Framework
Knowledge Security
Dutch Universities
## Inhoudsopgave

<table>
<thead>
<tr>
<th>Hoofdstuk</th>
<th>Titel</th>
<th>Pagina</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Chapter 1 - Introduction</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Context: local, regional, global</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>Principles and concepts</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Application of this framework</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Organisation of this framework</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Chapter 2 - Opportunities and risks of international collaboration</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Opportunities for universities through internationalisation</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>Risks of global research and education</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>Chapter 3 - Governance and policy frameworks</td>
<td></td>
<td>19</td>
</tr>
<tr>
<td>European and international</td>
<td></td>
<td>21</td>
</tr>
<tr>
<td>National</td>
<td></td>
<td>22</td>
</tr>
<tr>
<td>Universities</td>
<td></td>
<td>23</td>
</tr>
<tr>
<td>Chapter 4 - Risk management</td>
<td></td>
<td>25</td>
</tr>
<tr>
<td>Local embedding</td>
<td></td>
<td>26</td>
</tr>
<tr>
<td>Knowledge Security Advisory Team</td>
<td></td>
<td>28</td>
</tr>
<tr>
<td>Support processes</td>
<td></td>
<td>29</td>
</tr>
<tr>
<td>Due diligence / preliminary investigation</td>
<td></td>
<td>32</td>
</tr>
<tr>
<td>Risk identification</td>
<td></td>
<td>33</td>
</tr>
<tr>
<td>Risk assessment</td>
<td></td>
<td>33</td>
</tr>
<tr>
<td>Risk response</td>
<td></td>
<td>34</td>
</tr>
<tr>
<td>Risk monitoring</td>
<td></td>
<td>34</td>
</tr>
<tr>
<td>Transition period</td>
<td></td>
<td>34</td>
</tr>
<tr>
<td>Appendices</td>
<td></td>
<td>36</td>
</tr>
<tr>
<td>Estimation of time spent</td>
<td></td>
<td>37</td>
</tr>
<tr>
<td>Participants Workgroup</td>
<td></td>
<td>38</td>
</tr>
</tbody>
</table>
Dear Reader,

The Dutch Universities cherish the openness of science and are, at the same time, aware of its drawbacks. This framework enables scientists and universities to better balance the openness of science on the one hand and preventing unwanted knowledge transfer on the other.

International cooperation is crucial for top research and the best academic education. An international focus provides us with opportunities and risks. Opportunities for research, education and innovation, for open knowledge sharing. Universities - because of their open, international character - are a target for espionage activities, for obtaining sensitive technologies and to influence opinions. The risks are therefore theft of knowledge by other countries and influencing staff in higher education and science, which can lead to (self) censorship and the erosion of academic freedom.

This framework was created in a working group on knowledge security, an interdisciplinary working group with experts from all Dutch Universities. In addition, other experts in the field of knowledge security were consulted. We would like to thank everyone who has been involved in working on this Framework for Knowledge Security.

We see this framework as a step in the increasingly conscious handling of risks in the area of knowledge security. Universities ensure that they:
1. are compliant with relevant legislation and regulations
2. translate risk inventories into faculties, programmes and research groups
3. further develop a framework and decision making process
4. set up a knowledge safety advisory team per university
5. develop training and awareness of all staff focused on knowledge security
6. include knowledge security in the university’s risk management system

Ultimately, everyone has a role to play in managing security risks. We would therefore like to conclude with an appeal to all academics to use the framework consciously and to make well-considered decisions regarding international partnerships, and, of course, to continue to provide excellent academic education and to conduct doing ground-breaking research.

Kind regards,

Pieter Duisenberg

Chairman Association of Universities
Chapter 1
Introduction
Chapter 1
Introduction

The freedom to choose research and education topics and the freedom to make research results available are academic achievements. At the same time, universities want to prevent the use of research results for unethical or otherwise undesirable purposes as much as possible. To support institutions in making decisions and policies concerning knowledge security, Dutch universities have drawn up this framework to knowledge security.

This framework for Dutch universities can be used to uphold and use in shaping their institutional policy. It offers guidelines to enable institutions to make well-informed and substantiated decisions about international collaborations. This framework is aimed at a target audience of university administrators, researchers, the university sector as a whole and relevant Dutch ministries. The publication of the framework also answers the call from government and society to take responsibility as a sector for safeguarding knowledge security.¹

International collaboration is becoming increasingly challenging. Universities are concerned about academic values and freedoms and other ethical principles in some partner countries. State actors (including in the Netherlands) can use resources in ways that infringe on staff members’ academic freedom. This also puts pressure on open science and open access ambitions. Universities are responsible for safeguarding academic values. Academic freedom is legally guaranteed both in the Netherlands (under the Constitution and the Dutch Higher Education and Research Act) and at the international level (in the EU Charter and the European Convention on Human Rights). Academic freedom is a fundamental and human right.

Context: local, regional, global
Universities collaborate with businesses, public authorities and knowledge institutions in many ways: in research, in education and in the development of innovative solutions to societal problems. Such collaboration often arises from bottom-up initiatives: research groups seek out like-minded people on the other side of the world or just across the border, a degree programme organises an educational exchange, or a start-up chooses an international company to work with as part of its growth strategy. Universities have checks and balances to evaluate and approve these collaborations, while working to raise awareness of the fact that such partnerships can sometimes involve threats as well.

The qualities of our researchers are recognised in the Netherlands and beyond, putting us on the radar of both well-intentioned and malicious individuals, groups and countries. They can pose a threat to our norms, values, security, people and economy. This threat can manifest itself in various ways, such as through cyber attacks or espionage, but also through manipulation or sabotage of scientific research. International relations are subject to change as well, which means that the risks can change. These developments jeopardise the (cyber)security of our institutions, our staff and our students.

How do universities deal with the complex balancing act they find themselves in every day, between opportunities on the one hand and risks on the other? With their Letter to Parliament on Knowledge Security, three Dutch ministries (Education, Culture and Science; Justice and Security; and Economic Affairs and Climate Policy) marked the start of efforts to focus on this issue both nationally and within each university. To support universities in making decisions and policies concerning knowledge security, parties in the sector have drawn up this framework. Application of this framework should ensure that students and staff can learn, teach and carry out research in a safe environment, free from unwanted knowledge transfer or adverse influence, while preserving academic values.

Principles and concepts
Definition in Letter to Parliament from Ministry of Education, Culture and Science dated 27 Nov 2020:

‘Knowledge security is first and foremost about preventing the unwanted transfer of (sensitive) knowledge and technology, which could negatively impact the national security of our country and damage the Dutch capacity for innovation. It also concerns the covert influence of state actors on higher education and science, which can lead, among other things, to forms of (self-)censorship that are detrimental to academic freedom. Finally, knowledge security involves ethical issues that may be related to collaboration with individuals and institutions from countries where fundamental rights are not respected.’

---

2 Call from the President of the Royal Netherlands Academy of Arts and Sciences (KNAW): Universities, protect your employees.
3 Collaboration between AIVD (Dutch General Intelligence and Security Service), MIVD (Dutch Military Intelligence and Security Service) and NCTV (National Coordinator for Counterterrorism and Security), ‘State Actors Threat Assessment’.
Such issues could include the ‘leaking’ of sensitive scientific knowledge and technology to countries and regimes which then use this knowledge to harm us and our partners, or use it against citizens in their own countries or elsewhere in a way that we would consider unethical or socially irresponsible. This can happen in many ways, such as through cyber attacks or espionage, but also through manipulation or sabotage of scientific research. Issues surrounding (self-)censorship could play a role as well, causing researchers and students to no longer feel free to speak out or express criticism of certain countries. These developments jeopardise the (cyber)security of our institutions, staff and students. Ensuring the safety of our students and staff is therefore an important starting point for this framework.

The freedom to make research results available and the freedom to choose research topics are and will remain the most important academic achievements. Academic freedom is explicitly recognised as a fundamental and human right in the EU Charter and the European Convention on Human Rights. At the same time, universities want to comply with European and Dutch laws and regulations. Such legislation is further discussed in Chapter 3. Universities also want to prevent the use of research results for unethical or otherwise unwanted purposes as much as possible. It is crucial to carefully consider the proportionality of the potential risks and subsequent measures. University research is conducted across the full breadth of disciplines, but not every field is equally a potential target for unwanted influence or unwanted knowledge transfer. In fact, in the majority of research, the risk is low.

Current practices
Universities have always had various check and balances to evaluate collaborations in the areas of research, education and valorisation. Within Dutch universities, for example, there are guidelines for good governance, public-private partnerships, intellectual property and academic integrity. These documents are and will remain relevant in the context of knowledge security, offering universities and staff perspectives for action.

Application of this framework
The purpose of this framework is to provide a base for assessing the opportunities and risks of international collaboration. This framework offers university administrators a country-neutral assessment framework for making policies and decisions about knowledge security. The framework is designed to be applicable to all universities, regardless of research focus, scale or expertise. The framework is applicable to individual employees of universities, their Executive Boards, the university sector as a whole and the relevant Dutch ministries (Education, Culture and Science; Interior and Kingdom Relations; Economic Affairs and Climate Policy; Defence; Justice and Security; and Social Affairs and Employment). These represent four distinct target groups and application possibilities.

---

5. Insert VSNU guidelines for good governance code, public-private partnerships, intellectual property and academic integrity.
For *individual employees*: increasing awareness of opportunities and risks as well as knowledge of their own perspectives for action and the decision-making structure in countries and programmes which the government has labelled as risky.

- for researchers;
- for those responsible for the intake of international students and for student and staff exchange programmes;
- for those responsible in the HR process for the appointment of international staff;
- for those responsible for developing the structure and content of joint projects/programmes;
- support staff such as lawyers and contract officers.

For the *boards* of universities:

- development framework that outlines the opportunities and risks for each part of the university, defines the European and national frameworks, and explains how and where this should be considered in an integrated manner;
- a framework that serves to identify on which fronts staff, students and knowledge must be protected;
- a starting template for a process and a structure to give knowledge security a permanent place in business operations, decision-making and primary processes at universities, including a targeted approach for training and communication;
- adjustment/use of applications for registration of research projects, archiving, communication and auditing needs;
- sharing dilemmas and case histories with other universities;
- such an approach leads to a better response and stronger preparation when new cases relating to this issue arise.

For the *university sector* as a whole:

- inventory of opportunities and risks of international collaboration, in which the risks are managed in light of increased international and strategic competition and growing political polarisation;
- a draft for a structured process and an indication of the resources needed to identify, address and deal with the opportunities and threats of international collaboration, in cooperation with other players in the higher education sector.
For the *ministries involved* in knowledge security (in addition to Education, Culture and Science; Justice and Security; and Economic Affairs and Climate Policy, also: Foreign Affairs; Social Affairs and Employment; and Defence):

- well-defined need: what universities need from the ministries (institutional embedding, resources, knowledge) so that students and staff can learn, teach and conduct research in a safe environment;
- development of national and European policies on technology sovereignty to prevent a lack of alternatives within Europe, when strategic collaboration with certain regions is not an option due to knowledge security risks.

**Organisation of this framework**

This introduction describes the reasons for and context of the framework. Chapter 2 then discussed the opportunities and risks of research and education on a global scale. Balancing these opportunities and risks is and remains a complex issue. Chapter 3 outlines the international, governmental and university-specific governance structures for managing this issue. Chapter 4 describes how this can be implemented within universities using a decision tree that includes stakeholders, responsibilities and risk management processes. Attention is devoted to due diligence, information provision/communication, knowledge sharing and security.
Chapter 2
Opportunities and risks of international collaboration
Chapter 2
Opportunities and risks of international collaboration

Opportunities for universities through internationalisation
Dutch universities seek cooperation with other universities, businesses and public authorities that have additional knowledge and research facilities in order to work together in consortia to solve societal problems. Universities collaborate in many ways: in research and education and in developing innovative solutions and valorisation. Such collaboration often arises from bottom-up initiatives: research groups seek out like-minded people on the other side of the world, just across the border or within the Netherlands; a degree programme organises an educational exchange; or a start-up chooses an international company to work with as part of its growth strategy.

International partnerships give Dutch universities access to people and resources, enabling the Netherlands to maintain its leading position in world of science. In addition, such partnerships provide a fresh look at research topics, cultures and customs in other countries. International collaboration also offers the Netherlands the opportunity to spread our (academic) standards, values and customs around the world. For example, Dutch universities have been successfully promoting open access and open science for years. In short, without international collaboration, it is impossible for a small country like the Netherlands to conduct research and facilitate education at a world-class level.

The process of globalisation and the associated increase in worldwide interaction and the use of (digital) networks between people and organisations has a major impact on society and the daily lives of many. Never before have we been exposed to such a large number of internationally-oriented organisations and people from such a large variety of cultural backgrounds as in today’s global labour market, in all sectors, both academic and otherwise, in both the public and private sector. Globalisation and internationalisation therefore offer countless opportunities for research and education, and have become mainstays of university life. They are integral parts of the modern university.

Research
A growing number of issues in contemporary scientific research are complex, interdisciplinary and socially relevant. In addition, themes like sustainability, public health, the energy transition and migration are by definition cross-border issues that depend on cooperation between disciplines and across national borders. By sharing knowledge in global alliances within larger ecosystems of businesses, (semi-)public authorities, NGOs, and education and research institutions, we can work towards solutions for a better world. Such partnerships are crucial to improve access to talent, knowledge, complementary research environments, state-of-the-art research facilities and funding. This ultimately leads to a positive impact.
Education
Universities constantly strive to improve, strengthen and enrich the international orientation of their Bachelor’s and Master’s curricula through education and research initiatives with leading (academic) partners worldwide. These partnerships enable students to develop competences such as intercultural understanding, diversity in context and integration through interaction with peers in student exchange programmes and joint projects. This means that, in addition to using the international insights and knowledge that they acquire from the curriculum, students must learn to deal with diversity and master intercultural skills during the course of their studies. The learning process should be facilitated in such a way that students develop an international outlook and a broad understanding of the world around them.

This issue will become increasingly relevant in the near future due to the developments surrounding lifelong learning (LLO). Many professionals will be seeking out training and education programmes in the Netherlands and abroad in the years ahead. Due to the growth in microcredentials, Dutch universities can also expect a digital influx of international talent.

Risks of global research and education
In addition to the opportunities based on our level of research and education, there are of course also risks for the Netherlands and the academic world. It is explicitly not the purpose of this framework to eliminate all possible risks. However, it is essential to have a good understanding of the risks (through risk management) and an effective way to manage them (through proper agreements in a governance structure). Various reports describe the risks to the Netherlands, Europe and the academic world (including Rathenau, Clingendael, NCTV).

In next four sections, we describe the main categories of these risks in the same order as the four types of knowledge security outlined in Chapter 1. Lastly, we describe the risk of an overly rigid approach to knowledge security cases.

Risk to national and international security
The most obvious knowledge security risk is that posed to national and international security. For some of these risks, national and international legislation is already in place. Examples include export restrictions on dual-use technologies through the Wassenaar Arrangement, missile technology through the multilateral Missile Technology Control Regime (MCTR) and EU regulations for countering the spread of biological and chemical weapons. However, these treaties and laws are not conclusive on subjects that pose a risk to national and international security, and by definition they lag behind the state of the art, as evidenced by recent conference insights on omni-use technology and the application of the abovementioned treaties and laws to so-called emerging technologies. It is the responsibility of individual researchers, departments and universities to develop a broad understanding of the possible consequences of their research. This is a complex, but absolutely necessary task.
A few examples show the complexity of this risk:
- researchers from risk countries who apply for a research position at a department that conducts research on dual-use technologies;
- cyber incidents concerning access to researcher data that fall under the Missile Technology Control Regime;
- publication of research on virus mutations which, in the hands of malicious parties, could lead to the development of biological weapons;
- publication of vulnerabilities in software that could lead to large-scale cyber incidents.

Risk to economic security
There is an inherent tension between academic entrepreneurship (including free dissemination of knowledge and as much fruitful collaboration as possible) and national protection of our relative innovative capacity (compared to other countries). This tension is particularly evident when it comes to research that has more economic and instrumental utility. One way of identifying this tension and assessing interests is by using the so-called Technology Readiness Level (TRL) of the research in question. The EU has broken this down into nine usable levels, from fundamental research to economically viable production.⁶ The exact application of the EU TRLs requires some practice, but is useful to discuss and weigh the tensions between academic entrepreneurship and the protection of economic security. This classification can also be used in the risk assessment for national and international security, as legislation usually does not provide unambiguous requirements in this regard. A few examples show the complexity of this risk:
- partnership with foreign agricultural industry for more efficient vegetable cultivation;
- use of foreign computer systems for research into nanotechnology.

Risk of (covert) influence on researchers or lecturers
Influence has many forms, origins, directions and effects. For example, influence can be exerted through ‘positive’ factors (e.g. financial, ideological, resources, access, positions, recognition) or ‘negative’ factors (e.g. controversy, blackmail, coercion, political pressure, bureaucracy, denial of entry or visas, fines). The originators can be individuals, organisations or public authorities in the Netherlands or abroad. The direction of influence can be aimed at institutions, faculties, departments or individual staff members. The effects can include (self-)censorship, infringement of academic freedoms, interference with choice of research topics, infringement of research integrity, forced termination of research, and damage to the reputation of the institution, department or individual researchers. The recent call from the President of the Royal Netherlands Academy of Arts and Sciences for universities to protect their staff⁷ shows that this risk should be taken very seriously.

---
⁶ The EU describes nine levels: from ‘basic principles observed’ in Level 1, through ‘technology validated in lab’ in Level 4 to ‘actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)’ in Level 9.
⁷ https://www.scienceguide.nl/2021/03/president-knaw-universiteiten-bescherm-je-medewerkers/
Some examples (without value judgements) show the complexity of this risk:
- influencing of researchers from the diaspora of risk countries;
- denial of entry or visas for researchers travelling to high-risk countries;
- nuanced adjustments to research results at the request of the research sponsor;
- exclusion of researchers from public debate due to threats;
- threat of student exchange cancellation due to incidents in the process of collaborating with a foreign university.

Risk of unethical or inappropriate use of research results or education
There is a risk that the knowledge, skills and technology gained from research and education could be used unethically or otherwise inappropriately. Assessing these risks in advance is usually complicated, partly because unethical or inappropriate use is subject to interpretation. Furthermore, the relationship between the theoretical research results or teaching material and its practical unethical or inappropriate use is not always strong. Some examples (without value judgements) show the complexity of this risk:
- Research in the field of artificial intelligence can be used to make automated camera surveillance more efficient, and thus useful for state-backed oppression.
- Research into seed breeding can be used to make heroin cultivation more efficient, thus lowering the street price of heroin.
- Computer science students, who have been taught how the security of information systems works, can be recruited by (state) actors to break into the systems of businesses and public authorities.

Risk of an overly rigid approach to knowledge security
A final – but important to recognise – risk concerns an overly rigid, one-dimensional approach to knowledge security. Causes can include a lengthy, bureaucratic or non-transparent process. This can have major consequences: the competitive position of the institution within the Netherlands or Europe can be affected; important research themes/problems can be delayed; individual researchers or departments can become demotivated or start working around the established processes; the quality and application of research can be compromised and the institution can be held liable for prematurely terminated research or contributions to a consortium.
To overcome these risks, an agile and transparent approach is needed. It should be closely linked to the primary research process, include a clear process and deadline, and above all have a ‘yes, unless’ mentality. In addition, it is important to periodically evaluate the entire system of knowledge security checks and balances at the university based on national and international case histories and make adjustments if necessary.

Existing measures
As the Letter to Parliament also explains, universities, the VSNU, Dutch ministries, the international community and numerous other institutions have not been sitting idly by in recent years. There are numerous (functioning) measures, procedures, guidelines and checklists to identify and manage risks related to knowledge security. In drawing up this framework, we do not wish to ignore these documents. In designing the framework, we also advise working within the context of existing governance, processes, procedures, measures, checklists, etc. as much as possible. However, the initiative for this framework alone shows that these are currently insufficient to adequately manage the risks of knowledge security. On the one hand, this is due to the fact that not all documents and processes are known to those parties involved; on the other hand, the general awareness of knowledge security risks is low. It will therefore be necessary not only to align with existing material, but also to make changes, additions or complete revisions and to inform the relevant parties about these materials. As we do not aim to include an exhaustive list of existing documents, below are the most important ones for immediate use:

Laws and regulations
- EU export control regimes for dual-use technologies based on Wassenaar Arrangements, Missile Technology Control Regime and EU regulations for combating the proliferation of biological and chemical weapons;

Sectoral regulations, guidelines and codes
- Dutch Universities Governance Code;
- Netherlands Code of Conduct for Research Integrity;
- Royal Netherlands Academy of Arts and Sciences (KNAW) brochure on challenges and dilemmas in international scientific collaboration from 2014;
- VSNU overview of guidelines for public-private partnerships and intellectual property;
- International examples of guidelines, including from Australia, Germany, the United Kingdom, Sweden and Canada;

Specific checklists for collaboration with China from The Hague Centre for Strategic Studies (HCSS)\(^\text{10}\) and the Leiden Asia Center (LAC);
- Points for attention for collaboration with China from policy paper ‘Netherlands-China: a new balance’.
- Local initiatives for checklists, procedures and risk processes for entering into international partnerships.

Chapter 3 describes how the governance of knowledge security within the Netherlands should be safeguarded. Chapter 4 then outlines how risk management processes can be implemented at universities to assess where the abovementioned documents can be used effectively, and where additional measures and processes are needed. This also ties in closely with recent investments at universities to take an integrated approach to security issues. Because knowledge security is a multidisciplinary domain, an integrated approach is ideal.

\(^{10}\) HCSS, ‘Checklist for Collaboration with Chinese Universities and Other Research Institutions’.
Chapter 3
Governance and policy frameworks
Chapter 3
Governance and policy frameworks

Dutch universities act on the basis of the Dutch Constitution, the European Convention on Human Rights and the EU Charter of Fundamental Rights. As stated in the ‘Magna Charta Universitatum’, the freedom of research and education is an essential condition for the success of universities.

Ultimate responsibility for both awareness and self-regulation of knowledge security lies with the Executive Board. However, the university is characterised by the decentralised organisation of science and research, with a great deal of autonomy for academic staff and faculties. The primary tasks of the university – scientific research and education and valorisation of research, as described in the Dutch Higher Education and Scientific Research Act (WHW) – are carried out by faculties. Universities are also open network organisations. The academic staff are connected to global scientific networks and thus to the global social and economic environment as well. These complex networks make management and decision-making processes within the university complicated.

There is an explicit interest in joining forces and arriving at a common approach in the field of knowledge security: for the Ministry of Education, Culture and Science and for security services, but also for institutions and the researchers and staff involved. An approach that has proportionality as its guiding principle, because the transparency and accessibility of education and science should never be compromised. Neither should academic freedom, research integrity and institutional autonomy.

The Dutch government, in turn, works to increase knowledge security in various ways. There is an approach aimed at state threats\textsuperscript{11}, for instance, and the government’s China memorandum also contains a detailed discussion of knowledge-related aspects.\textsuperscript{12} In addition, there is increased scrutiny of students and researchers who may be linked to the North Korean or Iranian ballistic missile programmes.\textsuperscript{13}

\textsuperscript{11} Link to Letter on State Threats
\textsuperscript{12} Netherlands-China: a new balance
\textsuperscript{13} Link to Letter to Parliament on enhanced supervision of students and researchers from risk countries
Universities need clear guidelines from the Dutch government. The government and parliament provide public knowledge institutions with frameworks for:

a. What responsibility they expect knowledge institutions to take for national security;

b. How they should weigh security interests against other interests, such as those of free science, economic development, innovation capacity and competitiveness, contributing to global public goods, attracting top talent, and good bilateral relations. After all, the Letter to Parliament confirmed that the institutional autonomy of the institutions is and remains essential;

c. Which standards knowledge institutions should adhere to in order to guarantee a level playing field.

International collaboration and certain activities may be subject to specific laws and regulations that must be complied with.

**European and international**

**International sanctions**

The United Nations (UN) and the European Union (EU) impose international sanctions on countries, organisations, companies and individuals. This may be done in case of a threat to international peace and security, for example. The EU can also impose sanctions to defend peace, international security, human rights, respect for international law, democracy and the rule of law. There are sanctions to prevent the proliferation of nuclear weapons, for instance, as well as sanctions against countries, individuals and organisations that violate human rights and sanctions against people involved in terrorist activities.

Sanctions are coercive measures. This does not involve military means. The purpose of sanctions is to:

- change inappropriate behaviour of individuals, companies, organisations or countries;
- make it more difficult to behave in this inappropriate manner;
- deter others from engaging in the same inappropriate behaviour.

Currently, measures are in place for around 30 countries. When pursuing international partnerships, it is therefore important to check whether there are any sanctions against certain countries, universities or companies.

---

14. See explanation of the Sanctions Act in the Netherlands and the national sanctions list of individuals and organisations involved in terrorist activity.

15. See sanctions list at www.sanctionsmap.eu
For students and researchers, having studied at a sanctioned university does not actually pose a problem, provided that:
- he/she has no formal appointment there;
- he/she no longer has any ties with the university;
- he/she is not dependent on the university;
- the university itself assesses (espionage) risks and cyber risks.

Failure to comply with the sanction rules constitutes a criminal offence. Violations can also involve reputational risks for universities or individual researchers. A proper assessment of the relevant sanction legislation is therefore crucial.

**Export control and dual use guidelines**

Export controls are intended to restrict the export and communication of sensitive technology and strategic goods. Sometimes research or a product is useful for both civil and military applications. This is then called ‘dual use’. An example would be research on carbon, which is used for wind turbine blades and bicycle helmets, but also for military drones. Encryption software is useful for preventing data theft, but it can also be used in a military context.

In order to limit the proliferation risk, dual-use goods, software and technical knowledge are not exported to certain countries, entities and individuals, in accordance with the obligations imposed by the government. Export control regulation is binding, also for our sector. Violations are subject to sanctions under the Economic Offences Act. To export dual-use goods, software or technical knowledge to other countries, it is necessary to apply for an export licence. In May 2021, the new ‘EU Regulation for Export Controls of Dual-Use Goods’ was adopted by the Council of the European Union. This regulation includes a greater focus on cyber and surveillance technologies that can be used for human rights violations outside the EU.

Surveys show that some universities are currently monitoring how this new legislation affects academic freedom and what impact this has on education and research.

**National**

**Missile Technology Control Regime (MTCR)**

The Dutch government is increasingly concerned about Iran’s ballistic missile programme and has therefore enhanced its monitoring of students and researchers who may have a link with Iran's ballistic missile programme. EU Iran Sanctions Regulation 267/2012 provides the legal basis for this action. To carry out this monitoring, an assessment framework has been established that allows for the screening of all students and researchers who are currently studying or conducting research within specific areas of education and research, in which knowledge that is relevant to Iran’s ballistic missile programme could be acquired.

---

16 More information can be found here: EU compliance guidance for research involving dual-use items
This list of education and research areas has been drawn up in collaboration with the universities concerned.

**Expertise and advisory service desk for knowledge security**

The Letter to Parliament does not yet specify the exact details of this national service desk; this will happen later in 2021. Given the name, we expect it to have mainly an advisory and supporting role, possibly identifying risks or enforcing measures in acute situations.

**Universities**

Executive Boards develop guidelines for knowledge security, implement procedures and codes of conduct, and monitor compliance. Researchers and departments comply with codes of conduct and integrity, and identify and address issues relating to knowledge security. This framework therefore builds on the Netherlands Code of Conduct for Research Integrity and the Dutch Universities Governance Code, specifically the following passages:

**Netherlands Code of Conduct for Research Integrity:**
- ‘Institutions provide a working environment that promotes and safeguards good research practices. They ensure that researchers can work in a safe, inclusive and open environment, where they feel responsible and accountable, can share concerns about dilemmas and can discuss errors made without fearing the consequences (“blame-free reporting”). These obligations on the part of institutions are duties of care.’
- ‘Ensure compliance with all relevant statutory regulations, codes of conduct, instructions and protocols.’

**Dutch Universities Governance Code:**
- ‘The university upholds values linked to its social mission. The university promotes an open culture in which any topic can be discussed and in which executives, staff and students feel free to hold each other to account. That culture is disseminated within and outside the organisation.’
- ‘The university promotes the creation of a safe environment in which students and staff can thrive and develop professionally.’

There are unfree countries where knowledge institutions are under the direct rule of the authorities. If a collaboration partner is a public institution or has close ties to the government, this can affect the content of the collaboration and any future dispute resolution procedures. In such a case, the university should always consider whether all academic values as described in the Netherlands Code of Conduct for Research Integrity can be safeguarded.
To establish a solid structure of checks and balances at universities, the following is necessary:

<table>
<thead>
<tr>
<th>Government</th>
<th>University</th>
</tr>
</thead>
<tbody>
<tr>
<td>- provide an ongoing inventory of countries, companies and degree programmes that the government has identified as risky;</td>
<td>- communicate this (risk) inventory to faculties, programmes and research groups;</td>
</tr>
<tr>
<td>- establish the expertise and advisory service desk for knowledge security to provide information about companies and countries and to share dilemmas concerning collaboration ventures;</td>
<td>- define framework/decision tree with impact areas and associated risk analysis processes. This should indicate which analysis is required for which type of collaboration venture;</td>
</tr>
<tr>
<td>- act as an information point for HR staff on risks related to staff recruitment and student intake;</td>
<td>- develop governance/decision-making structure that specifies which type of collaboration and/or knowledge security risk requires advice or agreement at which level;</td>
</tr>
<tr>
<td>- determine a clear division of tasks and definition of roles for services involved, such as AIVD (Dutch General Intelligence and Security Service), MIVD (Dutch Military Intelligence and Security Service), with regard to screening projects, companies/organisations, individuals and consortia.</td>
<td>- make arrangements for periodic reviews: by whom, when and with what reporting and escalation lines.</td>
</tr>
</tbody>
</table>

Both the Dutch government and universities have a relationship with the EU and other EU and non-EU countries. In addition to education, research and export and trade policy, digital (cyber security) policy is also becoming increasingly relevant to our sector within the EU. In all these areas, measures are being taken that affect knowledge security, as evidenced by the recent tightening of restrictions on Horizon 2020 participation for China and the US.

The following chapter on risk management includes further details on the above process and framework.
Chapter 4
Risk management
Chapter 4
Risk management

Local embedding
As discussed at length earlier, the final responsibility for knowledge security at an institution rests with the Executive Board and the Supervisory Board. The Executive Board will then decide to delegate decision-making powers to one or more bodies within its institution, up to a certain risk level. In this respect, knowledge security is in line with risk management in other security domains. Each institution (and each Executive Board) has different characteristics, profiles and practices that factor into determining the level of risk to be authorised and where that authority will lie.

To assist Executive Boards in this decision, below are sample impact areas and criteria that could be included in an authorisation decision tree. For each of the impact areas selected, the Executive Board can determine who has the authority to decide on which criterion. Once the authorisation has been determined, the elected body follows a more detailed risk process (see below). For each of the sample impact areas, typical stakeholders who can be involved in scoring the impact area are listed.17

---

17 In the majority of cases, scoring the impact area will not require extensive (factual) analysis. In some cases, it is also possible that the stakeholders listed will not be involved.
### Impact areas for knowledge security risk

1. **Scientific/strategic urgency for own institution**
   - Dean/director

2. **Type of collaboration**
   - Dean/director

3. **Values of collaboration** *(e.g. academic, medical-ethical, political, philosophical)*
   - Ethics Committee

4. **Research or education topic**
   - Knowledge Security Advisory Team

5. **Country or countries involved**
   - Knowledge Security Advisory Team

6. **Participating organisations**
   - Knowledge Security Advisory Team

7. **Likelihood of self-censorship** *(academic freedom)* in country/countries or research or educational topic
   - Knowledge Security Advisory Team/Ethics Committee

8. **Reputation due to collaboration**
   - Ethics Committee

9. **Scope of collaboration (in €)**
   - Finances

10. **Duration of collaboration**
    - Finances

11. **Additional institution-specific impact areas**
    - ...

### Parties involved

- Dean/director
- Ethics Committee
- Knowledge Security Advisory Team
- Executive Board
- Faculty Board (or institutional board)

### Executive Board

- Pursuing institutional partnership, making or accepting financial investment
- Conflicts between university values and collaboration
- Topic on export control list
- High-risk country
- High-risk organisation

### Faculty Board (or institutional board)

- Participation in consortium, exchange of researchers and students
- Collaboration is in line with the university’s values
- List of sensitive research topics
- Average risk level (foreign) organisation

### Content of MoU/LoI
- Yes
- Content of MoU/LoI can already cause reputational damage

---

18 When assessing the organisations concerned, it is important to include the organisation’s entity structure in the considerations. For example, a knowledge institution to be assessed could fall into the lowest category as an organisation, but be a subsidiary of a foreign organisation that is affiliated with the government of a risk country in a higher category. In addition, a university’s commercial activities *(e.g. spin-offs)* could also be linked to unfree countries.

19 Memorandum of Understanding / Letter of Intent.
For each case, all impact areas can be ‘filled in’ to show whether it will be necessary to bring the case to the Executive Board. In this example, the decision was made to distinguish between two levels: Executive Board authorisation and Faculty Board authorisation. The Executive Board is free to determine the number of levels, the impact areas and the corresponding criteria.

Knowledge Security Advisory Team

The authority of the Executive Board to make decisions (up to a certain level) on knowledge security issues is centralised and/or decentralised in the university. To support these decisions, we recommend setting up a Knowledge Security Advisory Team as a virtual team. Such a Knowledge Security Advisory Team should be equipped with relevant experts to advise on specific cases. A survey of cases discussed in existing advisory teams has shown that the following are common areas of expertise:

- experts in the field of safety risk management (e.g. integral safety adviser or safety coordinator);
- experts in the field of information security (e.g. information security manager or (C)ISO, (Chief) Information Security Officer);
- experts in the field of international collaboration (e.g. (senior) policy advisor).

Depending on the case, additional experts may need to be consulted. These could include (independent) experts in the field of:

- research topic;
- countries or regions concerned;
- research methodology;
- HR;
- valorisation;
- data (e.g. Research Data Officer);
- privacy & ethics;
- intelligence & security;
- contracting (legal affairs/purchasing);
- contact person for the (forthcoming) national expertise and advisory service desk for knowledge security.

The survey also shows that explicit earmarking of these additional experts contributes to their involvement and commitment. Finally, and especially for smaller institutions, those responsible should consider whether expertise can be set up in a multi-university context. For example, one university could lend expertise on certain countries or research topics to a Knowledge Security Advisory Team at another university. A shared service for small institutions can also be set up through the IV-HO Platform to organise a process where advisory teams from institutions can learn from each other.
The seniority of the experts involved (especially the core team) is crucial to the complexity of knowledge security cases. Those involved in these cases have a lot at stake and their interests are by definition multidisciplinary. It is strongly recommended to formally decide on the establishment of the Knowledge Security Advisory Team and to give the Advisory Team direct escalation authority to the Executive Board (both solicited and unsolicited). If a university chooses to set up more than one Knowledge Security Advisory Team (e.g. to accommodate the decentralised organisation of the university), it is advisable to appoint one Knowledge Security Contact Person for this service desk.

**Support processes**

In order to support the risk management processes of the authorised body of the line organisation in knowledge security cases, a few supporting processes are essential: an ongoing awareness campaign at the university; an emphasis on the whistleblower policy in relation to knowledge security; and a centralised record of collaborations with partners outside the EU.

**Awareness campaign**

The Letter to Parliament on Knowledge Security states that knowledge institutions’ awareness of knowledge security is still insufficient. An awareness campaign should be set up to raise awareness at all levels and roles, from the Executive Board to individual researchers and from faculties to support services. However, raising awareness is not a one-off exercise: attention to risks diminishes over time, the threat landscape is constantly changing and the influx of new employees (and therefore culture) is high. The goal of raising awareness is to support both the individual responsibility of researchers and departments and the ultimate responsibility of the Executive Board with concrete knowledge about knowledge security. Protecting the university and its staff starts with being aware of the risks involved.

As a rule, the design and content of awareness campaigns will be strongly influenced by the specific research and education topics, current and future collaborations, management philosophy, prevailing culture and numerous other criteria. When designing the campaign, we recommend using media/formats that take into account the intended purpose, as explained below:

- Static formats such as email, posters and e-learning materials are effective ways to inform staff.
- Interactive formats such as dilemma sessions and dialogue sessions are ideal for persuading staff.
- Game-like formats such as simulating an incident or going through a fictitious case are best for instilling behaviour among staff.
For the content, we recommend taking into account the position which staff members are in:

- For Executive Board members, complex multidisciplinary cases (e.g. cases that include contact with the press or national government) are appropriate.
- Researchers benefit more from recognising manifestations of knowledge security cases in their own research area (e.g. self-censorship).
- Support services benefit more from recognising manifestations among the colleagues (e.g. influence) or services (e.g. cyber incidents) they work with.

Awareness of knowledge security requires an accompanying focus on attitude and behavioural aspects. There is a real risk of unfair treatment, exclusion and discrimination of students and staff from high-risk countries. By ensuring that awareness of the risks does not turn into hostile attitudes, and that students and staff are not excluded or treated unfairly, we uphold the academic values of freedom, respect and open academic discussion. These academic values must be exemplified, in research and especially in the training of young researchers and in education in general.

**Whistleblower policy**

All universities already have a whistleblower policy for (anonymously) reporting suspicions of illegal or immoral practices within the university. This includes the knowledge security risks described above. When raising awareness of these risks, the existence and scope of the whistleblowing policy should also be highlighted. Individual employees who have concerns about knowledge security (e.g. in the case of an overly optimistic assessment of a collaboration agreement), should know that they can turn to a confidential adviser to discuss these concerns.

**Register of collaboration partners (from outside the EU)**

Research by the Rathenau Institute shows that not all universities have a clear and unambiguous picture of the collaborations they enter into with partners from outside the EU. This type of overview forms the basis for effective risk management, especially with respect to monitoring and reviewing known risks. Knowledge Security Advisory Teams will need to be involved in the creation and maintenance of such records. The recording of such information should ideally take place centrally: although the Executive Board may delegate decentralised teams, this does not relieve the Executive Board of its ultimate responsibility for this security domain. An Executive Board should always be able to access information about the significant collaborations it enters into, without having to consult the parties involved. The centralised maintenance of such a register also ensures faster response times to any requests made under the Government Information (Public Access) Act.

---


21 This includes collaborations for education, research and valorisation.
It should be noted that collaboration takes many forms and can be interpreted broadly. If a researcher has regular email contact with a colleague on the other side of the world about a common interest, this can be seen as collaboration. Many such collaborations originate from the bottom up and come and go before they crystallise.

Introduction to risk management

In recent years, universities have invested in making their risk management processes more mature. The VSNU, the Netherlands Association of Universities of Applied Sciences and the Ministry of Education, Culture and Science endorse integral safety as a method to move from rule-based to risk-based security policy. At some universities, this has now led to the harmonisation of processes, which in regulated sectors is called enterprise risk management: an organisation-wide, standardised risk management structure that is often supervised by an independent body (e.g. a risk committee). For universities, this generally means that risk management takes place both in the veins of the organisation (in the faculties and service units) and at a central level. Decentralised risks roll up to the central management structure, creating an integrated risk picture. This ensures that risk management focuses on strategic, tactical and operational risks (what prevents us from realising our vision, strategy and policy plans?), while also paying attention to so-called upside risks (what is the risk of not doing something?).

This puts the Executive Board and Supervisory Board in a better position to protect the university, its interests, its staff and society. A well-functioning risk management process underpins and legitimises the choices made by the Executive Board.

Knowledge security will have to be incorporated within the existing risk management processes. It can therefore hitch a lift on the maturity of the existing processes. Furthermore, because knowledge security is such a multidisciplinary risk area, comprehensive organisation of security risk management is a crucial condition for the successful implementation of this framework. Examples include (also based on the Letter to Parliament):

- access to physical areas with sensitive technology;
- pre-employment screening of staff for high-risk subjects/topics;
- procurement of advanced computer systems from high-risk countries;
- assessment of external financing;
- dealing with insider threat risks posed by employees;
- responding to reports in accordance with the whistleblower policy.

---

The examples show that risk management has two tracks: a continuous risk management process and ad-hoc activities (risk analyses). For both tracks, the same process of risk identification, risk assessment, risk response and risk monitoring can generally be followed. To support these processes effectively, a set-up and maintenance process (Deming’s ‘Plan-Do-Check-Act’ cycle) is needed. This process helps the individual activities and tracks to run smoothly, and typically includes:
- a description of the risk management process and steps, including roles and responsibilities;
- an agreed risk terminology, for example in the form of a risk table or a business impact reference table;
- risk categories with the corresponding risk tolerance;
- a link to staff awareness processes for the various risk areas;
- a standardised approach and template to identify risks, including ‘trigger lists’;
- a standardised approach and template to assess risks based on impact and likelihood;
- a standardised approach to choosing a risk response;
- a risk register\(^{23}\) to track and monitor residual risks and measures;
- an evaluation system to assess the effectiveness of the entire risk management process and to identify areas for improvement.

**Due diligence / preliminary investigation**

One of the ad-hoc processes as part of risk management is carrying out due diligence, or careful preliminary investigation of partnerships. There are two natural moments when such a process can be started: prior to a new collaboration and when extending or renewing a collaboration. Applying this risk management process to ongoing collaborations requires a significant investment, especially at large universities. It is therefore wise to only examine existing partnerships if there is a high knowledge security risk. For example, in the case of collaboration with high-risk countries, an abbreviated due diligence process can be carried out every two years.

Knowledge security is one of the many topics of interest in a due diligence process (alongside reputation, scientific integrity, finance, governance etc.). The risks to be assessed can be identified, weighted and evaluated using the generic risk management process for knowledge security. The Knowledge Security Advisory Team can be consulted in this regard. The decision to pursue a partnership (after taking additional measures or otherwise) lies with the line organisation and must be carefully considered based on – although not exclusively – knowledge security.

\(^{23}\) Note that this is an institution-wide risk register, and not just one for knowledge security.
**Risk identification**

Knowledge security should be included as part of the regular risk identification process. The complexity of these risks requires the explicit involvement of knowledge security expertise (e.g., the Knowledge Security Advisory Team) in addition to regular risk managers. Risk identification can then be effectively carried out by using so-called ‘trigger lists’ for aspects of knowledge security. These lists can be used to remind individuals involved in the process of developments that are taking place, or cases that may be important.

Examples of trigger lists to support the process include lists of:
- high-risk or otherwise unfree countries;
- research and education topics that are sensitive or appear on export control lists;
- incidents at the university itself or a broader overview from sources such as the national service desk, the intelligence and security services, umbrella organisations or the media;
- departments in order to periodically highlight developments of these departments in the process;
- recent geopolitical and technological developments that are relevant to the university.

As an input for risk identification, the following can also be included:
- reports from the whistleblower policy;
- reports from the national service desk, the Knowledge Security Advisory Team or other relevant reports;
- incidents from the past;
- new partnerships;
- complete list of partnerships.

**Risk assessment**

The concepts of probability and impact can be used to assess risks in order to determine how large a risk is for the institution. Many universities work with standardised impact categories and risk terminology, which makes risk assessment much easier. It can also help to take a scenario-based approach in cases of identified risks that are difficult to assess. However, the current impact categories may not fully capture the impact of knowledge security.

For your consideration, here are some (detailed) examples of impact types that could deserve a place among the current impact categories. These concern the impact on:
- academic freedom (being allowed to publish or speak about one’s work);
- staff values (equal treatment regardless of gender, sexuality or personal beliefs);
- the physical and intellectual freedom of staff members;
- the innovative capacity of the Netherlands.
Risk response

In line with standard risk management processes, a response to assessed risks comes next. The response is usually based on the university’s risk tolerance. Standard responses include:

- Risk acceptance. It is crucial to record the details in a risk register, including the name of the risk owner and end date for the current risk acceptance.
- Taking measures. It is crucial to record the details in a risk register, including measures taken and how they support the transition from an inherent risk to a residual risk.
- Avoiding the risk. The decision to avoid the risk can influence future risk management, and recording the details can be helpful in this regard.
- Sharing the risk. Relatively unusual, but universities could share the risk with other (education/research) institutions, the government or even an insurer.

Risk monitoring

A solid risk management process monitors whether residual risks change after the risk response to the identified and assessed risks. Change in residual risk can occur due to a change in the underlying risk (i.e. a change in likelihood and impact) or due to a change in the effectiveness of the risk response (e.g. because the measures prove ineffective, or the risk acceptance period expires). For this process, risk monitoring utilises the risk register, which contains the following details at minimum: the inherent risk, the risk response, the residual risk and the risk owner. Periodic reviews are conducted to determine whether relevant changes have taken place, after which risk identification, assessment and response are reconsidered.

Transition period

For universities that have not yet integrated the risk area of knowledge security into their risk management processes, a transition period applies. The transition period consists of a number of phases, some of which could be carried out in parallel.

1. **Establishment of Knowledge Security Advisory Team**: the crucial first step is the establishment of the Advisory Team. As soon as the other phases start, the Advisory Team will be asked to take on coordinating activities and provide advice on current issues.
2. **Creation of decision tree for impact areas and knowledge security authorisations**: once the Advisory Team has been established, we recommend setting up the outer guardrails for knowledge security via the decision tree for impact areas and mandating. These guardrails guide the subsequent phases and put the Advisory Team into position.
3. **Knowledge security awareness campaign for the Executive Board, deans and directors**: once the guardrails and the Advisory Team are in place, the first cases can be presented. Initially, these cases will likely only concern new international partnerships or those up for extension, or other existing situations that are relevant to knowledge security.
4. **Embedding of knowledge security in existing risk management processes**: once the Advisory Team has conducted trial runs with international partnerships, the risk area of knowledge security can be more broadly embedded in existing risk management processes.

5. **Awareness campaign for departments, researchers and service units**: in parallel to embedding knowledge security in existing risk management processes, this risk area can be further brought to the attention of departments, researchers and service units through a broader awareness campaign. This awareness campaign can draw on cases from the previous phases.

6. **Embedding in integral security**: finally, knowledge security will gradually become embedded within integral safety. The areas of overlap of knowledge security are as diverse as those of integral security. In the spirit of this framework, successful knowledge security policies ultimately cover all policy areas. Strengthening these policies makes all the links in the chain stronger.

An analysis of universities that have already begun focusing on the risk area of knowledge security shows that the multidisciplinary importance of the risk area does not require the appointment of a specific knowledge security advisor, but rather the creation of a (virtual) team which brings together various fields of expertise. Effective handling of the risk area of knowledge security requires capacity. The capacity required will vary from university to university in each phase of the transition. To deal with this uncertainty, it may be wise to initially work with project capacity. When the required capacity can be estimated more accurately, permanent structures can follow.
Appendices
Estimation of time spent

As an example, the capacity estimate of the Advisory Team can be calculated based on the number of cases to be assessed. To illustrate, we will use a standard normal distribution below to calculate this, specifically looking at the distribution of collaborations to be assessed according to their risk to knowledge security. The expectation is that many of the collaborations will not be submitted to the Advisory Team after going through the decision tree (all to μ+σ: 84.1%). Of the collaborations to be assessed (15.9% of total), we expect the first 13.6 percentage points to be consultations of about one hour. The next 2.1 percentage points concern relatively simple cases of 2½ hours per adviser (totalling one workday) and the last 0.1 percentage points represent deeper analysis of two days per adviser (totalling six workdays). This would mean that for every 5,000 collaborations, about 1 FTE is needed for the Knowledge Security Advisory Team.

![Normal distribution of knowledge security cases according to risk](image)

**Figure 1. Normal distribution of knowledge security cases according to risk**

<table>
<thead>
<tr>
<th>Part of distribution</th>
<th>Percentage of collaborations</th>
<th>Time spent by Knowledge Security Advisory Team per case</th>
<th>Days per 5,000 collaborations</th>
<th>Form of involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to μ+σ</td>
<td>84.1%</td>
<td>-</td>
<td>-</td>
<td>Knowledge Security Advisory Team not involved</td>
</tr>
<tr>
<td>σ to 2σ</td>
<td>13.6%</td>
<td>1 hour</td>
<td>680 hours</td>
<td>Consultation (one hour)</td>
</tr>
<tr>
<td>2σ to 3σ</td>
<td>2.1%</td>
<td>1 day</td>
<td>840 hours</td>
<td>Analysis &amp; advice</td>
</tr>
<tr>
<td>3σ and beyond</td>
<td>0.1%</td>
<td>6 days</td>
<td>240 hours</td>
<td>Comprehensive analysis</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>1,760 hours</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 2. Example of time spent by Knowledge Security Advisory Team per 5,000 collaborations*

24 There is no scientific basis for assuming that knowledge security cases will be normally distributed according to risk. This example is for illustration purposes only.
## Participants Workgroup

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>University</th>
</tr>
</thead>
<tbody>
<tr>
<td>Floor van der Heijden</td>
<td>Chair</td>
<td>TU/e</td>
</tr>
<tr>
<td>Anouk Tso</td>
<td>UPI</td>
<td>UvA</td>
</tr>
<tr>
<td>Daria Ratsiborinskaya</td>
<td>UPI</td>
<td>EUR</td>
</tr>
<tr>
<td>Rogier Ragetlie</td>
<td>IV</td>
<td>EUR</td>
</tr>
<tr>
<td>Leo Harskamp</td>
<td>IV</td>
<td>LEI</td>
</tr>
<tr>
<td>Yoni Shem Tov</td>
<td>IV</td>
<td>VU</td>
</tr>
<tr>
<td>Mireille van Emmerik</td>
<td>IV</td>
<td>UM</td>
</tr>
<tr>
<td>Raoul Vernede</td>
<td>UCISO</td>
<td>UU</td>
</tr>
<tr>
<td>Niek Brunsveld</td>
<td>AOV</td>
<td>UvA</td>
</tr>
<tr>
<td>Willem-Rutger van Dijk</td>
<td>AOV</td>
<td>TuD</td>
</tr>
<tr>
<td>Marieke Wagenaar</td>
<td>AOV</td>
<td>RUG</td>
</tr>
<tr>
<td>Mark Kas</td>
<td>AOV</td>
<td>RUG</td>
</tr>
<tr>
<td>Irna van der Molen</td>
<td>AOV</td>
<td>UT</td>
</tr>
<tr>
<td>Frans Pingen</td>
<td>AOV</td>
<td>WUR</td>
</tr>
<tr>
<td>Harry Steinbusch</td>
<td>China Netwerk</td>
<td>X</td>
</tr>
<tr>
<td>Lisa Gorter</td>
<td>Secretaris</td>
<td>VSNU</td>
</tr>
<tr>
<td>Anno Bunnik</td>
<td>Adviseur</td>
<td>VSNU</td>
</tr>
<tr>
<td>Jascha van Hoorn</td>
<td>Adviseur</td>
<td>VSNU</td>
</tr>
<tr>
<td>Willemijn Lamet</td>
<td>Adviseur</td>
<td>VSNU</td>
</tr>
<tr>
<td>Martijn Verwegen</td>
<td>Domeinleider</td>
<td>VSNU</td>
</tr>
</tbody>
</table>

Vertaling ontbreekt