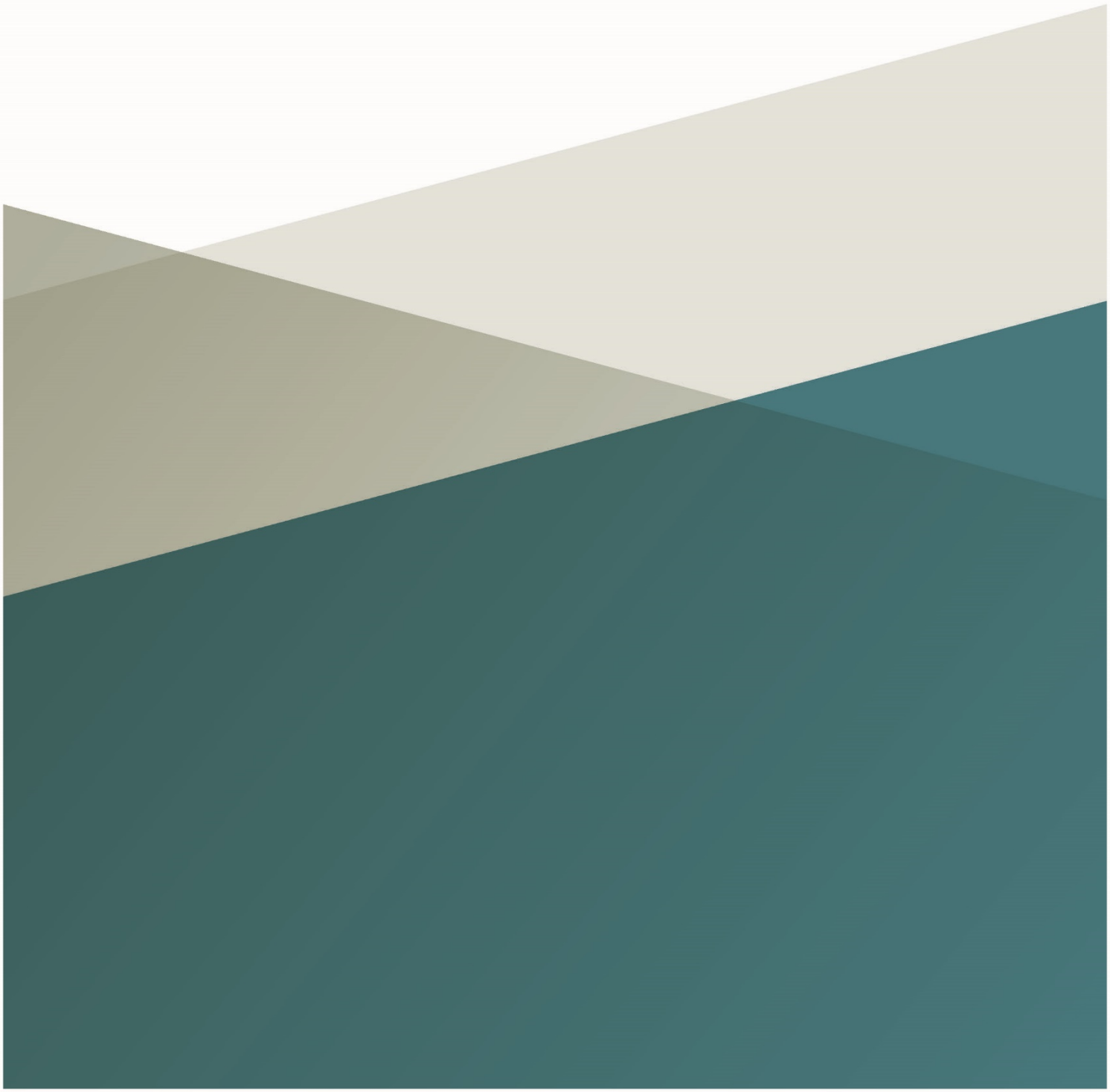
An Roinn Breisoideachais agus Ardoideachais,
Taighde, Nuálaíochta agus Eolaíochta
Department of Further and Higher Education,
Research, Innovation and Science

Research Security Guidelines for Ireland

2026



Contents

1. Scope and Key Definitions **5**

2. Why Research Security Matters **6**

3. Core Principles **7**

4. Roles and Responsibilities **9**

4.1 Research Performing Organisations (RPOs) — Core Institutional Responsibilities 9
4.2 Research Funders — Enabling and Supporting Role 9
4.3 Government — Coordination, Guidance, and Strategic Support 10

5. Key Actions for Research Performing Organisations **12**

6. Implementation Approach **15**

Phase 1: Preparation (6-12 Months) 15
Phase 2: Integration (Ongoing) 15
Phase 3: Monitoring and Evaluation 16

7. International Context and Alignment **17**

8. Review and Updating **18**

Appendices 19

Executive summary

These guidelines establish Ireland's approach to research security, balancing the imperative to protect sensitive knowledge with our commitment to open, international research collaboration, in a proportionate and risk-based manner, and apply to both funded and unfunded research. Research security is a shared national responsibility, with Research Performing Organisations (RPOs), funders, and Government each playing distinct and complementary roles. **Research Performing Organisations (RPOs) have the primary responsibility for research security at institutional level**, with government and funders providing enabling support through guidance, resources, and coordination.

These guidelines are intended as enabling guidance rather than a regulatory or enforcement framework. They do not introduce new obligations, but support institutions in understanding and implementing relevant existing responsibilities in a proportionate manner. Implementation through funder or institutional mechanisms should reflect the same principles of proportionality, risk-based application, and engagement with the research performing sector.

Key Principles: risk management rather than risk avoidance; proportionate responses based on institutional autonomy; clarity of roles and responsibilities; avoidance of bureaucratic complexity that stifles innovation.

1. Scope and Key Definitions

Research security refers to the identification and management of risks associated with international research and innovation collaboration. These risks include undue foreign interference, unwanted transfer of sensitive knowledge or data, misuse of research results, and actions that may undermine academic freedom, institutional integrity, or fundamental values. Research security is an enabling framework that supports open and responsible research by managing risks in a proportionate and context-sensitive manner.

Dual-use research refers to civilian research activities conducted for legitimate scientific, societal or economic purposes that may also have potential applications in security or defence contexts. The presence of dual-use potential does not in itself imply heightened risk, and many areas of high-quality civilian research may involve theoretical or indirect dual-use relevance without creating material security concern; rather, it requires appropriate, proportionate assessment based on the specific nature, sensitivity and intended use of the research[1].

Defence-related research refers to research explicitly commissioned, funded, or directed for military or defence purposes. Such research is governed by distinct legal, policy and funding frameworks and is outside the primary scope of these civilian research security guidelines.

These guidelines apply to civilian research and innovation, including research with potential dual-use characteristics, with implementation expected to be proportionate to the scale, nature, and risk profile of the activity concerned. They are designed to support RPOs in managing risks without discouraging legitimate international collaboration or knowledge creation. The focus is on ***risk management rather than risk avoidance***, ensuring appropriate safeguards while preserving openness, academic freedom and international engagement.

[1] Dual-use research may also engage obligations under EU export control law (EU Dual-Use Regulation 2021/821), particularly in relation to intangible technology transfers. RPOs must assess whether their research activities involve items or technologies subject to export control and implement appropriate compliance measures.

2. Why Research Security Matters

International research collaboration is essential for Ireland as a small, open economy. It enables engagement with global talent, drives research excellence and generates solutions to complex challenges. Ireland's research system is strengthened by — and depends upon — the integrity of openness, international collaboration, and trusted global partnerships.

However, the geopolitical importance of research and innovation has grown significantly. Potential risks include intellectual property theft, foreign interference, and unwanted transfer of knowledge in ways researchers do not intend. Research communities are particularly exposed to risk because of the openness and international interconnectedness that are fundamental strengths of modern research.

Proportionate risk management enhances rather than constrains international partnerships. The vast majority of international research collaboration is legitimate and low-risk; research security measures are intended to support informed and proportionate safeguards where specific risks arise. Where proportionate safeguards are in place, the existence of risk, or the occurrence of an incident, does not in itself indicate institutional failure. The objective is to find the appropriate balance between openness and protection of what is important to us.

These guidelines are designed to support researcher mobility and international engagement, particularly for early-career researchers for whom international collaboration is essential to career development. Implementation should ensure that research security measures remain enabling rather than restrictive, supporting responsible research without creating disincentives for international engagement, interdisciplinary collaboration, or researcher mobility.

3. Core Principles

These guidelines are founded on nine core principles, aligned with G7 Common Values and EU Council Recommendations:

1. **Academic Freedom and Openness:** Research security measures must preserve academic freedom, institutional autonomy, and the openness that enables research excellence. Openness and international collaboration are strategic assets, not risks to be minimised.
2. **Institutional Autonomy and Responsibility:** RPOs play a central role in research security decision-making, reflecting their institutional autonomy, governance responsibilities, and proximity to research activity, within a broader shared responsibility framework involving government and funders. RPOs have primary responsibility for research security decisions, based on their governance mandates, further developing and strengthening expertise in identifying sensitive research, and proximity to research activities.
3. **Research Funders and Government Departments:** have a central enabling role in supporting RPOs through advice and guidance, coordination, supporting capacity-building, raising awareness and facilitating development of and access to shared tools as well as providing expertise and appropriate national supports.
4. **Proportionality and Risk-Based Approach:** Responses must be proportionate to actual risks. Not all international collaboration presents significant risk. Security measures should be scaled appropriately to avoid unnecessary burden. Overly precautionary or defensive interpretations should be avoided, particularly for legitimate research collaboration in low-risk disciplines or with trusted international partners. This will prevent unnecessary restrictions and compliance escalation.
5. **Transparency and Non-Discrimination:** Decisions must be transparent, evidence-based, and free from discrimination. Research security concerns must never be used to justify bias, xenophobia, or prejudice against individuals based on nationality, ethnicity, or background.
6. **Clarity of Roles and Responsibilities:** Roles must be clearly defined to ensure accountability. While collaboration across stakeholders is essential, collaborative implementation should not obscure accountability.
7. **Simplicity and Agility:** The research security should be integrated into existing governance structures wherever possible, avoiding unnecessary duplication, standalone compliance processes, or disproportionate administrative burden that constrains innovation, agility, and responsiveness.
8. **Consistency and Coordination:** Alignment across government departments, agencies, and funders is essential to avoid fragmentation, duplication, and unnecessary

administrative burden. Consistency strengthens effectiveness without compromising institutional flexibility.

9. **Research Integrity:** Research security and research integrity may intersect in certain areas, particularly around disclosure, transparency, and external influence, but remain distinct governance domains with separate objectives and institutional frameworks.

4. Roles and Responsibilities

Research security is a shared responsibility, with each actor having distinct and complementary roles. Clarity on these roles is essential to ensure effectiveness, avoid duplication and support proportionate implementation across the system.

4.1 Research Performing Organisations (RPOs) — Core Institutional Responsibilities

RPOs play a lead role in research security given their institutional autonomy, governance responsibilities, and proximity to research activity and specialised expertise in identifying and managing risks in sensitive research areas. RPO responsibilities discharged within the broader national framework of appropriate national coordination, guidance, and shared support mechanisms, include in particular:

- Conducting proportionate risk assessments for international partnerships, visiting researchers, and sensitive research projects.
- Establishing appropriate internal governance structures for research security.
- Developing and delivering awareness training for researchers, tailored to disciplinary contexts, drawing where appropriate on nationally developed resources and shared training models as well as drawing on EU resources.
- Ensuring transparency in funding sources, affiliations, and conflicts of interest.
- Implementing safeguards for data, intellectual property, and research infrastructure.
- Making decisions on research security matters within their remit based on institutional judgement and expertise, informed where appropriate by national guidance, legal requirements, and relevant advisory supports.

RPOs retain autonomy in determining proportionate implementation approaches appropriate to their institutional profile, while operating within relevant national and legal frameworks.

4.2 Research Funders — Enabling and Supporting Role

Research funders support research security by encouraging proportionate consideration of research security within funding processes, while avoiding unnecessary duplication of institutional or EU-level requirements and respecting RPO autonomy in operational implementation. Funder responsibilities include:

- Including risk appraisal questions in funding application processes to encourage up-front risk identification.

- Supporting proportionate disclosure arrangements relating to funding sources, affiliations, and potential conflicts of interest, aligned where possible with existing institutional and funder processes.
- Deferring to RPO expertise and judgment in cases involving high-risk research, rather than imposing additional controls.
- Coordinating across funding agencies to ensure consistent approaches and avoid fragmented or contradictory requirements. Where possible, national requirements should build on, rather than duplicate, existing EU-level processes such as Horizon Europe ethics reviews, security scrutiny, and due diligence mechanisms.
- Developing in-house research security expertise to support informed engagement with RPOs.

Funders do not make independent research security determinations on individual projects; their role is to ensure RPOs have considered risks and have appropriate safeguards in place.

4.3 Government — Coordination, Guidance, and Strategic Support

The Department of Further and Higher Education, Research, Innovation and Science (DFHERIS) and other relevant Government Departments provide strategic coordination and support, without micromanaging or overriding RPO judgments. Government responsibilities include:

- Providing a clearly identified central point of contact for research security matters, serving as an interface between RPOs, funders, and Government Departments for the purposes of guidance, signposting and coordination.
- Facilitating coordination across government departments and agencies to ensure alignment and consistency.
- Developing and maintaining accessible national guidance materials, shared tools, risk assessment templates, training resources, and practical implementation supports developed in consultation and collaboration with RPOs and funders.
- Supporting awareness-raising campaigns and capacity-building initiatives including in relation to EU resources.
- Facilitating multi-stakeholder forums for information exchange and peer learning.
- Exploring mechanisms for the provision of advisory support to institutions, including appropriate signposting or access to relevant national guidance on entities of concern, export control interpretation, and broader geopolitical risk considerations, to support informed institutional decision-making where appropriate.

- Monitoring system-level effectiveness through aggregate data, without intervening in individual institutional decisions.
- Actively participating in EU-level peer learning mechanisms for research security.
- Facilitating Irish RPO access to the expected forthcoming European Centre of Expertise on Research Security and to the EU due diligence platform for international partner assessment, as well as promoting use of these tools within the national research community.

Government does not direct RPO decisions on specific research projects or partnerships. Its role is to enable informed decision-making by RPOs through guidance, coordination and resources when necessary.

5. Key Actions for Research Performing Organisations

RPOs should implement proportionate research security measures tailored to their institutional context, research profile, and risk exposure. **These guidelines apply on a risk-based basis across civilian research activity, with implementation proportionate to the scale, nature, and risk profile of the activity concerned. For low-risk activities, the focus should be on awareness and proportionate safeguards rather than extensive administrative processes.** Recommended actions include:

1. **Governance and Leadership:** Assign clear responsibility for research security at senior management level. Designate appropriate institutional responsibility for coordination of research security, taking into account institutional scale, profile, and existing governance arrangements. Integrate research security into existing governance structures, for example, existing compliance, risk management or other relevant institutional functions. The institutional context must be taken into account while supporting a broadly coherent and aligned approach across the sector.

2. **Risk Assessment:** Conduct baseline institutional risk audits to identify areas of heightened sensitivity, informed by relevant EU and national guidance on critical and sensitive technologies. Tiered risk assessment processes will be used for international partnerships, visiting researchers, and collaborative projects. Risk assessment templates and checklists are aids to judgment, not substitutes for expert assessment. They support, but do not replace, institutional expertise and context-specific evaluation. Many activities in sensitive domains are civilian, fundamental, or exploratory in nature and require differentiated assessment based on specific characteristics rather than blanket treatment of entire disciplines.

3. **In applying the tiered risk framework,** RPOs should note that the four technology areas identified by the European Commission as priority areas for economic and research security:
   (a) advanced semiconductors
   (b) artificial intelligence
   (c) quantum technologies and
   (d) biotechnologies
   should be treated as areas requiring heightened consideration within institutional risk assessment processes.

   RPOs may apply a lower risk classification to specific activities within these domains where they can demonstrate that the activity is civilian, fundamental, or exploratory in nature and does not involve transfer of sensitive knowledge or technology to

entities of concern, but institutional assessment should document the rationale for proportionate classification.

4. **Awareness and Training:** Develop or draw on available awareness-raising initiatives to reach researchers, research support staff, and leadership. Deliver tailored training using train-the-trainer models adapted to disciplinary contexts as appropriate to institutional needs, supported where possible through nationally coordinated shared resources and guidance and training materials where available and appropriate. Training should emphasise practical risk identification rather than theoretical compliance.

5. **Transparency and Disclosure:** Ensure transparency in funding sources, affiliations, and potential conflicts of interest for research staff. Institutions should establish proportionate disclosure arrangements relating to relevant external affiliations, commitments, and funding relationships, informed by national and legal guidance where applicable. Establish clear internal protocols for managing conflicts of commitment.

6. **Partnership Vetting:** Implement proportionate due diligence processes, drawing on available national and EU guidance/tools where available, for international research agreements, memoranda of understanding, and joint calls. Assess risks related to entities established in or controlled by third countries, particularly where security concerns may arise.

7. **Data and IP Protection:** Implement secure protocols for sensitive data and intellectual property, including encryption, access controls, and need-to-know principles. Align with OECD guidelines on data protection. Ensure cybersecurity measures for research infrastructure are robust, particularly for equipment or laboratories with third-country linkages.

8. **Visitor and Travel Protocols:** Establish proportionate institutional protocols for hosting visiting researchers and managing foreign delegations. Draw on nationally developed guidance, where available, regarding travel-related research security risks.

9. **Incident Response:** Establish clear institutional mechanisms for reporting research security incidents, appropriate to institutional context, including anonymous reporting channels. Ensure incident response processes are clear, supportive, and non-punitive to encourage disclosure. Most research security matters should be handled at institutional level based on RPO expertise and judgment.
   Engagement with national authorities is appropriate for:
   (a) incidents involving potential threats to national security;
   (b) cases requiring state-level intelligence or export control interpretation;
   (c) situations where coordination across multiple institutions is needed; or

(d) incidents with potential criminal dimensions.
RPOs retain decision authority and should consult government advisory services when additional support would be helpful, not as a requirement.

10. **Non-Discrimination:** Ensure implementation avoids direct or indirect discrimination or stigmatisation, and that research security measures do not disproportionately affect individuals based on nationality, ethnicity, or background.

11. **Export Controls and Dual-Use Compliance:** RPOs must be aware of and comply with their obligations under the EU Dual-Use Regulation 2021/821 and national implementing measures.

12. **Research Integrity and Security:** Research integrity and research security governance should be appropriately aligned where areas of overlap arise. Integrity risks with a security dimension include covert influence on research outputs or conclusions, manipulation of peer review processes, misrepresentation of funding sources or affiliations, and undisclosed conflicts of interest arising from foreign relationships.

6. Implementation Approach

Implementation will follow a phased approach that integrates with existing national structures (e.g., the System Performance Framework for HEIs, oversight agreements for funders). This approach promotes sustainability, proportionality, and continuous adaptation to evolving threats. Given existing capacity constraints across institutions, flexibility in timelines and sequencing is essential to ensure sustainable and proportionate implementation, supported by appropriate national coordination, shared resources, and practical guidance.

Phase 1: Preparation (6-12 Months)

Focus on building foundational capacity across the system.

RPOs: Conduct baseline risk audits to inform institutional risk profiles. Appoint appropriate internal coordination arrangements, reflecting institutional scale, profile, and existing governance structure. Update relevant policies with security considerations, integrating with existing processes such as existing governance, compliance, risk management, IP, or other relevant institutional structures.

Funders: Revise application forms to consider proportionate research security prompts or disclosures where appropriate, while avoiding duplication of existing institutional or EU-level requirements. Develop common approaches across agencies to ensure consistency.

Government: Establish central point of contact within DFHERIS. Launch awareness-raising campaigns to reach the widest audience. Develop templates, examples of research security incidents, and senior management checklists through collaborative engagement with the sector. Facilitate the development of guidance and indicative protocols for overseas travel, hosting visitors, and managing foreign delegations to support consistent approaches across RPOs, informed where appropriate by relevant national expertise and risk intelligence.

Phase 2: Integration (Ongoing)

Embed research security into daily operations.

RPOs: Implement tiered risk assessment processes for partnerships, visiting researchers, and sensitive projects. Establish proportionate disclosure arrangements and training tailored to disciplinary and institutional context. Protect data and IP through secure protocols (encryption, need-to-know access controls).

Funders: Integrate proportionate consideration of research security into funding cycles, while avoiding unnecessary duplication of institutional or EU-level requirements and deferring to RPO expertise in high-risk cases.

Government: Facilitate information exchange through multi-stakeholder forums (e.g., the Higher Education Institutions for Research Security [HEIRS] community of practice, funder

peer learning). Provide cybersecurity guidance from the National Cyber Security Centre (NCSC) tailored to research and innovation needs. Offer non-binding advisory services, including appropriate signposting, guidance, or access to relevant national expertise regarding entities of concern and related risk considerations. In the longer-term, further explore the security considerations relating to the visa application process for researchers.

Phase 3: Monitoring and Evaluation

Ensure ongoing effectiveness and adaptation.

RPOs: Perform periodic proportionate self-assessments, as appropriate, and report to funders and DFHERIS with appropriate metrics where required such as incident rates, training completion, compliance audits. Conduct periodic review mechanisms appropriate to institutional context to evaluate resilience.

Funders: Support ongoing implementation through funding processes, using proportionate reporting where appropriate. Draw on insights from funded activities to inform the evolution of guidance and funding approaches, and work collaboratively across agencies to promote consistency while minimising duplication and administrative burden for RPOs.

Government: Incorporate feedback loops based on lessons from national incidents, international peers (e.g., G7 best practices), and EU initiatives (e.g., the European Centre of Expertise on Research Security, due diligence platforms, resilience testing methodologies). Share aggregated data across stakeholders to inform policy refinements, while maintaining RPO autonomy and avoiding direct intervention. Consider alignment with existing governance and oversight structures where proportionate and appropriate, while avoiding unnecessary duplication or administrative burden. Conduct regular reviews to address emerging threats in critical technologies, ensuring the approach remains evidence-based and scalable.

7. International Context and Alignment

These guidelines are informed by and aligned with:

- **EU Council Recommendation on Enhancing Research Security (May 2024),** which provides a common EU framework emphasising enhanced self-governance and proportionate responses, and the importance of institutional capacity-building and support mechanisms.
- **G7 Common Values and Principles on Research Security and Research Integrity,** which affirms that openness and security are complementary and mutually reinforcing, and that protecting research security requires partnership between governments, funders, institutions, and researchers.
- **G7 Best Practices for Secure and Open Research,** which provides high-level guidance recognising that all stakeholders have roles in ensuring security and integrity of research.

Ireland's approach reflects these international frameworks while being tailored to national context, ensuring compatibility with EU-level supports (e.g., the European Centre of Expertise on Research Security, due diligence platforms) and alignment with commitments in the Programme for Government 2025. Implementation should continue to evolve in line with emerging EU-level developments in research security, economic security, and dual-use policy. Openness and international collaboration remain not only values to protect but strategic assets for Ireland's research system. Research security measures are understood as enabling, rather than constraining, research excellence, international collaboration, and researcher mobility.

8. Review and Updating

These guidelines will be subject to ongoing review and periodic updating in light of knowledge and experience gained in implementation by all parties, their effectiveness in securing national and institutional research security objectives, changes in the international environment for research security, and evolution of international best practice, with ongoing engagement with the research performing sector to inform future refinement and implementation experience.

Appendices

The following appendices provide supporting information and practical tools:

- **Appendix A:** Risk Assessment Templates and Checklists
- **Appendix B:** Examples of Research Security Incidents and Case Studies
- **Appendix C:** Training and Awareness-Raising Resources
- **Appendix D:** Relevant National and International References

[Appendices to be developed collaboratively with RPOs and funders, and relevant government stakeholders during Phase 1 implementation, including practical implementation guidance and shared tools where appropriate]