- Om een inschatting te maken van het **risicoprofiel van een land**, kunt u gebruik maken van openbare dreigingsinformatie, zoals het Dreigingsbeeld Statelijke Actoren van NCTV, AIVD en MIVD. Daarnaast kunt u internationale ranglijsten raadplegen: een slechte score op rankings over academische vrijheid en respect voor de rechtsstaat moet alarmbellen doen afgaan. Een slechte score betekent niet noodzakelijkerwijs dat u niet met instellingen uit dat land kunt samenwerken, wel moet u dan goede voorzorgsmaatregelen treffen.
- Vervolgens is het van belang dat u zich in het kader van **due diligence** verdiept in de achtergrond van de buitenlandse partner of opdrachtgever.

Risicoanalyse en Risicomanagement zijn ook een onderdeel van het SURFaudit Toetsingskader.
Het toetsingskader verschilt echter van de Leidraad wat betreft inhoud en concepten.
Voor de ontwikkeling van het volwassenheidsmodel is uitgegaan van de Leidraad.

Toetsingskader kennisveiligheidsrisico's

Onderwerp	Risicoanalyse
Omschrijving	Toetsingskader kennisveiligheidsrisico's
Ambitie	Risico's voor kennisveiligheid worden geïdentificeerd voor interne doeleinden om actuele risicoprofielen te bepalen, en relevante onderzoekers en het management krijgen ondersteuning en advies over maatregelen voor kennisveiligheid.
1 Initieel	• Er is geen formele risicobeoordeling die voorschrijft in welke gevallen ondersteuning en advies op het gebied van kennisveiligheid nodig is. • Relevante medewerkers identificeren kennisveiligheidsrisico's op ad-hoc basis.
2 Herhaalbaar	• Relevante risico's voor kennisveiligheid en bijbehorende adviezen worden gecommuniceerd naar het relevante personeel. De communicatie bevat een argumentatie om te verduidelijken welke elementen relevant zijn geweest bij het opstellen van het advies.
3 Gedefinieerd	• Er is een risicobeoordelingsprocedure en toetsingskader gedefinieerd. Due diligence maakt deel uit van deze risicobeoordelingsmethodologie. • In de periodieke rapportage aan het hoger management is beschreven hoe de risicobeoordelingsmethodologie de informatie oplevert die nodig is om het advies op te stellen.
4 Meetbaar en gemanaged	• De universiteit evalueert periodiek de risicobeoordelingsmethodologie en verbetert deze indien nodig. • De periodieke rapportage aan het hoger management omvat een evaluatie van de ervaringen met de risicobeoordelingsmethodologie.
5 Continue verbetering	• Ondersteuning en advies voor onderzoekers, ondersteunend personeel en managers is aanwezig en wordt continu geëvalueerd en verbeterd (indien nodig) in een cyclisch proces. • De risicobeoordelingsmethodologie wordt uitgelegd in opleidings- en bewustmakingsactiviteiten.
Bron/referentie	VSNU Kader Kennisveiligheid, hoofdstuk 4; Nationale Leidraad Kennisveiligheid (2022), hoofdstuk 5

Kwetsbaarheid van onderzoeksfaciliteiten

Onderwerp	Risicoanalyse
Omschrijving	Kwetsbaarheid van onderzoeksfaciliteiten
Ambitie	Voor interne doeleinden wordt een kwetsbaarheidsbeoordeling van de meest waardevolle onderzoeksfaciliteiten uitgevoerd. Waar mogelijk worden risico-beperkende maatregelen genomen om deze kwetsbaarheden aan te pakken. Rapportage van de kwetsbaarheden en maatregelen wordt vertrouwelijk behandeld.
1 Initieel	• Sommige faculteiten, instituten of dienstverlenende afdelingen zijn zich bewust van kennisveiligheidsrisico's met betrekking tot hun onderzoeksfaciliteiten. • Mitigerende maatregelen worden alleen voorgesteld wanneer de faculteit, het instituut of de afdeling wordt geconfronteerd met een (urgent) incident.
2 Herhaalbaar	• Er zijn enkele risico's voor kennisveiligheid geïdentificeerd en beschreven voor enkele van de meest waardevolle onderzoeksfaciliteiten. • Risicobeperkende maatregelen zijn informeel beschreven.
3 Gedefinieerd	• Rollen en verantwoordelijkheden zijn beschreven en gecommuniceerd. • Periodiek wordt een integrale kwetsbaarheidsanalyse uitgevoerd op het gebied van kennisveiligheid. Deze beoordelingen worden vertrouwelijk behandeld. • Periodieke rapportage informeert het hogere management over de genomen maatregelen. Deze rapportages worden vertrouwelijk behandeld.
4 Meetbaar en gemanaged	• Kennisveiligheidsmedewerkers bespreken periodiek de kwetsbaarheden met managers van de onderzoeksfaciliteiten en stellen gezamenlijk aanpassingen voor als dat nodig is. Deze gesprekken worden vertrouwelijk behandeld. • De effecten van deze maatregelen worden periodiek gerapporteerd aan het hoger management. Deze rapportages worden vertrouwelijk behandeld.
5 Continue verbetering	• De overzichten en methoden van de interne kwetsbaarheidsbeoordelingen worden in een cyclisch proces geëvalueerd en (indien nodig) verbeterd.
Bron/referentie	VSNU Kader Kennisveiligheid, hoofdstuk 4; Nationale Leidraad Kennisveiligheid (2022), hoofdstuk 6

5. Risicomanagement

De Leidraad vat de adviezen in relatie tot risicomanagement als volgt samen:

- Het is raadzaam een aantal **standaardprocessen centraal in te regelen**. Afhankelijk van het risico-niveau zijn de benodigde risicoanalyses en controles strikter en ligt de beslisbevoegdheid op een hoger, centraler niveau.
- Het begint met het aanwijzen van een **portefeuillehouder op bestuurlijk niveau** en het instellen van een **Adviesteam Kennisveiligheid** van enkele deskundigen met relevante expertises om de portefeuillehouder bij te staan. Dit advies wordt behandeld in het hoofdstuk Bestuur en beleidskader van dit volwassenheidsmodel.
- Zorg op bestuursniveau voor een centraal en up-to-date **overzicht van veiligheidsgevoelige partnerschappen, financiering en buitenlandse promovendi en gastonderzoekers**. Dit overzicht vormt de basis voor effectief risicomanagement binnen uw instelling. Ook geeft het inzicht in het cumulatief effect van ontwikkelingen die los gezien onproblematisch lijken.
- Het creëren van een **open veiligheidscultuur** binnen uw instelling is essentieel. **Bewustwordings-campagnes** kunnen daar een nuttige bijdrage aan leveren. Sluit daarbij zo veel mogelijk aan op de belevingswereld van de doelgroepen via trainingsmodules, teamsessies en simulaties. Dit advies wordt behandeld in het hoofdstuk Training en bewustzijn van dit volwassenheidsmodel.

Risicoanalyse en Risicomanagement zijn ook een onderdeel van het SURFaudit Toetsingskader. Het toetsingskader verschilt echter van de Nationale Leidraad Kennisveiligheid wat betreft inhoud en concepten. Voor de ontwikkeling van het volwassenheidsmodel is uitgegaan van de Leidraad.

Overzicht van veiligheidsgevoelige partnerschappen, financiering, promovendi en gastwetenschappers

Onderwerp	Risicomanagement
Omschrijving	Overzicht van veiligheidsgevoelige partnerschappen, financiering, promovendi en gastwetenschappers.
Ambitie	(Veiligheidsgevoelige) Internationale meerjarenovereenkomsten, zoals MoU's, Lol's, contracten of overeenkomsten, worden gearchiveerd en kunnen op centraal niveau worden opgevraagd. Er is een centraal systeem voor financiële transacties. Er is een centraal registratiesysteem voor alle promovendi en gastwetenschappers.
1 Initieel	• (Veiligheidsgevoelige) Internationale overeenkomsten worden op verschillende niveaus gearchiveerd en zijn beschikbaar voor relevante personeelsleden op facultair niveau. • Financiële transacties worden geregistreerd en zijn beschikbaar voor relevante medewerkers op facultair en centraal niveau. • Promovendi die in dienst zijn van de universiteit worden geregistreerd in het systeem voor werknemers.
2 Herhaalbaar	• Alle (veiligheidsgevoelige) internationale overeenkomsten worden opgeslagen en kunnen worden opgevraagd op centraal of facultair niveau. Er kunnen verschillende systemen zijn. • Alle financiële transacties worden opgeslagen en zijn opvraagbaar op centraal of facultair niveau. Er kunnen verschillende systemen worden gebruikt. • Alle promovendi en gastwetenschappers worden geregistreerd op centraal of facultair niveau. Er kunnen verschillende systemen gebruikt worden.
3 Gedefinieerd	• Verantwoordelijkheden voor archivering, registraties en autorisaties zijn toegewezen aan de verschillende systemen. • Een overzicht van (veiligheidsgevoelige) internationale afspraken, financiering, promovendi en gastonderzoekers kan centraal worden opgevraagd, via verschillende systemen. • Periodieke rapportage aan hoger management bevat een overzicht van (veiligheidsgevoelige) internationale afspraken, financiering, promovendi en gastonderzoekers.
4 Meetbaar en gemanaged	• De overzichten die worden gemaakt, (kunnen) worden gebruikt voor analytische doeleinden en strategische besluitvorming met betrekking tot kennisveiligheidrisico's. • De procedures voor het maken van overzichten van (veiligheidsgevoelige) samenwerkingsverbanden, financiering, promovendi en gastonderzoekers worden periodiek geëvalueerd en waar nodig aangepast.
5 Continue verbetering	• De overzichten worden opgenomen in een managementinformatiesysteem. • De resultaten worden gebruikt voor training en bewustwording over kennisveiligheidsrisico's binnen de organisatie. • De procedures worden binnen de universiteit geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.
Bron/referentie	EU Recommendation 2021/1700; Nationale Leidraad Kennisveiligheid (2022), hoofdstuk 6.

Integrale veiligheid

Afstemming met het (integrale) veiligheids- en beveiligingsbeleid aan de universiteit is belangrijk voor kennisveiligheid, vanwege de relatie met sociale veiligheid, fysieke veiligheid en cyberveiligheid.

Kennisinstellingen hebben een zorgplicht ten opzichte van werknemers en studenten als het gaat om hun **sociale veiligheid**. In het geval van studenten en onderzoekers uit landen waar fundamentele rechten niet worden gerespecteerd, kan de veiligheid ernstig worden geschaad door de acties van de staat van herkomst.

Onderwerp	Risicomanagement
Omschrijving	Integrale veiligheid
Ambitie	Het kennisveiligheidsbeleid is afgestemd op het (integrale) veiligheidsbeleid van de universiteit, met name op het gebied van fysieke veiligheid en sociale veiligheid.
1 Initieel	• Sommige medewerkers die zich bezighouden met veiligheid en beveiliging zijn op de hoogte van kennisveiligheidsrisico's. • Sommige medewerkers die zich bezighouden met kennisveiligheid zijn bekend met de veiligheids- en beveiligingsrisico's die van invloed kunnen zijn op de kennisveiligheid.
2 Herhaalbaar	• De afstemming tussen het kennisveiligheidsbeleid en het veiligheidsbeleid is beschreven en bekend bij de relevante medewerkers.
3 Gedefinieerd	• Het kennisveiligheidsbeleid is afgestemd op het veiligheidsbeleid van de universiteit. • De afstemming wordt periodiek gerapporteerd aan het hogere management.
4 Meetbaar en gemanaged	• De afstemming tussen het kennisveiligheidsbeleid en het veiligheidsbeleid wordt regelmatig geëvalueerd en bijgesteld. • Periodieke rapportages aan het hoger management bevatten een evaluatie van de afstemming van het kennisveiligheidsbeleid op het veiligheidsbeleid van de universiteit.
5 Continue verbetering	• De afstemming tussen kennisveiligheid en het veiligheids- en beveiligingsbeleid wordt voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.
Bron/referentie	

6. Training en bewustzijn

Training van personeel en management

Onderwerp	Training en bewustzijn
Omschrijving	Training van personeel en management
Ambitie	(Beginnende) onderzoekers, management en relevant ondersteunend personeel nemen deel aan trainingen of opleidingen op het gebied van kennisveiligheid die door de universiteit worden aangeboden.
1 Initieel	• (Beginnende) onderzoekers, management en relevant ondersteunend personeel worden af en toe geïnformeerd over risico's en maatregelen op het gebied van kennisveiligheid.
2 Herhaalbaar	• Algemene informatie over kennisveiligheid is beschreven en beschikbaar gemaakt. • Er worden informele bijeenkomsten over kennisveiligheid en relevante maatregelen gegeven.
3 Gedefinieerd	• De universiteit biedt cursussen over kennisveiligheid aan verschillende doelgroepen. • Periodieke rapportage aan het hoger management bevat een beschrijving van de cursussen en de deelname eraan.
4 Meetbaar en gemanaged	• De opzet en deelname van cursussen wordt periodiek geëvalueerd en (indien nodig) verbeterd. • Periodieke rapportage aan het hoger management omvat een evaluatie van cursussen en hun deelname.
5 Continue verbetering	• Het ontwerp en de deelname aan cursussen wordt binnen de universiteit geëvalueerd en (indien nodig) verbeterd in cyclische processen.
Bron/referentie	EU Recommendation 2021/1700, sectie 3.2.3; Tackling R&I Foreign Interference, hoofdstuk 3; Nationale Leidraad Kennisveiligheid (2022), sectie 8.2

Communicatieplan

Onderwerp	Training en bewustzijn
Omschrijving	Communicatieplan
Ambitie	Informatie over kennisveiligheid wordt gecommuniceerd en is toegankelijk voor medewerkers en studenten.
1 Initieel	• Informatie over kennisveiligheid wordt door medewerkers die betrokken zijn bij kennisveiligheid gedeeld met medewerkers en studenten wanneer zich relevante gevallen voordoen.
2 Herhaalbaar	• Informatie over kennisveiligheid is beschreven en wordt breder gedeeld door medewerkers die betrokken zijn bij kennisveiligheid.
3 Gedefinieerd	• Er is een communicatiestrategie met betrekking tot kennisveiligheid. • De communicatiestrategie maakt gebruik van verschillende communicatie-kanalen. • De taken voor communicatie van kennisveiligheidsinformatie zijn toegewezen.
4 Meetbaar en gemanaged	• Het communicatieplan en de daaropvolgende informatie en gerelateerde taken worden periodiek geëvalueerd en verbeterd (indien nodig). • De periodieke rapportage aan het hoger management omvat een evaluatie van de communicatie over kennisveiligheid.
5 Continue verbetering	• Het communicatieplan, de informatie en verantwoordelijkheden worden voortdurend geëvalueerd binnen de universiteit en (indien nodig) verbeterd in cyclische processen.
Bron/referentie	EU Recommendation 2021/1700; Tackling R&I Foreign Interference; Nationale Leidraad Kennisveiligheid (2022), sectie 8.2

Dienstreizen

De Leidraad vat de adviezen in relatie tot dienstreizen als volgt samen:

- U wordt geadviseerd een **bezoekersprotocol** uit te werken om risico's tijdens bezoeken aan sensitieve locaties te beperken. Omgekeerd vergt een **dienstreis** naar landen met een verhoogd risicoprofiel -bijvoorbeeld vanwege deelname aan een conferentie- de nodige voorbereiding en alertheid

Onderwerp	Training en bewustzijn
Omschrijving	Dienstreizen
Ambitie	Dienstreizen naar landen of bijeenkomsten met een verhoogd risicoprofiel worden voorbereid om kennisveiligheidsrisico's te mitigeren met gepaste maatregelen (bijv. een laptop meenemen zonder gevoelige gegevens of documenten op de harde schijf).
1 Initieel	• Onderzoekers en medewerkers die landen of bijeenkomsten met een verhoogd risicoprofiel bezoeken, beoordelen zelf de risico's en maatregelen voor kennisveiligheid. • Er zijn geen formele regels of verantwoordelijkheden.
2 Herhaalbaar	• Een protocol voor dienstreizen is beschreven en ter beschikking gesteld.
3 Gedefinieerd	• Het protocol voor dienstreizen naar landen of bijeenkomsten met een verhoogd risicoprofiel is goedgekeurd door het hoger management. • De verantwoordelijkheden voor de voorbereiding van dienstreizen zijn toegewezen, inclusief goedkeuring door het hoger management en ondersteuning door de IT afdeling (indien nodig). • Periodieke rapportage aan het hoger management bevat een beschrijving van het gebruik van het protocol.
4 Meetbaar en gemanaged	• Het protocol voor dienstreizen naar landen of bijeenkomsten met een hoog risicoprofiel wordt regelmatig geëvalueerd en (indien nodig) verbeterd. • Periodieke rapportage aan het hoger management omvat een evaluatie van de implementatie en het gebruik van het protocol.
5 Continue verbetering	• Het (gebruik van het) protocol voor zakenreizen naar landen of bijeenkomsten met een hoog risicoprofiel wordt voortdurend geëvalueerd binnen de universiteit en verbeterd (indien nodig) in een cyclisch proces.
Bron/referentie	Nationale Leidraad Kennisveiligheid (2022), section 8.3

7. Internationale partnerschappen

De Leidraad vat de adviezen in relatie tot internationale partnerschappen als volgt samen:

- Samenwerkingsovereenkomsten vormen een goed aangrijpingspunt voor het afwegen van kansen en risico's. Voor samenwerkingen met een verhoogd risico volstaan de standaard sjablonen voor overeenkomsten mogelijk niet. Het is zaak **juridische en veiligheidsexpertise in te schakelen**.
- Eenmaal gesloten, is het raadzaam de samenwerking regelmatig te evalueren en eventuele knelpunten vroegtijdig te adresseren. **Verleng overeenkomsten met verhoogd risico nooit stilzwijgend**. Zorg er binnen uw organisatie voor dat u ruim voor het verlengmoment wordt gealerteerd zodat u de afspraken kritisch tegen het licht kunt houden

Internationalisering

Onderwerp	Internationale partnerschappen
Omschrijving	Internationalisering
Ambitie	Het beleid en de procedures voor kennisveiligheid zijn afgestemd met de internationaliseringsstrategie van de universiteit.
1 Initieel	Ondersteunend personeel van het international office is bekend met kennisveiligheidsrisico's.
2 Herhaalbaar	De raakvlakken tussen het kennisveiligheidsbeleid en de internationaliserings-strategie zijn beschreven en bekend bij (sommige) betrokken medewerkers.
3 Gedefinieerd	De internationaliseringsstrategie is afgestemd op het beleid voor kennisveiligheid.
4 Meetbaar en gemanaged	De afstemming tussen het kennisveiligheidsbeleid en de internationaliserings-strategie wordt periodiek geëvalueerd en (indien nodig) verbeterd. Periodieke rapportage aan het hoger management omvat een evaluatie van de afstemming van het kennisveiligheidsbeleid met de internationaliseringsstrategie van de universiteit.
5 Continue verbetering	De afstemming tussen het beleid voor kennisveiligheid en de internationaliserings-strategie wordt binnen de universiteit geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.
Bron/referentie	

Samenwerking op onderzoek

Onderwerp	Internationale partnerschappen
Omschrijving	Samenwerking op onderzoek
Ambitie	De procedure voor formele internationale samenwerkingsovereenkomsten gericht op onderzoek, bedrijfsontwikkeling en/of adviesverlening omvat kennisveiligheidscontroles en -maatregelen.
1 Initieel	• Ondersteunend personeel dat betrokken zijn bij het opstellen van internationale samenwerkingsovereenkomsten zijn bekend met kennisveiligheidsrisico's en houden hier rekening mee. • Er zijn geen formele regels of verantwoordelijkheden.
2 Herhaalbaar	• De procedure voor het voorbereiden van internationale samenwerkings-overeenkomsten omvat kennisveiligheidsmaatregelen, waaronder due diligence en exportcontrole. • Sommige medewerkers die betrokken zijn bij de voorbereiding van internationale samenwerkingsovereenkomsten zijn bekend met kennisveiligheidsmaatregelen.
3 Gedefinieerd	• Medewerkers krijgen verantwoordelijkheden toegewezen voor het implementeren van kennisveiligheidsmaatregelen in de procedure voor het voorbereiden van internationale samenwerkingsovereenkomsten. • De procedure en het risicobeoordelingsformulier voor het voorbereiden van internationale samenwerkingsovereenkomsten inclusief kennisveiligheids-maatregelen zijn geformaliseerd en gecommuniceerd naar betrokken medewerkers op facultair en centraal niveau. • Periodieke rapportage aan hoger management bevat een beschrijving van relevante internationale samenwerkingsovereenkomsten waarin kennisveilig-heidsmaatregelen zijn genomen.
4 Meetbaar en gemanaged	• Kennisveiligheidsmaatregelen in de procedure voor het voorbereiden van internationale samenwerkingsovereenkomsten worden periodiek geëvalueerd en aangepast. • Bestaande internationale samenwerkingsovereenkomsten worden periodiek opnieuw geëvalueerd. • Periodieke rapportage aan het hoger management omvat een evaluatie van kennisveiligheidsmaatregelen in internationale samenwerkingen.
5 Continue verbetering	• Kennisveiligheidsmaatregelen in internationale samenwerking worden binnen de universiteit voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.
Bron/referentie	EU Recommendations 2021/1700 (export screening); Tackling R&I Foreign Interference; VSNU Kader Kennisveiligheid.

Samenwerking op onderwijs

Onderwerp	Internationale partnerschappen
Omschrijving	Samenwerking op onderwijs
Ambitie	De procedure voor formele internationale samenwerkingsovereenkomsten gericht op onderwijs omvat controles en maatregelen voor kennisveiligheid.
1 Initieel	• Ondersteunend personeel dat betrokken is bij de voorbereiding van internationale samenwerkingsovereenkomsten is bekend met kennisveiligheidsrisico's en houdt hier op ad-hoc basis rekening mee. • Er zijn geen formele regels of verantwoordelijkheden.
2 Herhaalbaar	• De procedure voor het voorbereiden van internationale samenwerkingsovereenkomsten omvat een aantal kennisveiligheidsmaatregelen, waaronder due diligence. • Medewerkers die betrokken zijn bij de voorbereiding van internationale samenwerkingsovereenkomsten zijn bekend met de kennisveiligheidsmaatregelen.
3 Gedefinieerd	• De procedure en het toetsingskader voor het opstellen van internationale samenwerkingsovereenkomsten inclusief kennisveiligheidsmaatregelen zijn geformaliseerd. • Medewerkers krijgen verantwoordelijkheden toegewezen voor het implementeren van kennisveiligheidsmaatregelen bij de voorbereiding van internationale samenwerkingsovereenkomsten. • Periodieke rapportages aan het hoger management bevatten een beschrijving van relevante internationale samenwerkingsovereenkomsten waarin maatregelen zijn genomen.
4 Meetbaar en gemanaged	• Kennisveiligheidsmaatregelen in de procedure voor het opstellen van internationale samenwerkingsovereenkomsten worden periodiek geëvalueerd, aangepast en gerapporteerd. • Periodieke rapportage aan het hoger management omvat een evaluatie van kennisveiligheidsmaatregelen in internationale samenwerking.
5 Continue verbetering	• De procedures voor kennisveiligheid (maatregelen) in relatie tot internationale samenwerking worden binnen de universiteit voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.
Bron/referentie	Nationale Leidraad Kennisveiligheid (2022), hoofdstukken 5 & 7. EU Recommendations 2021/1700 (export screening); Tackling R&I Foreign Interference; VSNU Kader Kennisveiligheid, hoofdstuk 2

8. Personeelsbeleid

De Leidraad vat de adviezen in relatie tot personeelsbeleid als volgt samen:

- De **werving en selectie** van nieuwe medewerkers is een cruciaal moment om veiligheidsrisico's in te schatten. Het is daarom van belang dat HR-medewerkers veiligheidsbewust zijn en signalen die wijzen op een verhoogd risico oppikken.
- Zorg ervoor dat nieuwe medewerkers **informatie en training** krijgen om hen veiligheidsbewust te maken. Daarnaast kan voorzien worden in opfrismodules en speciale trainingsprogramma's voor gastonderzoekers uit landen met een verhoogd risicoprofiel

Werving

Onderwerp	Personeelsbeleid
Omschrijving	Werving
Ambitie	Het algemene wervingsproces van nieuw personeel (voor functies met een hoog risico) omvat kennisveiligheidsmaatregelen, zoals een (licht) achtergrond-onderzoek (bijv. het beoordelen van eerdere werkgevers).
1 Initieel	• Sommige HR-medewerkers en ander relevant ondersteunend personeel op centraal en/of facultair niveau zijn bekend met kennisveiligheidsrisico's en nemen deze op in het algemene wervingsproces. • Er zijn geen formele regels of verantwoordelijkheden.
2 Herhaalbaar	• Het algemene wervingsproces van nieuw personeel op centraal niveau en/of sommige faculteiten omvat een aantal informele kennisveiligheidsmaatregelen, zoals een (licht) achtergrondonderzoek. • HR-medewerkers zijn bekend met informele kennisveiligheidsmaatregelen.
3 Gedefinieerd	• Het algemene screeningproces van nieuw personeel, inclusief kennisveilig-heidsmaatregelen, is geformaliseerd en gecommuniceerd naar HR op (relevant) facultair en centraal niveau. HR-medewerkers krijgen verantwoordelijkheden toegewezen. • Werving voor risicovolle functies vereist screening op hogere screenings-niveaus. • Periodieke rapportage aan hoger management bevat een beschrijving van de kennisveiligheidsmaatregelen in het wervingsproces.
4 Meetbaar en gemanaged	• Kennisveiligheidsmaatregelen in het algemene wervingsproces van nieuw personeel worden periodiek geëvalueerd en aangepast en gerapporteerd aan het hogere management.
5 Continue verbetering	• Kennisveiligheidsmaatregelen in het algemene wervingsproces worden binnen de universiteit voortdurend geëvalueerd en (indien nodig) verbeterd in een cyclisch proces.
Bron/referentie	Nationale Leidraad Kennisveiligheid (2022), hoofdstuk 8; VSNU Kader Kennisveiligheid, hoofdstukken 3 & 4.

9. Cyberveiligheid

Cyberveiligheid

Onderwerp	Cyberveiligheid
Omschrijving	Cyberveiligheid
Ambitie	Het beleid en de procedures voor kennisveiligheid zijn afgestemd met het cyberveiligheidsbeleid van de universiteit.
1 Initieel	• Ondersteunend personeel dat betrokken is bij cyberveiligheid is bekend met kennisveiligheidsrisico's. • Beleid voor gevoelige gegevens (classificatie en autorisatie) houdt op ad-hoc basis rekening met kennisveiligheidsrisico's.
2 Herhaalbaar	• De raakvlakken tussen kennisveiligheidsbeleid en cyberveiligheidsbeleid zijn beschreven en bekend bij (sommige) betrokken medewerkers.
3 Gedefinieerd	• Het cyberveiligheidsbeleid is afgestemd met het kennisveiligheidsbeleid. • Het beleid voor gevoelige gegevens (classificatie en autorisatie) omvat aandachtspunten en maatregelen voor kennisveiligheid.
4 Meetbaar en gemanaged	• De afstemming tussen het kennisveiligheidsbeleid en het cyberveiligheidsbeleid wordt periodiek geëvalueerd en verbeterd (indien nodig). • Periodieke rapportage aan het hoger management omvat een evaluatie van de afstemming van het kennisveiligheidsbeleid met het cyberveiligheidsbeleid van de universiteit.
5 Continue verbetering	• De afstemming tussen het kennisveiligheidsbeleid en het cyberbeveiligings-beleid wordt continu geëvalueerd binnen de universiteit en verbeterd (indien nodig) in een cyclisch proces.
Bron/referentie	Normenkader Informatiebeveiliging Hoger Onderwijs 2015. Toetsingskader Informatiebeveiliging Hoger onderwijs 2019. Surfaudit volwassenheidsmodel informatiebeveiliging HO v. 2.0