Capability Maturity Model *Knowledge Security*

19 April 2024

Universities *of*
The Netherlands

Colophon

This is a publication of
Universities of the Netherlands
PO Box 13739
2501 ES The Hague

www.universiteitenvannederland.nl

Design: Haagsblauw

Content

Introduction

Despite being a relatively new concern with a national approach presented at the end of 2020, knowledge security[1] has been recognized as a relevant challenge for the Dutch (and European) scientific community. This necessitates the formulation of new policies that are both precise and proportional, ensuring that the Dutch scientific system remains *as open as possible, as closed as necessary*.[2]

In January 2022 the Dutch government published the National Knowledge Security Guidelines, with input from UNL, VH, NWO, KNAW, NFU and the TO2-federation.[3] These guidelines delineate the definition and relevance of knowledge security, and explain key roles, considerations and practices in crafting such policies. The Dutch universities/UNL have taken the initiative to develop a *Capability Maturity Model*.[4]

The capability maturity model is developed by the universities themselves as an instrument within the partnership of the Universities of the Netherlands (UNL):

a. to support universities in designing and implementing their knowledge security policies,
b. to internally assess the maturity level for each specific topic and the desired maturity level, and
c. to enable an internal strategy and planning towards the desired maturity level;
d. To further improve the alignment of
e. universities' knowledge security policies in terms of the used concepts, and offer an outline of topics.

The model is explicitly not designed as a tool for external audits of knowledge security policies. Such audits would require other maturity levels, focusing more on specific requirements regarding the content of knowledge security policies. This particular aspect has not been included in this model, it focuses on the policy process instead of the policy content.

This introduction provides a brief overview of how the model can be utilized. The table on the next page provides an overview of the maturity levels.

As the National Guidelines advise, it is important to consider the diversity and differences in risk profiles between institutions. When utilizing the model, it is important to assess per area which level is desirable for one's own university. The model itself does not prescribe the optimal level for a university. For this reason, the following considerations should be taken into account when scoring the capability maturity model:

- The necessary capability maturity level depends on the *risk profile of the institution*.
  This capability maturity model is positioned to facilitate internal discussions on the aspired capability maturity levels. Conducting an internal risk assessment to assess the risk profile can help to make this determination.

[1] Various concepts are used for 'knowledge security'. On the European level, 'research security' is more common, while 'knowledge security' or 'kennisveiligheid' are more prevalent in the Netherlands. 'Knowledge safety' is also used as synonym to the concept in the Netherlands.

[2] rijksoverheid.nl

[3] english.loketkennisveiligheid.nl

[4] Based on: Surfaudit. Volwassenheidsmodel informatiebeveiliging HO v. 2.0; Kader kennisveiligheid universiteiten (VSNU, 2021); National knowledge security guidelines: secure international cooperation (Rijksoverheid, UNL, KNAW, VH, NFU, TO2 federatie, NWO, 2022); Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (European Commission, 2021) and Tackling R&I Foreign Interference. Staff working document (European Commission, Directorate-General for Research and Innovation, 2022).

Level	Label	Properties
1	**Initial**	Measures are not, or only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.
2	**Repeatable**	Measures are in place and executed in a structured and consistent, but informal, manner.
3	**Defined**	Measures are documented and executed in a structured and formal manner. Execution of measures can be proven, is tested and effective. Periodic reporting (e.g. in annual reports or at meetings) provide input to strategic decisions in relation to knowledge security.
4	**Managed and measurable**	The effectiveness of measures is periodically assessed by the university and improved when necessary. This is documented. Periodic evaluations (e.g. in annual reports or at meetings) report on the effectiveness of knowledge security policy and implementation.
5	**Continuous improvement**	A university wide knowledge security programme provides continuous and effective strategic control and risk issues resolution, e.g. through a PDCA cycle.

- The levels are defined on a general level. This implies that users of the model must consider *how the levels can be operationalized to fit their individual contexts*. It is possible to partially meet the properties of a certain level. In such a case you might score your institution as between two levels.
- *Periodic reporting* at levels 3 and 4 are a means to ensure management and other stakeholders remain informed. This reporting can be fulfilled in various ways, such as reporting during meetings, workshops, (annual) reports, infographics or dashboards. The different topics of the capability maturity model can be reported simultaneously and do not imply separate reporting mechanisms per area.
- *Evaluating and improving* at levels 4 and 5 are necessary for a learning approach. Similar to periodic reporting, the format for such evaluations can be diverse, ranging from a presentation followed by discussion and reporting of this discussion, to an evaluation that is based on a range of interviews or surveys.

This capability maturity model follows the Chapters of the National Knowledge Security Guidelines.
The authority to modify the model is solely reserved to UNL.

1. Protection of academic values

The National Guidelines summarize the following advices in relation to academic values:

- Core academic values, like **academic freedom** and **research integrity**, constitute the foundation of higher education and science in the Netherlands.
- These values also play a role in activities **with foreign partners**. They provide guidance for and during international collaborations. Foreign (guest-) **researchers and lecturers** are required to subscribe to and abide by the code of conduct, similar to Dutch colleagues.

Academic values

Area	Protecting core academic values
Description	Core values, such as academic freedom and research integrity
Ambition	Knowledge security measures are in balance with core academic values, such as academic freedom and research integrity. By incorporating academic values in the core values of the university, the university expresses commitment and provides guidance.
Level 1: initial	• Individual staff members refer to the balance between these core values and knowledge security measures on an ad-hoc basis.
Level 2: repeatable	• Relevant staff have (partially) described some situations, in which knowledge security measures can have an effect on these core academic values or vice-versa.
Level 3: defined	• The core academic values provide additional guidance to relevant staff in the implementation of the policy on knowledge security. • Complex dilemma's where knowledge security measures might affect core academic values (or vice-versa) are discussed with relevant staff.
Level 4: managed and measurable	• The university periodically evaluates whether its knowledge security measures are in balance with the core values, and improves its measures based on the evaluation. • Best practices on knowledge security in relation to core values are documented and communicated.
Level 5: continuous improvement	• Complex dilemma's (level 3) and best practices (level 4) provide input for training and awareness activities to encourage a learning approach and continuous improvement. • Alignment between knowledge security measures and core values is evaluated and improved (if needed) in a cyclical process.
Source / reference	National Knowledge Security Guidelines (2022), Tackling R&I foreign interference (2022).

Open Science

The National Guidelines summarize the following advices in relation to Open Science:

- **Open science** has the ambition to make publicly financed research output accessible for all. This is the norm in Europe. There may, however, be reasons to depart from dissemination, for example for the protection of national security. Make clear agreements in advance to avoid tension between striving for 'open as possible' and taking legitimate protective measures.

Area	Protecting core academic values
Description	Open Science
Ambition	Open science and knowledge security are aligned and staff is equipped to ensure research is as open as possible, as closed as necessary.
Level 1: initial	• Some open science advocates, data stewards and other relevant staff members are aware of knowledge security concerns in relation to open science practices. • Open science advocates, data stewards and other relevant staff members have informal contact with knowledge security staff on an ad-hoc basis.
Level 2: repeatable	• Open science policies and procedures describe both the ambition to be as open as possible, and to be as closed as necessary. • Open Science advocates, data stewards and other relevant staff are familiar with procedures and tools that can be used for the protection of data.
Level 3: defined	• Open science procedures (such as data management plans) refer to knowledge security where and when relevant. • Knowledge security procedures refer to open science when and where relevant.
Level 4: managed and measurable	• Technical, legal and/or administrative support is available to enable the protection of data and research results. • The balance between knowledge security and open science is periodically evaluated, reported and improved (if needed). • Best practices in relation to 'as open as possible, as closed as necessary' are documented and communicated.
Level 5: continuous improvement	• The alignment between knowledge security policies and open science procedures is evaluated, reported and improved (if needed) in a cyclical process. • Best practices (from level 4) are included in training and awareness activities to encourage a learning approach for continuous improvement
Source / reference	Tackling R&I Foreign Interference (2022), Chapter 1.5

Ethics

The National Guidelines summarize the following advices in relation to ethics:

- **Ethical dilemmas** can play a role in international cooperation. It is recommended to have an ethics committee for advice on international cooperation or projects that involve ethical dilemmas other than research integrity, such as the potentially unethical application of results, cooperation with military organisations, or with partners from countries where fundamental rights or international law are not respected. In the table below, these are here referred to as 'ethical dilemma's other than research integrity'.

Area	Protecting core academic values
Description	Ethics
Ambition	Regular research ethics are aligned with knowledge security concerns, specifically ethical issues other than research integrity.
Level 1: initial	• University ethics committee(s) are aware that ethical issues may arise other than research integrity.
Level 2: repeatable	• The ethical reviews sometimes include ethical dilemmas other than research integrity.
Level 3: defined	• The ethics policy allows for reviewing ethical dilemmas other than research integrity. • The respective roles of ethics committee(s) and knowledge security staff are discussed and mutually agreed upon.
Level 4: managed and measurable	• The alignment between knowledge security procedures and the ethical reviewing procedures are periodically evaluated and improved (if needed). • Periodic reporting to higher management includes an evaluation of the alignment of knowledge security procedures and ethical reviewing procedures.
Level 5: continuous improvement	• The alignment between knowledge security and ethical reviewing procedures is continuously evaluated and improved (if needed) in a cyclical process. • Ethical dilemmas other than research integrity are included in training and awareness raising activities.
Source / reference	National Knowledge Security Guidelines (2022)

Inclusiveness and non-discrimination

- Especially in a subject such as knowledge security, in which threat analyses and risk profiles play an important role, there is a danger that the approach will 'go too far' and lead to forms of arbitrary exclusion, suspicion and discrimination. This must be avoided at all costs.
- Have an open conversation about this within your institution and always take signals about this seriously.
- To avoid exclusion, stigmatisation, and discrimination in relation to knowledge security, please visit the Commission's staff working document on *Tackling R&I foreign interference* (2022).

Area	Protecting core academic values
Description	Inclusiveness and non-discrimination
Ambition	Knowledge security and export control measures are designed to ensure inclusiveness and non-discrimination.
Level 1: initial	Knowledge security staff is aware that negative effects of knowledge security measures may emerge such as exclusion, stigmatisation, or discrimination.
Level 2: repeatable	Knowledge security staff have (partially) described risks of exclusion, stigmatisation, and discrimination from knowledge security measures and how to mitigate these risks.
Level 3: defined	Knowledge security policy explicitly state principles to ensure inclusivity and non-discrimination.
Level 4: managed and measurable	The university periodically evaluates whether knowledge security measures may lead to exclusion, stigmatisation or discrimination and how to mitigate this. Periodic reporting to higher management on knowledge security include illustrations of exclusion or discrimination if and when these occurred.
Level 5: continuous improvement	When measures were indeed taken to mitigate such effects, these are evaluated and improved (if needed) in a cyclical process. Illustrations of discrimination, stigmatisation, and exclusion – and mitigating measures - are included in training and awareness raising activities
Source / reference	Oberon & Dialogic (2023). Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek. Sectorbeeld universiteiten. Rijksoverheid.

2. Governance and policy framework

Although some elements of risk governance and the processes are included under the heading 'risk management' in the National Guidelines, 'governance and policy implementation' are not addressed in a separate chapter. Given its importance, it is added here as a separate chapter, in line with the recommendations from the VSNU framework for knowledge security (2021) and the Recommendations EU (2021/1700).

Governance, responsibilities, and process

The National Guidelines summarize the following advices in relation to governance and policy framework:

- Risk management starts with the appointment of a **portfolio holder at board level** and the establishment of a **Knowledge Security Advisory Team** consisting of experts with relevant expertise to assist the portfolio holder.
- It is advisable to **regulate a number of standard processes at the central level**. Depending on the level of risk, stricter risk analyses may be needed, and decision-making should be taken at a higher, more central level.

Area	Governance and policy framework
Description	Governance, responsibilities, and processes
Ambition	Knowledge security responsibilities are assigned to roles and levels within the university at the central and/or faculty levels.
Level 1: initial	• Some staff members of the university are involved with knowledge security on an ad hoc and informal basis.
Level 2: repeatable	• Involvement with knowledge security across roles and levels is partially described and informally conducted.
Level 3: defined	• The Executive Board has assigned a portfolio holder knowledge security. • A knowledge security advisory team (or knowledge security programme team) is formally in place. • Responsibilities are assigned to roles and levels and documented.
Level 4: managed and measurable	• The division of tasks and responsibilities is periodically evaluated, reported and adjusted if necessary. • The composition and functioning of the knowledge security advisory team is periodically evaluated, reported, and adjusted if necessary.
Level 5: continuous improvement	• The division of tasks and responsibilities across roles and levels and the functioning and composition of the knowledge security advisory team is continuously evaluated and improved (if needed) in a cyclical process.
Source / reference	National Knowledge Security Guidelines (2022), chapter 6.

Knowledge security policy

Area	Governance and policy framework
Description	Policy
Ambition	Knowledge security policy, projects and activities are informed by the National Knowledge Security Guidelines and other relevant documents.
Level 1: initial	• Relevant staff conduct knowledge security activities on an ad-hoc basis. • Some knowledge security policy statements are drafted.
Level 2: repeatable	• Activities and processes related to knowledge security are partially described and informally conducted by staff involved with knowledge security.
Level 3: defined	• The university has a knowledge security policy that is approved by higher management. Stakeholders are informed of relevant aspects of the knowledge security policy. • Periodic reporting to higher management include a description of knowledge security activities and processes.
Level 4: managed and measurable	• The knowledge security policy is periodically evaluated and adjusted. • Periodic reporting to higher management includes an evaluation of knowledge security activities and processes.
Level 5: continuous improvement	• The university's knowledge security policy is continuously evaluated and improved (if needed) in a cyclical process.
Source / reference	

Implementation programme

Area	Governance and policy framework
Description	Implementation programme
Ambition	The knowledge security policy is translated into an implementation programme or internal compliance programme with standard operational procedures. Involved staff members have sufficient expertise for implementing and executing knowledge security measures.
Level 1: initial	• Staff involved with knowledge security procedures implement the knowledge security policy on an ad hoc basis. • There are no formal rules concerning compliance or responsibilities.
Level 2: repeatable	• Some elements of an implementation programme are (partially) described and informally conducted by staff involved with knowledge security. • Responsibilities are formalized only for some aspects of knowledge security.
Level 3: defined	• The implementation programme is approved by higher management and responsibilities are assigned. • Involved staff members have sufficient expertise for their role and responsibility in the implementation. • Periodic reporting to higher management includes a description of implementation progress.
Level 4: managed and measurable	• The implementation programme and progress are periodically evaluated and adjusted. • Periodic reporting to higher management includes an evaluation of the implementation programme.
Level 5: continuous improvement	• The implementation programme is continuously evaluated and improved (if needed) in a cyclical process. • The expertise of involved staff required for implementation is periodically assessed within the university, and, if necessary, additional training is provided.
Source / reference	Commission Recommendation (EU) 2021/1700.

3. Legal frameworks for sanctions and export control

The National Guidelines summarize the following advices in relation to legal frameworks for sanctions and export control:[5]

- Legislation and regulations exist to prevent and address threats, and institutions ought to comply. For example, within the European Union, there are strict rules for the export of **dual-use products and technology** that have both military and civil applications.
  They include all forms of transfer, and thus also **by email or cloud services**. In case of uncertainty about whether the export rules apply, a classification request can be submitted to the **Central Import and Export Office** (CDIU).
- In addition, **international sanction regimes** are in place against countries, organisations, and individuals. The current overview is available at www.sanctionsmap.eu. The sanctions against **North Korea** and **Iran** are particularly relevant to knowledge institutions, as they form the foundation for the **enhanced supervision** that applies to a limited number of disciplines.

The Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 aims to support universities and research organisations with the interpretation and implementation of the Dual Use Regulation 2021/821.

The need for a separate program / expertise on export control is dependent on the nature of the university, the international character of the university and whether or not the university is a university of science and technology, a general university with one or more technical departments or a university without research areas covered by the dual use regulations.

[5] Other relevant regulations, not mentioned by the National Guidelines, are: Knowledge embargo Iran in relation to the EU-Iran Sanctieverordening 267/2012 and the Sanctieregeling Noord-Korea 2017. Wet Veiligheidstoets Investeringen, Fusies en Overnames (18 mei 2022); Regeling geavanceerde productieapparatuur voor halfgeleiders (MinBuza.2023.15246-27, 23 juni 2023), European Chips Act 2023, Wet screening kennisveiligheid (in preparation). Other relevant laws are the GDPR and the EU Charter of Fundamental Rights, art. 21 on non-discrimination and the EU Convention on Human Rights. The European regulatory framework is expected to be extended given the package of initiatives under the EU economic security strategy (24 January 2024).

Legal frameworks and supervision

Area	Legal frameworks for sanctions and export control
Description	Legal frameworks
Ambition	Processes and procedures are in place for compliance with sanctions, export control and other relevant regulations.
Level 1: initial	• There is no structural awareness of laws and regulations on sanctions and export control that apply to international cooperation or to the recruitment or hosting of international students, staff or guest-researchers. • Staff members identify relevance of legal frameworks on an ad-hoc basis.
Level 2: repeatable	• There is some awareness of laws and regulations on sanctions and export control that apply to international cooperation. • Relevant staff, such as legal advisors, knowledge security staff, or contract officers, developed a way-of-working to comply with these regulations and communicate this to relevant staff or research groups on a case-by-case basis.
Level 3: defined	• The university has developed a comprehensive set of measures for internal compliance with sanctions and export control. Responsibilities have been assigned to staff to ensure compliance. • Periodic reporting to higher management includes reference to relevant legal frameworks and measures for compliance.
Level 4: managed and measurable	• The university periodically evaluates the procedures to ensure compliance with legal frameworks, and improves this if and when necessary. • Periodic reporting includes dilemmas and/or best practices with regard to (non-) compliance.
Level 5: continuous improvement	• Compliance with screening, sanctions and export control is continuously evaluated and improved (if needed) in a cyclical process. • Training and awareness raising activities include a clarification of the processes and procedures to comply with sanctions and/or export control
Source / reference	National Knowledge Security Guidelines (2022), chapter 4.

4. Risk Assessment

The National Guidelines summarize the following advices in relation to risk analysis:

- The accurate identification of **sensitive domains of knowledge** within an institution is important. Examples include dual-use technologies and knowledge that can be used for unethical purposes.
- It is also important to chart the institution's '**crown jewels**': the domains that pose risks associated with knowledge transfer and within which the institution is an international leader. A brief risk analysis should be conducted for each sensitive domain of knowledge.
- To estimate a country's risk profile, the State Actors Threat Assessment (*Dreigingsbeeld Statelijke Actoren*, NCTV), the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) can be used. In addition, international rankings can be consulted with regard to academic freedom and respect for the rule of law.
- As part of **due diligence**, it is important to examine the background of (security-sensitive) foreign partners or clients.

The topics Risk Assessment and Risk Management are also included in the SURFaudit Toetsingskader. This framework differs from the National Guidelines in the included topics and used concepts. For the development of the Capability Maturity Model for Knowledge Security, the National Guidelines are used to inform the selection and formulation of concepts and topics.

Risk assessment framework

Area	Risk assessment
Description	Risk assessment framework
Ambition	Knowledge security risks are identified for internal purposes to determine actual risk profiles, and relevant researchers and management are offered support and advice on knowledge security measures.
Level 1: initial	• There is no formal risk assessment that prescribes in which cases support and advice on knowledge security is needed. • Relevant staff members identify knowledge security risks on an ad-hoc basis.
Level 2: repeatable	• Relevant risks for knowledge security and corresponding advices are communicated to relevant staff. The communication includes an argumentation to clarify which elements have been relevant in drafting the advice.
Level 3: defined	• A risk assessment procedure and framework is defined. Due diligence is part of this risk assessment methodology. • Periodic reporting to higher management includes a description how the risk assessment methodology provides the information required to draft the advice.
Level 4: managed and measurable	• The university periodically evaluates the risk assessment methodology, and improves this if and when necessary. • Periodic reporting to higher management includes an evaluation of experiences with the risk assessment methodology.
Level 5: continuous improvement	• Support and advice to researchers, support staff and managers is in place and continuously evaluated and improved (if needed) in a cyclical process. • The risk assessment methodology is explained in training and awareness-raising activities.
Source / reference	VSNU Kader Kennisveiligheid, chapter 4; National Knowledge Security Guidelines (2022), chapter 5.

Vulnerability of research facilities

Area	Risk assessment
Description	Vulnerability of research facilities
Ambition	A vulnerability assessment of the most valuable research facilities is performed for internal purposes. Risk mitigating measures are taken to address these vulnerabilities when and where possible. Reporting of the vulnerabilities and measures is treated with confidentiality.
Level 1: initial	• Some faculties, institutes or service departments are aware of knowledge security risks in relation to their research facilities. • Mitigating measures are only proposed when the faculty is confronted with an (urgent) incident.
Level 2: repeatable	• Some knowledge security risks have been identified and described for some of the most valuable research facilities. • Risk mitigating measures are informally described.
Level 3: defined	• Roles and responsibilities are described and communicated. • An internal vulnerability assessment is conducted periodically in terms of knowledge security. These assessments are treated with confidentiality. • Periodic reporting informs higher management of the measures taken. These reports are treated with confidentiality.
Level 4: managed and measurable	• Knowledge security staff periodically discuss the vulnerabilities with managers of the research facilities and jointly propose adjustments if and when necessary. These discussions are treated with confidentiality. • The effects of these measures are periodically reported to higher management. These reports are treated with confidentiality.
Level 5: continuous improvement	• The overviews and the methods of the internal vulnerability assessments are evaluated and improved (if needed) in a cyclical process.
Source / reference	VSNU Kader Kennisveilighei, chapter 4; National Knowledge Security Guidelines (2022), chapter 6.

5. Risk management

The National Guidelines summarize the following advices in relation to both risk governance and risk management under the term ‘risk management’:

- Regulate a number of **standard processes** at the central level. This advice is covered in the area ‘Governance and policy framework’ in this model. Depending on the level of risk, stricter risk analysis may be needed, and decision-making should be taken at a higher, more central level.
- A current, central **overview of security-sensitive partnerships, funding and foreign PhD students and visiting researchers** should be provided at board level. This ‘dashboard’ forms the foundation for effective risk management within the institution. It also provides insight into the cumulative effect of developments that may not seem problematic in isolation.
- Risk management starts with the appointment of a **portfolio holder at board level** and the establishment of a **Knowledge Security Advisory Team** consisting of experts with relevant expertise to assist the portfolio
  older. This advice is covered in the area ‘Governance and policy framework’ in this capability model.
- The creation of an **open security culture** within the organization is essential.
  Employees should have access to counsellors of a wellbeing team to whom they can report signals of security risks. Awareness raising campaigns can be useful in this regard. In this model, awareness is included in the area ‘Training and awareness’.

The topics Risk Assessment and Risk Management are also included in the SURFaudit Toetsingskader. This framework differs from the National Guidelines in the included topics and used concepts. For the development of the Capability Maturity Model for Knowledge Security, the National Guidelines are used to inform the selection and formulation of concepts and topics.

Overview of security-sensitive partnerships, funding, PhD students and visiting scholars

Area	Risk management
Description	Overview of security-sensitive partnerships, funding, PhD students and visiting scholars
Ambition	(Security-sensitive) International multiannual agreements, e.g. MoU's, contracts, LoI's, agreements, are archived and can be retrieved at central level. There is a central system of financial transactions. There is a central registration system for all PHD students and visiting scholars.
Level 1: initial	• (Security-sensitive) International agreements are archived at various levels and available to relevant staff members at faculty level. • Financial transactions are registered and available to relevant staff members at faculty and central level. • PhD students who are employed by the university are registered in the system application for employees.
Level 2: repeatable	• All (security-sensitive) international agreements are stored and can be retrieved at the central or faculty levels. Different systems may be in place. • All financial transactions are stored and can be retrieved at the central or faculty levels. Different systems may be in place. • All PhD students and visiting scholars are registered at the central or faculty levels. Different systems may be in place.
Level 3: defined	• Responsibilities for archiving, registrations and authorizations are assigned for the various systems in place. • An overview of (security-sensitive) international agreements, funding, PhDs and visiting scholars can centrally be retrieved, through different systems. • Periodic reporting to higher management includes an overview of (security-sensitive) international agreements, funding, PhDs and visiting scholars.
Level 4: managed and measurable	• The overviews that are created are/can be used for analytical purposes and strategic decision-making in relation to knowledge security risks. • The procedures for creating overviews of (security-sensitive) partnerships, funding, PhD students and visiting scholars, are periodically evaluated and adjusted if needed.
Level 5: continuous improvement	• The overviews are embedded in a management information system. • The results are used for training and awareness-raising on knowledge security risks within the organisation. • The procedures are evaluated within the university and improved (if needed) in a cyclical process.
Source / reference	EU Recommendation 2021/1700, National Knowledge Security Guidelines (2022), chapter 6.

Management of related safety and security risks

Alignment with the (integral) safety and security policy at the university is important for knowledge security, because of its relation to social safety, physical security, and cybersecurity.

Knowledge institutions have a duty of care towards employees and students when it comes to their social safety. In the case of students and researchers from countries in which fundamental rights are not respected, security can be seriously compromised by the actions of the state of origin.

Area	Alignment with safety and security
Description	Safety and Security
Ambition	Knowledge security policies are aligned with the university's (integral) safety and security policies, in particular on physical security and social safety.
Level 1: initial	• Some staff members involved with safety and security are familiar with knowledge security concerns. • Some staff members involved with knowledge security are familiar with those safety and security concerns that could affect knowledge security.
Level 2: repeatable	• The alignment between knowledge security policies and safety and security policies is described and known to relevant staff members.
Level 3: defined	• Knowledge security policies are aligned with the university's safety and security policy. • The alignment is periodically reported to higher management.
Level 4: managed and measurable	• The alignment between knowledge security and safety and security policies is evaluated and adjusted on a regular basis. • Periodic reports to higher management include an evaluation of the alignment of knowledge security policies with the university's safety and security policies.
Level 5: continuous improvement	• The alignment between knowledge security and safety and security policies is continuously evaluated and improved (if needed) in a cyclical process.
Source / reference	

6. Training and awareness

Training of staff and management

Area	Training and awareness
Description	Training of staff and management
Ambition	(Early career) researchers, management and relevant support staff participate in knowledge security training or education programmes offered by the university.
Level 1: initial	• (Early career) researchers, management and relevant support staff are occasionally informed about knowledge security concerns and measures.
Level 2: repeatable	• Basic information on knowledge security is described and made available. • Informal meetings on knowledge security and relevant measures are given.
Level 3: defined	• The university offers courses on knowledge security to various target groups. • Periodic reporting to higher management includes a description of courses and their participation.
Level 4: managed and measurable	• The design and participation of courses is periodically evaluated and improved (if needed). • Periodic reporting to higher management includes an evaluation of courses and their participation.
Level 5: continuous improvement	• The design and participation of courses is evaluated within the university and improved (if needed) in cyclical processes.
Source / reference	EU Recommendation 2021/1700, section 3.2.3 ; Tackling R&I Foreign Interference, chapter 3; National Knowledge Security Guidelines (2022), section 8.2

Communication plan

Area	Training and awareness
Description	Communication plan
Ambition	Information about knowledge security is communicated and accessible to staff and students.
Level 1: initial	• Information about knowledge security is shared with staff and students when relevant cases occur by staff members involved with knowledge security.
Level 2: repeatable	• Information about knowledge security is described and more broadly shared by staff members involved with knowledge security.
Level 3: defined	• A strategy for communication in relation to knowledge security is in place. • The strategy for communication uses a variety of communication channels. • The tasks for communication of knowledge security information are assigned
Level 4: managed and measurable	• The communication plan and subsequent information, and related tasks are periodically evaluated and improved (if needed). • Periodic reporting to higher management includes an evaluation of the communication on knowledge security.
Level 5: continuous improvement	• The communication plan, information and responsibilities are continuously evaluated within the university and improved (if needed) in cyclical processes.
Source / reference	EU Recommendation 2021/1700I Tackling R&I Foreign InterferenceI National Knowledge Security Guidelines (2022), section 8.2.

Awareness of risks and measures in relation to business trips

The National Guidelines summarize the following advices in relation to business trips:

- It is advisable to develop a visitor protocol to reduce risks during visits to sensitive sites. Conversely, business trips to countries with increased risk profiles (e.g. to participate in conferences) require careful preparation and alertness.

Area	Training and awareness
Description	Business trips
Ambition	Business trips to countries or meetings with increased risk profiles are prepared to safeguard knowledge security risks with appropriate measures (e.g. bringing a laptop without sensitive data or documents on the hard drive).
Level 1: initial	• Researchers and staff visiting countries or meetings with increased risk profiles individually assess knowledge security risks and measures. • There are no formal rules or responsibilities.
Level 2: repeatable	• A protocol for business trips is described and made available.
Level 3: defined	• The protocol for business trips to countries or meetings with increased risk profiles is approved by higher management. • Responsibilities for preparing business trips are assigned, including approval by higher management and support from IT (if necessary). • Periodic reporting to higher management includes a description of the use of the protocol.
Level 4: managed and measurable	• The protocol for business trips to countries or meetings with high-risk profiles is evaluated and improved (if needed) on a regular basis. • Periodic reporting to higher management includes an evaluation of the implementation of the use of the protocol.
Level 5: continuous improvement	• The (use of the) protocol for business trips to countries or meetings with high-risk profiles is continuously evaluated within the university and improved (if needed) in a cyclical process.
Source / reference	National Knowledge Security Guidelines (2022), section 8.3.

7. International partnerships, procurement and contracting

The National Guidelines summarize the following advices in relation to international partnerships, procurement and contracting:

- Cooperation agreements provide a good starting point for considering opportunities and risks. For high-risk collaborations, standard agreement templates may not be sufficient. It would be wise **to bring in legal and security expertise**.
- Once an agreement has been concluded, it would be advisable to evaluate the partnership regularly and address any problems at an early stage. **High-risk agreements should never be renewed automatically**. Within the organisation, it is important to be alerted well before the renewal moment, in order to allow for a critical review of the agreements.

Internationalisation

Area	International partnerships
Description	Internationalisation
Ambition	Knowledge security policies and procedures are aligned with the university's internationalisation strategy.
Level 1: initial	• International office support staff members are familiar with knowledge security concerns.
Level 2: repeatable	• The interfaces between knowledge security policies and the internationalisation strategy are described and known to (some) involved staff members.
Level 3: defined	• The internationalisation strategy is aligned with knowledge security policies.
Level 4: managed and measurable	• The alignment between knowledge security policies and the internationalisation strategy is periodically evaluated and improved (if needed). • Periodic reporting to higher management includes an evaluation of the alignment of knowledge security policies with the university's internationalisation strategy.
Level 5: continuous improvement	• The alignment between knowledge security policies and the internationalisation strategy is evaluated within the university and improved (if needed) in a cyclical process.
Source / reference	

Research collaboration

Area	International partnerships
Description	Research collaboration
Ambition	The procedure for formal international cooperation agreements focusing on research, business development, and/or consultancies includes knowledge security checks and measures.
Level 1: initial	• Support staff members involved in preparing international cooperation agreements are familiar with and include knowledge security concerns. • There are no formal rules or responsibilities.
Level 2: repeatable	• The procedure for preparing international cooperation agreements includes knowledge security measures, including due diligence and export control. • Some staff members involved in preparing international cooperation agreements are familiar with knowledge security measures.
Level 3: defined	• Staff members are assigned responsibilities for implementing knowledge security measures in the procedure for preparing international cooperation agreements. • The procedure and risk assessment form for preparing international cooperation agreements including knowledge security measures are formalized and communicated to involved staff at faculty and central levels. • Periodic reporting to higher management includes a description of relevant international cooperation agreements in which knowledge security measures were taken.
Level 4: managed and measurable	• Knowledge security measures in the procedure for preparing international cooperation agreements are periodically evaluated and adjusted. • Existing international cooperation agreements are periodically reevaluated. • Periodic reporting to higher management includes an evaluation of knowledge security measures in international cooperation.
Level 5: continuous improvement	• Knowledge security measures in international cooperation are continuously evaluated within the university and improved (if needed) in a cyclical process.
Source / reference	EU Recommendations 2021/1700 (export screening); Tackling R&I Foreign Interference; VSNU Kader Kennisveiligheid

Education collaboration

Area	International partnerships
Description	Education collaboration
Ambition	The procedure for formal international cooperation agreements focusing on education includes knowledge security checks and measures.
Level 1: initial	• Support staff involved in preparing international cooperation agreements are familiar with and include knowledge security concerns on an ad-hoc basis. • There are no formal rules or responsibilities.
Level 2: repeatable	• The procedure for preparing international cooperation agreements includes some knowledge security measures, including due diligence. • Staff involved in preparing international cooperation agreements are familiar with the knowledge security measures.
Level 3: defined	• The procedure and risk assessment form for preparing international cooperation agreements including knowledge security measures are formalized. • Staff members are assigned responsibilities for implementing knowledge security measures in the preparation of international cooperation agreements. • Periodic reporting to higher management include a description of relevant international cooperation agreements in which measures were taken.
Level 4: managed and measurable	• Knowledge security measures in the procedure for preparing international cooperation agreements are periodically evaluated, adjusted, and reported. • Periodic reporting to higher management includes an evaluation of knowledge security measures in international cooperation.
Level 5: continuous improvement	• The procedures for knowledge security (measures) in relation to international cooperation is continuously evaluated within the university and improved (if needed) in a cyclical process.
Source / reference	National Knowledge Security Guidelines (2022), chapters 5 & 7; EU Recommendations 2021/1700 (export screening); Tackling R&I Foreign Interference; VSNU Kader Kennisveiligheid, chapter 2

8. Human Resources

The National Guidelines summarize the following advices in relation to the role of human resources policy:

- The **recruitment and selection** of new staff members constitutes a crucial moment for assessing security risks. It is therefore important for HR staff to be conscious of security and to pick up on any signals of increased risk.
- New staff members should receive **information and training** to make them conscious of security. In addition, refresher modules and special training programmes can be provided for visiting researchers from countries with increased risk profiles.

Recruitment

Area	Agreements and contracts
Description	Recruitment
Ambition	The general recruitment process of new staff (for high-risk positions) includes knowledge security measures, such as a (lightweight) background check (e.g. checking previous affiliations).
Level 1: initial	• Some HR individuals and other relevant support staff at the central and/or faculty levels are familiar with and include knowledge security concerns in the general recruitment process. • There are no formal rules or responsibilities.
Level 2: repeatable	• The general recruitment process of new staff at the central level and/or some faculties includes some informal knowledge security measures, such as a (lightweight) background check. • HR staff members are familiar with informal knowledge security measures.
Level 3: defined	• The general screening process of new staff including knowledge security measures is formalized and communicated to HR at (relevant) faculty and central levels. HR staff members are assigned responsibilities. • Recruitment for high-risk positions require screening at higher screening levels. • Periodic reporting to higher management includes a description of the knowledge security measures in the recruitment process.
Level 4: managed and measurable	• Knowledge security measures in the general recruitment process of new staff are periodically evaluated and adjusted and reported to higher management.
Level 5: continuous improvement	• Knowledge security measures in the general recruitment process are continuously evaluated within the university and improved (if needed) in a cyclical process.
Source / reference	National Knowledge Security Guidelines (2022), chapter 8; VSNU Kader Kennisveiligheid Universiteiten, chapters 3 & 4.

9. Cybersecurity

Cybersecurity

Area	Alignment with cybersecurity policies
Description	Cybersecurity
Ambition	Knowledge security policies and procedures are aligned with the university's cybersecurity policies.
Level 1: initial	• Support staff members involved with cybersecurity are familiar with knowledge security concerns. • Sensitive data policies (classification and authorization) include knowledge security concerns on an ad-hoc basis.
Level 2: repeatable	• The interfaces between knowledge security policies and cybersecurity policies are described and known to (some) involved staff members.
Level 3: defined	• Cybersecurity policies are aligned with knowledge security policies. • Sensitive data policies (classification and authorization) include knowledge security concerns and measures.
Level 4: managed and measurable	• The alignment between knowledge security policies and cybersecurity policies is periodically evaluated and improved (if needed). • Periodic reporting to higher management includes an evaluation of the alignment of knowledge security policies with the university's cybersecurity strategy.
Level 5: continuous improvement	• The alignment between knowledge security policies and cybersecurity policies is continuously evaluated within the university and improved (if needed) in a cyclical process.

Source / reference	Normenkader Informatiebeveiliging Hoger Onderwijs 2015;
	Toetsingskader Informatiebeveiliging Hoger onderwijs 2019;
	Surfaudit volwassenheidsmodel informatiebeveiliging HO v. 2.0