Summary

International cooperation and the open exchange of knowledge are essential for science and scholarship. At a time of tense and shifting geopolitical relations, however, the international nature of scientific research also entails risks: sharing knowledge can jeopardise national security (the undesirable transfer of knowledge), academic education and research can be improperly influenced by or from other states (interference) and knowledge can be used to suppress or undermine constitutional values, both in the Netherlands and elsewhere (ethical or integrity violations). The topic of ‘knowledge security’ is therefore high on the agenda, both nationally and internationally.

Dilemmas and discussions concerning knowledge security are at the heart of the mission and responsibilities of scientific endeavour; it is therefore crucial for the scientific community to deal with them scrupulously and judiciously. Given the importance and urgency of this issue, the Royal Netherlands Academy of Arts and Sciences (KNAW) considers it its duty to speak out about it.

Since 2022, the Dutch scientific community has followed the National Knowledge Security Guidelines and academic institutions can contact the National Contact Point for Knowledge Security for advice. This system appears to work well. With a view to planned further measures (including the screening of non-EU researchers based on a list of high-risk disciplines), the Academy wishes to stress that such measures must at all times be underpinned by the principles of open scientific exchange, academic freedom and institutional autonomy. More specifically, it makes the following recommendations:

1. Focus maximum efforts on raising awareness, and do not screen researchers on the basis of disciplines or technologies.
   - The most effective approach is to focus on reinforcing existing mechanisms and initiatives aimed at raising awareness and supporting researchers and administrators.
   - Systematically screening large groups of incoming researchers is too imprecise and difficult to implement; it also leads to a false sense of security and encourages exclusion and discrimination.
   - International coordination (at least at EU level) is needed if knowledge security policies are to be effective; the policy objectives will not be achieved if the Netherlands is alone in introducing measures.
2. **When drafting policies and implementing measures, proceed by weighing up the various interests carefully on a case-by-case basis.**
   - Measures must be in reasonable proportion to the desired objective. If less far-reaching measures are sufficient, they should be preferred.
   - When weighing up interests, there needs to be sufficient room to consider input from scientific researchers, in addition to information from government and the security services.

3. **Assign responsibilities at the lowest possible level and develop specific assessment frameworks for each knowledge domain.**
   - Individual researchers, research groups and managers must be supported and provided with information by both their own institution and the government. However, it must always be possible for decision-making to take place at a higher level.
   - Support can be reinforced by developing more specific frameworks, for example along the lines of the knowledge domains of technology, the exact sciences, the medical and health sciences, and the social sciences and humanities.
   - Risk assessment must be based on multiple relevant factors, such as the particular research topic, whether the specific case involves basic or applied research, the geopolitical situation, and the trustworthiness of partner institutions.

4. **Always differentiate between the three different meanings of 'knowledge security': (1) the undesirable transfer of knowledge, (2) interference and (3) ethical and integrity issues.**
   - On the one hand, the term 'knowledge security' brings issues into the domain of 'security' that do not belong there (for example purely economic considerations). On the other, it does not sufficiently encompass the various risks at stake in actual practice (for example ethical dilemmas).
   - It is essential to be alert to these different meanings: depending on the context, a careful distinction must be made between the type and extent of the risk and the associated interests that are involved.
Introduction

Science and scholarship are international. People all over the world are engaged in research on fundamental, practical, and societal problems and challenges. Close cooperation across borders and the open exchange of views and information are essential in this regard; only then is it possible to share knowledge, findings and doubts, to critically test one another’s questions, answers and methods, to achieve deeper insights together and to communicate with one another despite differences.

In a world of tense and shifting geopolitical relations, however, this inherently international nature of science increasingly poses risks. Scientific knowledge is a great good, but it can also be misused (including strategically), for example for warfare, repression, sabotage, distortion of economic competitiveness or political influence and interference. As a result, the topic of 'knowledge security within international partnerships' has recently been prioritised on the national and international agenda. Both in the Netherlands and elsewhere, measures and guidelines are being developed with a view to making international research cooperation not only sound and effective, but also 'secure'.

Formally, the term 'knowledge security' covers the following three issues:

1. The undesirable transfer of knowledge, i.e. the transfer of knowledge and technologies that may pose a threat to national security.
2. Interference, i.e. the (covert) influencing of academic education and research by or from other states, potentially threatening the academic freedom and security of students and researchers.
3. Ethics/integrity, i.e. issues that may arise, for example, when collaborating with researchers in countries where the government fails to respect human rights, or does so insufficiently.

In the Netherlands, the Minister of Education, Culture and Science has taken the lead in the discussion of knowledge security. Efforts have so far focused on raising awareness of dangers and risks among administrators, institutions and researchers, and providing support in formulating policies for international research cooperation. In this context, January 2022 saw the publication of the National Knowledge Security Guidelines, drawn up by the Ministry of Education, Culture and Science and various parties in the knowledge domain, including the Academy. In addition, a National Contact Point for Knowledge Security has been established. This is a nationwide initiative with access to representatives of the relevant ministries and the security services. The Contact Point provides advice and support on assessing the opportunities and risks involved in international research cooperation, for example by means of a 'Threat Assessment of State Actors'. Administrative arrangements have also been made with academic institutions on raising security awareness within their organisation and conducting risk analyses. Finally, in November 2020, the Minister of Education, Culture and Science announced their intention to present a parliamentary bill for a Knowledge Security Screening Act. This would make it possible to screen third-country nationals and potentially refuse them entry to certain ‘high-risk’

---


2 The threat assessment is a joint analysis by the AIVD, MIVD, and NCTV intelligence/security services of state actors that may harm the country’s security interests and how that may occur. Dutch government, Dreigingsbeeld Statelijke Actoren (2 November 2022): https://www.rijksoverheid.nl/documenten/rapporten/2022/11/28/tk-bijlage-dreigingsbeeld-statelijke-actoren-2.

3 The initial reference was to a ‘binding assessment framework for high-risk disciplines.’ See letter from the Ministers of Education, Culture and Science and Justice and Security and the State Secretary of Economic Affairs and Climate Policy to the House of Representatives, 27 November 2020, Kamerstukken II 2020/2021, 31288, No. 894.
Reasons for an Academy position paper

The current and proposed knowledge security measures are of the utmost importance to the scientific community. But however valuable they may be from the security perspective, far-reaching measures aimed at protecting knowledge security can involve drastic restriction of academic freedom and of scientific progress, which is founded on international cooperation and the internationally embraced principle of Open Science. International scientific cooperation and knowledge exchange are also an important form of soft diplomacy: it is crucial, precisely in times of geopolitical tension, that researchers can continue to transfer knowledge, maintain relationships, and exchange points of view. Experiences during the Cold War make this clear.

At the same time, however, the risks involved in international cooperation and knowledge exchange are widely recognised and understood within the scientific community. It is understandable that the government wishes to control how knowledge is acquired and shared internationally. It is also clear that academic institutions and individual researchers cannot address the problem of knowledge security and risk entirely on their own. Carrying out risk assessments is a complex matter and long-term security implications of today's decisions (such as setting up a project, starting a partnership, appointing a PhD candidate or postdoc) are often not immediately obvious. This can make it difficult for both individual researchers and administrators to assess the scale and impact of such decisions. An additional complicating factor is that scientific research often takes place at interfaces, for example between the public and private domains.

Within this zone of tension, the parties involved think differently about the manner and extent of intervention or regulation and the allocation of responsibilities with regard to knowledge security. The same applies to the trade-offs that need to be made between divergent interests and values. It is crucial that the scientific community deals with this scrupulously and judiciously. After all, the complexities and discussions concerning knowledge security are at the heart of the mission and responsibilities of science. Any measures imposed may well offer institutions guidance in fulfilling their responsibility to society, but they can just as easily lead to constraints on academic freedom. The Academy therefore views it as its duty to speak out about this issue.

It is against this background that this position paper first briefly addresses the term 'knowledge security'. It then discusses what the Academy believes should be the principles underpinning sound knowledge security policy. The paper goes on to review existing and announced policies based on these principles and finally formulates proposals for further policy.

---

4 Statistics Netherlands (CBS) defines a third-country national as ‘a person with a nationality other than that of one of the member states of the European Union, Norway, Iceland, Liechtenstein, or Switzerland.’ CBS. ‘Derdelander’ (September 2023): https://www.cbs.nl/nl-nl/onze-diensten/methoden/begrippen/derdelander.
1. The term 'knowledge security'

The definition of 'knowledge security' (kennisveiligheid) as currently used in various Dutch government documents is very broad. In practice, it relates not only to national security or to the terms defined in the introduction to the present position paper (undesirable knowledge transfer, interference, and ethical and integrity issues) but also, for example, to social safety and physical and economic security (including competitiveness). The term therefore gives rise to ambiguity about the nature of the risks to knowledge security and the desired or necessary measures.

On the one hand, not all of the genuine risks associated with international research cooperation can readily be associated with the term 'knowledge security'. Although issues of ethics and integrity are formally included in the definition, the term does not refer to them in so many words. As a result, ethical risks – in terms of the consequences of knowledge exchange for fundamental rights or constitutional values, both in the Netherlands and elsewhere – are wrongly still often excluded from discussions around knowledge security.

On the other hand, the word 'security' has connotations that do not apply equally to all the risks and threats that are subsumed under the term in actual practice. Although the term does highlight the urgency of the issues concerned, it also brings issues into the domain of 'security' and associated regulations that probably do not belong there. The frequent use of such terms as 'dual use' (for technology that can have both civilian and military applications) and 'foreign interference' (for influence and interference activities on the part of foreign governments) brings a certain degree of 'securitisation' into the debate as well, even where it only concerns, for instance, partnerships or exchanges that potentially affect the economic competitiveness of the Netherlands. Using the term 'knowledge security' thus frames the issue in a way that may obstruct frank and constructive discussion. It is difficult, after all, to be opposed to security or in favour of practices that pose a potential security risk.

Finding an alternative is no easy matter, however. In a number of countries, issues that in the Netherlands would be classed as 'knowledge security' are instead regarded as issues of 'integrity'. The advantage of that term is that it makes clear that ethical issues can also play a role in the debate. Using it may, however, lead to confusion with the term 'research integrity' as used in the Netherlands Code of Conduct for Research Integrity.

Because the term 'knowledge security' is now well established and a workable alternative is not readily available, the Academy will continue to use it in the present position paper. In the light of the concerns mentioned, it does however wish to add two important caveats:

1. The term 'knowledge security' must be used explicitly in the broad sense that has been articulated in the introduction; the same must also be done systematically in the course of wider debate on the subject.

---


It is necessary to **be aware at all times of the influence that security framing has** on policy choices and trade-offs. This means that in specific cases a careful distinction must be made between different types of risks and the interests involved, depending on the type of knowledge security at stake and the context in which risks arise.

2. **Guiding principles for policy**

A knowledge security policy that pays sufficient attention to the interests of science, scientists and academic freedom should be based on the following principles.

1. **It is necessary to avoid the constant creation of new frameworks, mechanisms and guidelines.** The government already has various mechanisms at its disposal – for example the National Knowledge Security Guidelines and mechanisms based on UN and EU sanctions policies – to take action in the event of security risks. Dutch knowledge institutions are also working hard to develop independent policies and to implement measures where necessary. The best approach is therefore to merge, further develop and, where necessary, critically review **mechanisms and initiatives that are already available.** Only where existing mechanisms are deficient can further measures be put in place.

2. **In determining the substance of measures and their application in specific cases, the basic principle must at all times be the proportionality of policies and regulations** (i.e. the reasonableness of the relationship between the aim and the means employed to achieve it). This means that the purpose served by certain measures or decisions must always be clearly stated. In that context, it is important to keep a watchful eye on the framing implied by the term 'knowledge security' and to emphasise its different meanings (undesirable knowledge transfer, interference, and ethical and integrity issues). Policies will sometimes aim to protect national security or to ensure that knowledge is not used elsewhere to suppress or undermine constitutional values, but they also may merely be aimed at avoiding harm to the competitiveness of the Netherlands. Hence, within the overall goal of protecting knowledge security, sub-goals are conceivable that are not always equally legitimate or important for all parties involved.

3. **Depending on the stated goal, there must always be a careful assessment of the suitability and necessity of the intended knowledge security measures in order to achieve that goal. If less far-reaching measures are sufficient, they should be preferred.** If that is not the case, a measure will not be proportionate.

4. **The various interests must always be weighed up,** based on the fundamental principles of open scientific exchange and academic freedom. This must also include assessing whether the energy required to introduce and implement a measure, and the costs involved, outweigh what the intended measure is likely to deliver specifically in terms of knowledge security.

In short, when assessing the proportionality of a measure (i.e. estimating its effectiveness and necessity, and weighing up the various interests involved), it is essential to **work on a case-by-case basis.** Measures that are formulated merely in general terms – such as designating all research in broader disciplines as potentially sensitive – in principle fail to satisfy the requirements of proportionality. Such measures are, on the one hand, often too broad, in the sense that they also impact research that does not pose a threat. That is problematic, because these measures do have the potential to greatly diminish academic freedom in the disciplines concerned. On the other hand, such measures may be too narrowly focused, in the sense that high-risk knowledge exchange may also occur in disciplines other than those selected.

---

10 In October 2023, the Knowledge Security Sector Review [Sectorbeeld Kennisveiligheid] will be shared with the House of Representatives; it was drawn up on the basis of a recent audit among all Dutch universities.

To avoid such 'over- and under-inclusiveness', it is desirable to examine the potential risks for each type of situation, or for each specific case of collaboration or exchange, and to carry out a proportionality assessment as referred to above. This should include considering the distance between, on the one hand, the research and, on the other, the development of possible applications of that research that may impact certain aspects of knowledge security. That can be done, for example, on the basis of technology readiness levels (TRLs), i.e. how far a technology is along the path from the earliest stage of research to technical and commercial maturity.  

Finally, the aforementioned principles mean that when defining knowledge security measures, an implementation test must always be performed in order to check whether what is proposed is realistically feasible in terms of lead time, quality, and the necessary financial investment. A non-discrimination test is also needed to ensure that measures do not facilitate unequal treatment, for example because they systematically disadvantage certain individuals or groups without sufficient objective justification.

3. Assessment of existing and announced policies

Awareness-raising and support

In light of the principles formulated above, we can conclude that certain aspects of the Dutch government’s current knowledge security policy are functioning properly. General awareness of risks has been greatly increased and the National Knowledge Security Guidelines and National Contact Point for Knowledge Security are proving valuable.

It should be noted, however, that researchers also need specific guidelines that are sufficiently tailored to their own field and which they can apply effectively themselves. Because the Contact Point does not handle cases that can be traced back to individuals, it is currently helpful mainly in assessing larger, institutional partnerships and less suitable for advising on specific individual situations such as the appointment of an individual employee.

Knowledge Security Screening Act

The Academy has major reservations regarding the proposed Knowledge Security Screening Act [Wet Screening Kennisveiligheid], both with regard to its proportionality and its feasibility in practice. Such legislation should make it possible to screen third-country nationals who wish to conduct research or work within certain disciplines so that they can be excluded in the event of a potential threat. As currently envisaged, screening covers a broad list of ‘sensitive technology areas’ that will be listed in an annex to the Act. The Academy is not convinced of the necessity and proportionality of such a tool based on a predetermined list. In particular, the Academy has the following objections to utilising a list as the basis for screening:

1. Such a list will hardly be effective. Screening is aimed at excluding ‘evil spirits’ who proactively seek to acquire sensitive knowledge, whereas knowledge can just as well ‘leak out’ through standard partnerships and international knowledge exchanges to which the Act will not apply. Technological advances also proceed at very high speed, making it extremely difficult to keep a list up to date and raising the question of who is responsible for doing so. Moreover, it will presumably be relatively easy to bypass the list. As a result, the mechanism will mainly create a false sense of security: if a subject, discipline or technology is not on the list, the actual effect may be to weaken the perceived knowledge security.

---


13 See the letter from the Minister of Education, Culture and Science to the Dutch House of Representatives (5 April 2023), Kamerstukken II 2022/23, 36200 VIII, No. 213.
need to be extra vigilant, with genuine security risks thus escaping attention. It is therefore more effective to **make more vigorous use of existing measures**, for example by increasing awareness of security risks among institutions and individual researchers and providing support for decisions about research collaboration right across the board (and not just in areas on a list).

2. The **risk of over- and under-inclusiveness** when screening individuals against a general list of 'sensitive technology areas' is expected to be substantial. It is almost inevitable that a list will be either too generic or, conversely, too specific. This is a problem not only from the practical point of view, in that the measure is therefore ineffective; it also means that more people than strictly necessary will have their academic freedom curtailed and that Open Science will be unnecessarily constrained.

3. From a more practical perspective, a system as currently envisaged will require an organisation able to process large numbers of applications at short notice, probably without much real knowledge of the scientific topics in question. This means that the **feasibility and practicability are questionable**. Such a system is also at odds with the aforementioned principle that clustering existing policies is better than introducing a new system.

4. A system based on screening increases the very real **risk of exclusion and discrimination**, for example on the basis of nationality. Moreover, even the appearance of exclusion and discrimination may foster distrust at the expense of the constructive dialogue needed on a complex topic like knowledge security.

5. If the Netherlands were to decide to be the first EU Member State – and for the time being the only one – to screen incoming researchers, there would be a risk that such researchers (even those who do not pose a risk) would instead go to countries with a less stringent knowledge security policy. That is not only a problem from the point of view of knowledge security; it is also detrimental to the competitiveness of a small country like the Netherlands and to national and international scientific progress. The Netherlands in fact benefits from open international exchanges in science and technology, both as regards attracting talented people and absorbing and applying knowledge and insights developed elsewhere (the reciprocity of scientific cooperation). It is therefore necessary **to not act unilaterally but only in cooperation with other EU countries or, preferably, in a broader EU context** and in collaboration with international and transnational partners, such as the OECD and UNESCO.

In light of the above objections and caveats, **the Academy strongly recommends to not introduce a screening act, as currently proposed** and instead put in place measures based on current, pre-existing frameworks and policy lines.

### 4. Proposed approach

In its report *Academic Freedom in the Netherlands* (2021), the Academy defines academic freedom as the principle that staff of academic institutions are free to perform their scientific research, disclose their findings and teach.\(^{14}\) Although the autonomy of academic institutions does not fall within this definition, the Court of Justice of the European Union ruled in 2020 that this autonomy must be seen as the institutional expression of academic freedom.\(^{15}\) Within the tasks and limitations imposed on them by law, government should therefore give institutions a large degree of autonomy in terms of administrative organisation, staffing, funding, and academic affairs. **Institutional autonomy is thus critical to guaranteeing academic freedom.** Responsibility for knowledge security therefore lies primarily with academic institutions, of

---


course within existing statutory guidelines and frameworks, such as UN or EU sanction regimes, and elaboration of these by the government.\textsuperscript{16}

Despite increasing efforts in this area, universities and other research institutions do not (yet) always have an adequate infrastructure and sufficient capacity and expertise to make well-considered choices in line with the principles formulated in Section 2 above. This means that it is necessary to allocate responsibilities regarding knowledge security in a graduated manner, according to the principle of assigning responsibilities at the lowest possible level.

The best way to guarantee the academic freedom of individual researchers and research groups is to allow them to decide as much as possible for themselves. Where that is not possible – for example because the potential risks are too great or there is too much (moral) doubt – there must always be the possibility of enlisting support or having decision-making take place at a higher level. In this regard, it is extremely important to provide sufficient support in identifying and assessing risks and determining at what level a decision can best be made.

More specifically, this means that if individual researchers wish to enter into partnerships with a foreign institution or appoint a researcher from a third country, they are responsible for seeking support and information (for example on what is or is not desirable or permissible) and for drawing attention to suspicious (or potentially suspicious) situations. Most universities now have a knowledge security coordinator who systematically collects and follows up such alerts and questions. Leaders of research groups and institutes also bear this responsibility and must be able to support individual researchers. Faculty boards must be able to provide sound advice for group leaders and researchers regarding more complex issues, in all cases with a view to academic freedom, Open Science, and non-discrimination. Responsibility for entering into partnerships and knowledge exchanges and for safeguarding institutional autonomy and academic freedom ultimately lies with the board of the institution concerned, which therefore has a role in providing support for the assessments and trade-offs that are to be made at lower levels. Finally, it is the government's responsibility to create frameworks, provide thorough information and raise awareness. The government can also play an important role by providing access, via the National Contact Point for Knowledge Security, to information about risks and security, as well as the expertise and experience that has been built up in this respect in recent times.

To assess risks specifically and effectively and to determine where problems and dangers lie, the deployment of specialised scientific expertise is essential at all levels. This requires systematic involvement and input from researchers, who must always be able to share their views on the sensitivity of particular research projects or partnerships in the light of the various aspects of knowledge security. Where relevant, specialist knowledge on the security situation must naturally also be brought in, for example from the security services. The National Contact Point for Knowledge Security offers excellent possibilities for this. In all cases, such knowledge will need to be assessed in the light of the varied and specialised scientific expertise.

\textit{Institutional assessment framework for knowledge security}

Effective knowledge security policy, which observes institutional autonomy and proportionality, requires a properly functioning system of checks and balances based on the principles of Open & Responsible Sciences and the existing codes of conduct and structures within the Dutch science system (including the Netherlands Code of Conduct for Research Integrity). All deliberations on measures to be implemented must be underpinned by the fundamental principle of open scientific exchange and academic freedom. This means that potential partnerships or

\textsuperscript{16}The \textit{Netherlands Code of Conduct for Research Integrity} (2018) obviously also provides a relevant framework here.
appointments should be assessed according to the principle of ‘yes, provided that’ rather than ‘no, unless’. A thorough balancing of the interests and risks involved can then take place for each particular situation or case, partly on the basis of the overall risk assessment.

Given the recently established, widely supported and demonstrably effective sector plan structure in the Netherlands, the Academy’s proposal (to be worked out in greater detail) is to create an assessment framework for each of the four knowledge domains – engineering and technology, the exact sciences, health sciences and medicine, and the social sciences and humanities – based on a detailed analysis of the type of knowledge security problems within that domain. In addition, where this is not already in place, a knowledge security team can be set up for each institution. Faculties, group leaders, and individual researchers will be able to approach the team with specific questions about partnerships, appointments, etc.; those questions can then be answered in the light of the domain-specific assessment frameworks. To be able to advise effectively on possible measures or action to be taken, the teams need to have access to the expertise of researchers and, via the National Contact Point for Knowledge Security, to know-how and information available within the government and security services. Advice on follow-up action can always include referring an issue to a higher administrative tier so that higher-level decisions can be made.

It is also necessary for risk assessments to always be based on a range of different factors, i.e. utilising a multidimensional model that considers the subject of the research; the type of research (basic or applied); the presumed trustworthiness of partner institutions; the geopolitical ambitions of governments; the international (scientific) dynamics; the type of technology and TRL level; the extent of freedoms in the country where a partner is based or comes from; etc. Already in 2014, the Academy gave some guidance to clarify how such factors always affect risk assessments to varying degrees. In addition, the principles of proportionality and case-by-case assessment referred to in Section 2 must play a key role in this process.

Based on the advice given and decisions taken at institutional level in particular cases, a national database of previous cases and considerations could gradually be compiled. It would serve as a reference for what decisions were taken and on the basis of what arguments (of course ensuring personal data protection and the safety of researchers). Such an approach can lead to policy based on best practices, as well as to consistency and accountability, in line with the idea that effective checks and balances are necessary so as to maintain the right balance between knowledge security and academic freedom and openness.

**Conclusion**

International scientific collaboration and the open exchange of knowledge are essential, but also entail risks, particularly in a world that is increasingly characterised by large-scale armed conflict, rapidly shifting geopolitical relations, threats to constitutional values and more and more vicious use of modern technologies. In certain cases, national, physical, societal or economic security may be harmed by knowledge being shared, or knowledge transfers may lead to a threat to fundamental rights or constitutional values. When adopting measures in this zone of tension, academic freedom and institutional autonomy must be prioritised. An integrated knowledge security policy must be multi-layered and allow for individual risk and proportionality assessments based on scientific expertise.

This means that general measures such as systematically screening foreign researchers in

---

certain disciplines are unadvisable. What is advisable, however, is to build on the positive experience gained with the National Contact Point for Knowledge Security and in working via knowledge sectors. That can be accomplished, for example, by drawing up assessment frameworks for each knowledge sector or domain, based on the principles outlined in the present position paper. Local knowledge security teams can also be set up at institutional level. Based on advice from these teams, assisted by the National Contact Point for Knowledge Security, individual researchers, group leaders, faculties, and institutions can then make assessments and decisions according to the type of situation or on a case-by-case basis.

About this publication

This Academy position paper was prepared by the Academy’s Committee for the Freedom of Scientific Pursuit (CVW), whose members are:

- Prof. J.H. (Janneke) Gerards, Utrecht University (chair)
- Prof. R. (Roberta) D’Alessandro, Utrecht University
- Prof. W.G.J. (Jan Willem) Duyvendak, University of Amsterdam
- Prof. P.A. (André) Nollkaemper, University of Amsterdam
- Prof. W. (Wim) van Saarloos, Leiden University
- Prof. M.H.N. (Maartje) Schermer, Erasmus MC

The committee is assisted by its secretary Dr M.J. (Melle) Kromhout, in collaboration with R.M.A. (Rosa) Lokenberg.

The content of the position paper was compiled partly on the basis of the Expert Meeting on Knowledge Security with members of the Academy and The Young Academy, held on 26 June 2023 at the Trippenhuis in Amsterdam.

A draft of the position paper was submitted for comment to:

- Prof. M. (Maghiel) van Crevel, Leiden University
- Prof. E.M.H. (Ernst) Hirsch Ballin, Tilburg University
- Prof. I.R. (Ibo) van de Poel, Delft University of Technology
- The Academy advisory councils: Council for the Humanities, Council for Medical Sciences, Council for Natural Sciences and Engineering, and Social Sciences Council

The Academy is extremely grateful to the reviewers for their suggestions. The reviewers bear no responsibility for the content of this position paper.