RESEARCH SECURITY FRAMEWORK & DUE DILIGENCE PROCESS

I. CONTEXT:

Openness, international cooperation, and academic freedom are at the core of world-class R&I. However, with growing international tensions and the increasing geopolitical relevance of R&I, our researchers can potentially be subjected to risks when collaborating internationally. There are concerns about the potential misuse of European R&I, as well as the possibility of external influences that could compromise the Union's security or undermine its core values and fundamental rights. Foreign interference, that is "activities that are carried out by or on behalf of a foreign actor, which are coercive, covert, deceptive or corrupting and are contrary to the EU's sovereignty, values and interests"[1], is considered a real and growing threat to R&I activities in Europe.

'Research security' refers to anticipating and managing risks such as the undesirable transfer of critical technology, exerting a malign influence on research, and ethical or integrity violations by third countries.

While the newly adopted Council Recommendation of 23 May 2024 on enhancing research security reconfirmed Europe's commitment to openness, it called for a more nuanced approach to how we engage with global partners. The EU recognizes the need to strike a balance between fostering international cooperation while also safeguarding its interests. Therefore, it is crucial, first for the research community to be informed of the risks, and second to be aware of the protective measures available to them. It is important that Irish Higher Education Institutes (HEI) have a degree of research security measures in place so as to continue be seen as competitive and attractive partners in the context of global research collaboration.

The new text outlines several recommendations for member states to strengthen research security. These recommendations include:

- Developing **national strategies**, which may involve creating national guidelines or compiling a list of relevant measures and initiatives.
- Establishing or enhancing **support services** to assist R&I sector participants in managing risks associated with international research collaboration.
- Strengthening **inter-departmental cooperation** within the government.
- Building a **stronger evidence base** to inform research security policy decisions.

Why are Research Performing Organisations (RPOs) at particular risk?

[1] Tackling R&I foreign interference - Publications Office of the EU

According to a briefing by the European Commission[2] RPOs are at risk because:

- Europe's HEIs have a strong record of internationalisation.
- This openness and collaboration have greatly contributed to their success but has simultaneously facilitated foreign interference.
- HEIs are often insufficiently aware of potential threats and have not taken preventive measures.
- Provided the complexity of the threats, it is difficult to tackle these issues in isolation.

It is important to manage these risks while, at the same time, support international cooperation and openness, adhering to the principle '*as open as possible, as closed as necessary'*.

Four areas of attention were cited by the European Commission as especially vulnerable to foreign intervention. They have created a **toolkit**[3] which suggests protective measures RPOs can choose from and tailor to meet their organisation's specific needs.

Area	Protective measures
Values	1. Identify countries and partner institutions where academic freedom is at risk 2. Conduct a vulnerability assessment to understand external pressures on academic freedom and integrity 3. Strengthen commitment to academic freedom and integrity at institutional/ individual levels 4. Continue to cooperate with partners in repressive settings
Governance	1. Publish a Code of Conduct for Foreign Interference 2. Establish a Foreign Interference Committee
Partnerships	1. Develop general prerequisites for implementation of a risk management system 2. Establish a sound procedure for developing robust partnership agreements
Cyber-security	1. Raise awareness of cybersecurity risks 2. Detect and prevent cybersecurity attacks from foreign interference actors 3. Respond to and recover from cybersecurity attacks from foreign interference

The main provisions for RPOs in the Council recommendation according to Department of Further and Higher Education, Research, Innovation and Science (DFHERIS)[4] are:

1. Engaging in the **exchange of information and good practices** and considering resource pooling to make best use of scarce resources and expertise
2. Implementing **internal risk management procedures**, including risk appraisal and due diligence on prospective partners – while minimising the administrative burden
3. **Considering possible risks when entering into R&I agreements/MOUs**
    a. *including key framework conditions such as respect for EU values and fundamental rights, academic freedom and IP*

[2] Slaven MISLJENCEVIC. ERA workshop - foreign interference. 13 January 2023.
[3] European Commission. Tackling R&I foreign interference. Staff working document
[4] Department of Further and Higher Education, Research, Innovation and Science. Enhancing Research Security briefing. October 2024.

   b. *providing for an exit strategy if conditions are not complied with*

4. **Assessing the risks relating to foreign government-sponsored R&I talent programmes** – such as undesirable obligations on beneficiaries – and ensuring they comply with the host's mission and rules
5. **Assigning research security responsibility** at the appropriate organisational levels
6. Investing in dedicated **in-house research security expertise and skills** and facilitating **access to training** programmes
7. Ensuring **full transparency of funding sources and affiliations of research staff** in scientific publications and all other forms of dissemination of research results
8. **Introducing compartmentalisation** (physical and virtual) to ensure access to particularly sensitive data and systems is on a strictly need-to know basis – for online systems, put robust cybersecurity arrangements in place
9. **Assessing the risks related to equipment, labs and research infrastructure** sponsored by or acquired from entities established in or controlled by third countries
10. Preventing all forms of discrimination and stigmatisation (direct and indirect) and **protecting individual safety** – with a particular focus on coercion of diaspora by their home country and other forms of malign influence

DFHERIS are currently undertaking a consultation process to develop national guidelines/supports to augment and support the development of institutional-level guidelines.

II. INSTITUTIONAL APPROACH:

In line with upholding academic freedom and maintaining openness, UCC is committed to continuing to cooperate with partners in third countries including those in repressive settings. As set out in our institutional framework *Belonging at UCC: A Strategic Framework for Equality, Diversity and Inclusion 2025 - 28* UCC is committed to EDI. However, a balance must be struck between fostering cooperation while also safeguarding the interests of UCC and its research community. While it is important not to hinder research progress within UCC, or place undue burden on researchers - particularly at pre-award - adequate checkpoints must be put in place. Additionally, it is crucial to raise awareness of research security considerations across the university. Lastly, it is important to be mindful that some external entities collaborating with UCC may be subject to their own research security restrictions.

In practical terms, UCC will:

- Engage in the exchange of information and good practices and resources with other HEIs, including through the Community of Practice *Higher Education Institutions for Research Security (**HEIRS**)* established in March 2025 which brings together representatives from across HEI research offices.

- Introduce internal risk appraisal and due diligence process for engaging in international cooperation:
    - ***Pre-award stage:*** as appropriate, implement internal risk management procedures, including risk appraisal and due diligence on prospective partners, and assessing the risks relating to foreign government-sponsored funding programmes (including R&I talent programmes) ensuring they comply with UCC's mission and rules.
    - ***Post-award stage:*** as appropriate, assess possible risks when entering R&I agreements/MOUs, including consortium agreements. Such assessment should

consider partner alignment with EU values, fundamental rights, academic freedom and IP and provide for an exit strategy if conditions are not complied with.

    - Concerns related to reciprocity and intellectual property rights-related issues should be addressed in the relevant partnership agreement (that is entered into with the prospective partner).
    - Following the risk appraisal process, and where issues have been identified, a Risk Management Plan should be developed that sets out how risks will be addressed and mitigated.

  - ***Risk registers:*** Research security should be included as a risk on college and research institute risk registers along with the UCC risk register.

In addition:

- Assign responsibility for research security within the organisation, develop awareness-raising activities and training. While oversight sits within *UCC Research*, research security must be a whole of university approach with awareness at all levels, including UCC personnel who engage in research, and heads of functional units. *UCC Research* will liaise with other units, for example OCLA, HR Research, as relevant. Awareness-raising is paramount to safeguarding the interests of UCC and its research community. There are instances where *UCC Research* is not privy to activities that may present a research security risk; for example, non-funded research, ongoing affiliations, researcher engagement in doctoral supervision, talent programmes and staff exchanges. *UCC Research* will continue to work closely with the Office of the Vice President for Global Engagement, to build awareness across UCC, knowledge of the international landscape, and take a consistent institutional approach to engagement and collaboration with global partners.

- Take research security into account when recruiting new research staff. In this context, there are several elements which should be considered (for example nationality, existing and prior affiliations, and the likelihood of being linked to malign actors or influences), while being mindful of staff wellbeing and the risk of discrimination and stigmatisation.

- To protect sensitive knowledge and research facilities, implement physical and virtual safeguards, such as compartmentalisation and robust cybersecurity measures.

- Support the wellbeing of our researchers who find themselves subject to externally applied pressures in this context.

Most importantly, *UCC Research* will act as a central point of contact, supporting researchers with queries in relation to both export control and research security (directed to exportcontrol@ucc.ie). Undertaking a risk assessment with respect to international partners and new researchers is complex. Therefore, UCC personnel are advised to undertake an initial assessment, drawing on an available decision making tool, and reach out to *UCC Research* to seek guidance on scenarios deemed to present a higher risk. Higher risk collaborations will need to be reviewed on a case by case basis.

UCC Personnel who Undertake Research:

- Should be aware of the security risks associated with their research. Certain research domains may present a higher risk (please see resources under IV. TRAINING AND RESOURCES *Identifying Dual-Use Items*).

- Drawing on an available decision making tool, personnel are advised, insofar as possible, to undertake risk appraisal and due diligence on prospective partners before engaging in collaborative research. This extends to due diligence before hiring international research staff from third countries. In this context, there are several elements which should be considered (for example nationality, existing and prior affiliations, and likelihood of being linked to malign actors or influences). Personnel are advised to undertake such assessment being mindful of staff wellbeing and the risk of discrimination and stigmatisation, and recognising the limitations of certain parameters. An assessment should be undertaken by the lead PI and revisited periodically given that circumstances related to research security may change.

- Are advised to undertake necessary training (see **IV. TRAINING AND RESOURCES**).

- Should ensure full transparency of funding sources and affiliations of research staff in scientific publications and all other forms of dissemination of research results.

- Must ensure that they fully comply with the Export Control Internal Compliance Protocol (ICP). Export Control, while representing a component of research security, is provided for in legislation. Applying for and obtaining an export control licence, where required, is mandatory.

Heads of School/Functional Unit:

- Are advised to introduce internal guidance to protect the individual safety, and support the wellbeing, of researchers working in their School/Unit who may be at risk of discrimination and stigmatisation (direct and indirect). This is particularly advisable for researchers from third countries where there is a risk of coercion by their home country and other forms of malign influence.

- Assess the risks related to any equipment, labs and research infrastructures sponsored by or acquired from entities established in or controlled by third countries.

In the majority of cases, prospective partners and new research staff will present no risk to UCC. The above guidance is intended to ensure that the small proportion of higher risk scenarios are brought to the attention of *UCC Research* such that an appropriate decision can be made and/or safeguards put in place where possible. While this framework document and UCC's general approach to research security remains country agnostic, it must be acknowledged that certain countries will present a greater concern at different timepoints in line with international developments. As such, the decision making tool is a living document which will reflect these changes. In general, researchers should be prompted to ask security relevant questions of their research, even if they cannot necessarily answer these questions and ultimately need to seek additional advice from *UCC Research.*

III. DEVELOPING A RISK APPRAISAL PROCESS:

A number of resources are available to guide organisations when undertaking a risk assessment, including Trusted Research | NPSA, which provides a collaboration checklist which can be used by researchers and research offices to determine the level of risk incurred by a collaboration, and the European Commission fact-sheet on risk appraisal which includes a number of questions to be considered under each element. The latter has been drawn on to form the basis of a risk appraisal process at UCC, and used to inform deliberations carried out as part of the internal *UCC Research* SOP described below. Considerations to be addressed in the 'in-take phase' of an international R&I partnership or project.

1. UCC's International Profile:

- What are our vulnerabilities? What are our strengths? Examples to consider include:
  - Where UCC is a scientific leader in a research domain or has exceptional research infrastructure – this makes the institution a potential target.
  - Financial dependencies that could be related to a partnership/project – this makes the institution vulnerable.

2. Research Domain

- Is the partnership/project focussing on a research domain, or does it involve methodology or research infrastructure that would be considered particularly sensitive from a security or ethical/human rights perspective?
- Does partnership/project involve dual-use technology? (see **Identifying Dual-Use Items**)
- Does the partnership/project incorporate a key enabling technology?

3. Profile of the Country of the Partner Organisation

- Does the partnership/project include partners based in or affiliated with third countries with a high-risk profile (examples: flawed rule of law (see WJP Rule of Law Index), aggressive civil-military strategies, limited academic freedom (see Academic Freedom Index)).
- Is the country subject to export sanctions with relevance to R&I (see EU Sanctions Map)
- Is the research domain of particular interest to the country in which the partner is based or to which it is affiliated?
- Is there an explicit government policy to become world leader in the field?

4. Profile of the Partner Organisation

- What do we know about the partner organisation we wish to cooperate with?
- Is the partner organisation linked to the government? Does it have links to the military?
- What is its governance structure? Where does the partner organisation get its funding from?
- Has the partner organisation been involved in any reported/ media covered scandals or security-related incidents?
- What do you know about background and affiliations of the local researchers/staff involved?
- What do you know about the partner organisation's intentions regarding the end-use or application of the research outputs? Is our interest in the collaboration at the same level as the interest from the partner organisation?

If relevant basic information about the prospective partner organisation cannot be found in the public domain, this should raise concerns.

UCC Research Due Diligence Process - Funded Research

The below steps outline the processes undertaken by *UCC Research* in line with the institution's Research Security Framework. These processes serve as current internal controls as part of the relevant risk, captured in the OVPRI Risk Register, for managing risks associated with potential reputational damage to the institution, misuse of University R&I, undermining of UCC's values and mission, and loss of commercial business, due to foreign interference and/or geo-political dynamics.

Pre-Award Phase:

1. Research security is a standing agenda item at monthly OVPRI Research Officer meetings. These meetings present an opportunity to highlight potential leads and risks associated with an potential engagement at an early stage. The focus of scrutiny is informed by current geopolitical priorities.

2. Risk appraisal and due diligence on any foreign-sponsored funding programmes and on prospective partners - including those identified through the Research Officer meetings above - is undertaken by the relevant Research Officer supporting the proposed pre-award engagement.

Post-Award Phase:

3. Risk appraisal and due diligence on prospective partners/engagements is carried out by the relevant Contracts Officer in the course of reviewing/preparing the relevant legal documentation governing the proposed engagement.

4. Risk appraisal and due diligence, where possible, could also occur in the context of ethical approval; for example concerns may be raised by the Coordinator of the University Ethics Committee and Social Research Ethics Committee

Note: *Under GDPR regulations, checks at Pre- and Post-award Phases may only use information available in the public domain and cannot access any legal documents or criminal history records.*

5. If any issues/concerns are identified, a Due Diligence Briefing is provided to the Director of Research Support & Policy for review. The Director then convenes the *UCC Research* External Due Diligence Group (Director of Research Support & Policy (chair), relevant Senior Research Officer, & Post-Award Manager) to discuss engagements which may present a risk to the University. Representatives from OCLA can also be consulted at this point or earlier, where required.

The External Due Diligence Group will evaluate the risk level and make a determination as to whether the benefits of the engagement outweigh the risk, and to define next steps:

One option is to escalate the matter, in consultation with the VP for Research & Innovation, to the University Research Risk Committee (VP for Research & Innovation (chair), Director of Research Support and Policy, Corporate Secretary, Bursar/CFO, and VP for Global Engagement) for further consideration at institutional level.

If a decision is made not to escalate to the University Research Risk Committee, then a Risk Management Plan will be developed that sets out how risk(s) will be addressed and mitigated.

6. The University Research Risk Committee will discuss the escalated risk, along with consequences, and further actions to be taken. There are two determinations that can arise from these discussions:

A. Low Risk Collaborations:

7. The Committee considers the risks (and relevant Risk Management Plan), and makes the decision to proceed with the proposed engagement. Additional, follow-on, actions to include ongoing monitoring of the engagement.

B. High Risk Collaborations:

8. The Committee arrives at a decision that institutional research security cannot be guaranteed, and the proposed engagement should not proceed. Rationale for the decision, and any associated mitigating actions including follow-ups, are captured and shared with relevant stakeholders.

9. Following the process, the decision for each engagement is recorded along with relevant information from the Due Diligence Briefings. Regular reports on the Due Diligence Process (and outcomes) are shared with relevant internal stakeholders as per the OVPRI Risk Management Reporting Process.

The database of due diligence exercises and outcomes is consulted as part of future due diligence checks.

IV. TRAINING AND RESOURCES

Multiple legal frameworks are relevant to research security, including data protection, intellectual property, export control, and national security and investment.

It is important for UCC personnel who are engaged in research to be aware of the relevant policies and procedures, a full list of which can be found here: Research Policies. For example, export control regulations regulate the transfer of listed items (controlled products and materials) to other countries and are in place to prevent knowledge and technology falling into the wrong hands, which could impact our security, regional stability and protection of human rights. Further information and guidance specifically pertaining to export control is available in the ICP. This includes steps to take a post and pre-award.

Training

At minimum, UCC personnel engaged in research are advised to undertake the following training:

- Epigeum Research Integrity Training, which includes a specialist module on export control
- Introductory training on export control Export Controls Training for Researchers

All UCC personnel are advised to undertake Cybersecurity Awareness Training. Note that IT Security also provide several additional resources to staff IT Security - Home

The UK Government's National Technical Authority for Physical and Personnel Protective Security (NPSA) Trusted Research | NPSA hosts a particularly useful collection of resources and guidance, including scenarios (fictional case studies) which suggest individual researcher and institutional level mitigation strategies.

Identifying Dual-Use Items

Dual use items are items that can be used for civil and /or military purposes and which meet certain specified technical standards. This includes the components of these items.

Please see the Export Control Internal Compliance Programme and UCC Guidance Note on Export Control for access to consolidated lists of dual use items, and for further information export control law and how it might apply to activities carried out in UCC.

The Canadian Government has prepared a list of Sensitive Technology Research Areas which includes advanced and emerging technologies that are important to Canadian R&I but may also be of interest to foreign state, state-sponsored, and non-state actors. Although focused on Canada, this list provides a searchable, overview of key technologies which is a useful starting point when determining whether a partnership or project involves sensitive technology. This should be used in conjunction with official dual use list.

Undertaking Due Diligence

Resources to support you to undertake due diligence on a country, organisation or individual:

I. Countries

- EU Sanctions Map
- WJP Rule of Law Index
- Academic Freedom Index

II. Organisations or Individuals

- Government of Canada Named Research Organizations
- Chinese Defence Universities Tracker — ASPI noting this has not been updated regularly for years
- Iran Watch | Tracking Iran's Unconventional Weapon Capabilities
- CSET talent watch CSET Chinese Talent Program Tracker
- OpenCorporates
- Companies House (UK)
- Xapien
- Open Sanctions
- North Data Smart Research
- Trademo (private companies)

V. VERSION CONTROL

Procedure Name	RESEARCH SECURITY FRAMEWORK & DUE DILIGENCE PROCESS
Unit Owner	OVPRI
Version Reference	Version 1.0
Approved by	Director of Research Support and Policy
Effective Date	20.06.25
Review frequency	Every year
Next review date	20.06.26