UNIVERSITY OF COPENHAGEN

MEMORANDUM

1 MAY 2025

Subject: Systematic security screening at UCPH

RESEARCH AND INFORMATION SECURITY

NØRREGADE 10
DK-1165 COPENHAGEN K

DIR 35 32 57 01
MOB 51 29 84 66

louise.engberg@adm.ku.dk

REF: LE

Procedures for security screenings at UCPH

The security situation for Denmark and the entire Western world has changed significantly over the past decade. The Danish Police Intelligence Service (PET) specifically warns of the risk of illegal acquisition or unwanted knowledge transfer from Danish research institutions to foreign powers. UCPH and other Danish universities need to be better able to identify and protect critical research so that it does not un-intendedly end up in the hands of not like-minded states such as China, Russia or Iran. When the three states are explicitly mentioned in PET's campaign and in the UCPH material, it is based on PET intelligence on which countries, in particular, are attempting to gain illegal access to knowledge from Danish research environments.

In order to increase safety, UCPH, like the other Danish universities, has introduced screening procedures that must be followed regarding all forms of international collaboration involving persons with a *close connection* to one of the risk countries that PET points out especially (currently China, Russia, or Iran) and if they are to work with *critical research*.

As an Iranian, Russian or Chinese citizen, you may be subject to attempts to be influenced by, for example, the country's intelligence services. These regimes may also attempt to acquire knowledge in other ways, including through Danish citizens.

If you have a *close* connection with one of the high-risk countries, and if you engage in research that is of particular interest to the country for strategic, military, or competitive reasons, there will be an increased risk of being subjected, consciously or unconsciously, to influence.

Connection is defined as having either:

- Stayed in a risk country for at least 6 months.
- Have received funding from a risk country
- Has substantially published with researchers in a risky country

Critical research is understood as:

a) Research covered by the EU Recommendation on 10 critical technology areas

b) Research with dual-use potential (included in EU export control rules)

c) Other research of strategic importance for UCPH and GDPR sensitive data.

Critical research is explained in more detail in Section 2.

Research includes the physical place where research takes place, such as laboratories, offices etc., research data, equipment and research results**.**

In order to enhance security and to control who has access to UCPH's research, the Rectorate has decided to introduce systematic screening procedures that must be followed before making any agreements considering visits/collaborations/admittance to registers/ employment/enrolment of a person with a close connection to a risk country. Persons currently staying at UCPH by agreement and who have not previously undergone safety screening will have to be screened according to the same criteria if extension of stay/employment/collaboration is requested.

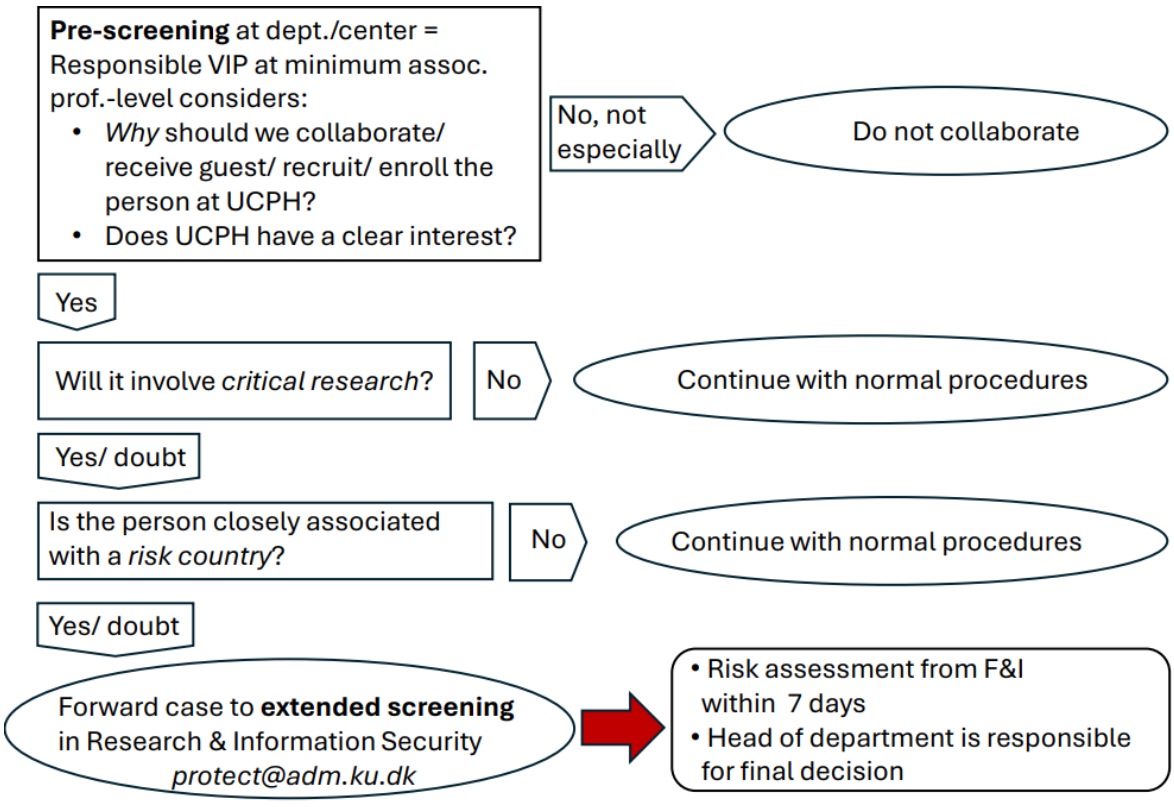
1. **General screening procedure at UCPH** (also outlined in flow chart below):

- *Pre-screening* is carried out at institutional level. *Pre-screening* is a reflection about: Who, what and why:
  Who: Is the person closely associated with a risk country?
  What: Does it involve in any way critical research (or is there doubt)
  Why? Does UCPH have a clear interest in the collaboration? Expected outcome must offset effort and risk.
    - If the pre-screening shows close association with a high risk country, *and* if it is within critical research (or if there are doubts), the case is forwarded to *extended security screening* in the group unit Research & Information Security

(protect@adm.ku.dk) with all available information about the person and the person's background (e.g. CV, publication list, email address, description of the (eventually) critical research, information about financing, previous association with UCPH, etc.).

- F&I (Research and Information Security) aims at responding with *extended security screenings* within 7 days.
  The extended screening is a risk assessment based on the submitted material and open-source information.
- The final decision is made locally after consultation from F&I and is a comprehensive assessment based on a balance of the expected benefits versus risks. The head of department/center is responsible for decision-making and the subsequent handling.
- If F&I recommends not to proceed with collaboration/visit/ hiring, based on an extended screening, and if the head of department/ center makes a decision that goes against the recommendation, the head of department is obliged to inform the dean with an argument for the decision.
- Do not make any decisions or predictions regarding employment before the safety screening has been completed. During a security screening, information that does not appear in a person's CV is regularly revealed.

Screening process at UCPH:



Below it is explained in more detail how the safety screening is handled in different situations.

1.1 Screening of loosely affiliated persons

Persons affiliated with the University of Copenhagen for shorter or longer periods without being employed or enrolled are collectively referred to as "loosely affiliated". These are mainly visiting researchers or PhD students. Loosely affiliated persons refers to persons who must have a UCPH username and access to UCPH's systems or registers/ handed-out key or access card (ADK), regardless of the duration of the stay.

1) ***Pre-screening***
   The host – a UCPH VIP min. at associated professor level – performs the pre-screening. In case of doubt, use in the first place the management string.

2) If a person is to engage with or stay in a research environment with access to critical research (or there are doubts about it) and the person has a connection to China/Iran/Russia ⇒ Extended screening in Research and Information Security (protect@adm.ku.dk).
   The head of department/centre is responsible for decision making and subsequent handling.

1.2 Screening in connection with recruitment & enrolment of PhD students:

HR is incorporating new procedures into recruitment procedures and documents. Until this is in place, a more handheld process is applied locally.

It should be included as footnote in all job listings (in line with GDPR-info) that one as applicant at the University of Copenhagen must be prepared for further screening related to international research collaborations as part of the recruitment process when UCPH considers it appropriate from a holistic consideration.

If the job offer involves access to potentially critical research:

1) Pre-screening at the department upon receipt of applications.
2) Persons associated with a high-risk country who are wanted to be interviewed, all information is forwarded for use for extended screening in Research & Information Security (protect@adm.ku.dk) as soon as possible. F&I aim at responding within 7 days.

1.3 Screening in other situations

Pre-screening and extended screening are also relevant in other situations where UCPH interacts with persons from a risk country, following the same principles as described above. For example, this can be in connection with offers for funding, guest stays, student project participation, delegation visits at UCPH, etc. Research and information security will be pleased to assist with advice and safety assessment in these cases.

---

2. Identification of critical research

Research includes the physical place where research takes place, such as laboratories, offices, etc., research data; equipment used in research, or which is subject to export control rules and research results.

It is important to be clear from the start whether the research is within a critical area, as it can affect the choice of partners, opportunities to seek funds, etc.

Critical research is divided into three groups:

a) Research covered by the EU Recommendation on 10 critical technology areas;
b) Research with dual-use potential (subject to EU export control rules)
c) Other critical research including GDPR-sensitive data

As a basic principle, research will only be regarded as critical if it contains confidential information, huge data set, or knowledge which can be used to influence, destroy, or manipulate public or private systems, and technology or information that has potential to harm national or international strategic or security interests.

Furthermore, research may be critical if it can expose researchers to threats/ harassment from certain groups or if the risk of sabotage is elevated. However, this should be assessed based on the work and experience of individual researchers.

Below are examples of critical research. It shall not be regarded as a full list.

a) Research covered by the EU Recommendation on 10 critical technology areas

The EU has identified 10 technology areas as especially critical due to the possibilities of the technologies, the risk of civil and military fusion (*dual-*

use), and the risk of misuse of the technologies for human rights violations.
General categories:

1. Advanced semiconductors (e.g. microchips)
2. Artificial Intelligence
3. Quantum technologies
4. Biotechnologies
5. Advanced connectivity, navigation and digital technologies
6. Sensor technologies
7. Space technologies
8. Energy technologies
9. Robotics technologies
10. Nanotechnologies

The recommendation of the European Commission is elaborated herein.

b) Research with dual-use potential (subject to EU export control rules)

Specific technologies/products or information/data that are specific enough to be able to produce a given technology/product that can have civilian and military applications.

Part of it is covered by EU export control rules. Specifically, these products fall under the following general categories:

Category 0 Nuclear materials, installations and equipment
Category 1 Special materials and related equipment
Category 2 Material treatment
Category 3 Electronics
Category 4 Computers
Category 5 Telecommunications and 'information security'
Category 6 Sensors and lasers
Category 7 Navigation and aircraft electronics
Category 8 Shipping
Category 9 Aerospace.

The rules for export control are detailed on the Danish Business Authority's website.

The EU checklist is updated annually. You can do a free-text search in the PDF file by pressing Ctrl F and entering words or characteristics of the products you want to investigate in the window that opens. This EU

publication contains the EU list of the research areas with the greatest risk of exposure to *dual use* (pages 38-39) as well as a list of warning signals (pages 42-43).

c) Other critical research and GDPR-sensitive data

- Is there research or data that could be misused to pose a security policy risk if it falls into the wrong hands (e.g. information on critical infrastructure/strategies)?

- Processes NATO classified data classified higher than "For service use"?

- Public services of social importance (e.g. forensic examinations and genomic sequencing)?

- Can loss of confidentiality, integrity, or data availability affect critical infrastructure?

- Is there a potential risk that researchers will not be properly credited or lose their intellectual rights in the broad sense if someone with hostile intentions gets access to the research before it is published?

- Is there research or equipment that supports research that could be used for purposes that could compromise ethics/human rights/protection of personal data if it falls into the wrong hands?

- Are there research areas where it could affect the international reputation of UCPH and/or the researcher and future collaboration and funding opportunities if someone with hostile intentions gets access to the research before it is published?

- Is there any other research where the university has a particular strength that should not be shared for strategic reasons that are not covered by the already mentioned?