G7 BEST PRACTICES FOR SECURE & OPEN RESEARCH

Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group

This document is a copy of the original document titled G7 Best Practices for Secure & Open Research published by the G7.

February 2024

Table of Contents

Vision Statement

In the G7 Common Values and Principles on Research Security and Research Integrity, members envisioned:

> *The continuation of a collaborative research system where the importance of all talent – domestic and international – is acknowledged. Openness and security are not contradictory but complementary and mutually reinforcing.*

The G7 members recognise that respecting freedom in scientific research is an indispensable cornerstone of democracy and a common core value for trustful and open research cooperation with international partners. Members commit to promoting international research cooperation and the conditions of freedom, independence, openness, reciprocity and transparency under which it flourishes.

To sustain this vision, G7 members developed and endorsed a set of principles of research security, which are common to the G7 members and academic communities and consistent with established common values of research integrity. This set of principles of research security and common values on research integrity are articulated in the G7 Common Values and Principles on Research Security and Research Integrity paper and can be found at Annex A and B below.

To support implementation of the aforementioned principles of research security and the common values on research integrity, the G7 members have developed a list of best practices to provide high-level information on practices that contribute to secure and open research. Recognizing that all stakeholders have a role to play in ensuring the security and integrity of research, these best practices are aimed at: governments, research funders, research institutions and researchers, either collectively or individually, based on their role in research. Examples of best practices that are being implemented by different G7 members are highlighted in Annex C.

To complement this best practices paper, a Virtual Academy will also be developed to support stakeholders across the G7 and beyond in implementing research security and research integrity practices within their institutions. This Virtual Academy will be a resource for users to explore how research security and integrity is addressed by each G7 member, and will include additional examples of best practices and case studies for reference.

Why does research integrity & research security matter?

Open and collaborative research underpins domestic and global responses to some of our most challenging and pressing issues. Fostering international scientific collaborations is important. These collaborations accelerate the pace of discoveries and increase the dynamism and openness of our research communities.

Research Integrity - the adherence to professional values, principles, and best practices which uphold the validity, social relevance, responsibility and quality of research – forms the base on which researchers can collaborate in a fair, innovative, open and trusted research environment. Research integrity ensures that individuals can be confident in the advancement of research knowledge and in the dissemination of its results.

At the same time, scientific advancements and their potential applications can make research a target for those who seek unauthorized access and transfer of research knowledge. These actors seek to advance their own goals and do so without recognition of – or benefit to – those involved in funding and conducting the work. While these activities may be done for a variety of economic, strategic, geopolitical, or military objectives, the end results breach the norms and values that form the foundations on which international research rests, including the security and integrity of research.

Research Security - involves the actions that protect our research communities from actors and behaviours that pose economic, strategic, and/or national and international security risks. It is an emerging area for many researchers, institutions, and governments. G7 governments recognize that our individual and collective approach to research security may evolve over time, and therefore our understanding of what constitutes best practices will also continue to evolve. The principle of adaptability must underpin the implementation of any research security best practice, recognizing that approaches may need to be adapted to account for new and emerging risks, and be proportionate and flexible enough to maintain and support the autonomy of research activities by research institutions and researchers, while preserving research quality.

Further information on the relationship between research integrity and research security risks, can be found in Annex B of the G7 Common Values and Principles on Research Security and Research Integrity paper.

What is "risk" in research security?

Governments and research community members will often refer to "risk" when discussing research security. The best practices articulated in this paper are often situated on identifying, understanding, and mitigating risk in relation to research security, making it important to define what is meant by the term.

For research security, risks can include activities that are illegal and/or non-transparent, such as:

- undue influence, interference, or misappropriation of research; including the outright theft of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity; and

- other clandestine activities and behaviours that have adverse economic, strategic, and/or national security implications.

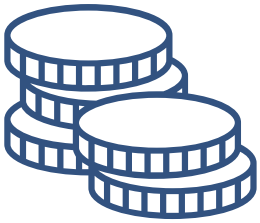
Risk in research security can originate from both within a research team or institution, or from outside of the research team or institution, through different means. The means by which actors can influence, interfere, or misappropriate research include through infrastructure (both digital and physical), people, and funding. These methods may be used illicitly as a point of entry for exploitation, but may also be accessed through licit or legal means, but without transparent disclosure of the intended purpose or end user, that could result in unintended or harmful uses of the research. The following areas of risk should be considered and assessed when developing a research project, with research security due diligence representing one additional aspect as part of the overall planning and assessment that goes into structuring a research project.

Infrastructure (digital and physical)

- Cyber threats can take the form of cyber-attacks (such as phishing or ransomware) that take advantage of vulnerabilities to access research data or results.
- Physical access can be used to acquire research data or results at the facilities where research is conducted.

People

- People from outside a research team or institution may seek to partner with researchers for their undisclosed purposes or benefits with security implications.
- People from within a research team or institution, who have direct or indirect access to knowledge or proprietary materials, could be self-motivated or supported or pressured by others to access or steal research for their own gain, or the gain of others; or poor security hygiene practices could facilitate this access by others.



Funding

- Funding could be used as an incentive to access or transfer research data, processes and outcomes, potentially without the transparent disclosure of the intended purpose or end user.

When we refer to "risk" within the below best practices for research security and integrity, we are referring to the aforementioned risks. While individual practices may evolve, these risk categories – and corresponding best practices - are deliberately broad, to allow their corresponding evolution to be addressed.

G7 Best Practices for Research Security & Integrity

No individual stakeholder holds all responsibility for the protection of research. It is a shared responsibility amongst all stakeholders. To acknowledge this, this paper is structured by best practice, and by the relevant stakeholders implicated by the practice. Collaboration between members of the research community is critical to ensure risks are addressed proportionately, quickly, and in a coordinated fashion. By working collectively stakeholders can strengthen the research community as a whole against research security risks.

The following list of best practices has been identified by the G7 members, drawing from existing initiatives and programs.

Many of these practices are suitable for the entirety of the research community – **governments, research funders** (including private, public and government funders), **research institutions** (including the associations that represent them, as well as government-run research institutions), and **researchers**.

Given that the context and structure of a research ecosystem varies across the G7 countries, best practices may be implemented differently by each member to suit the needs of their research community.

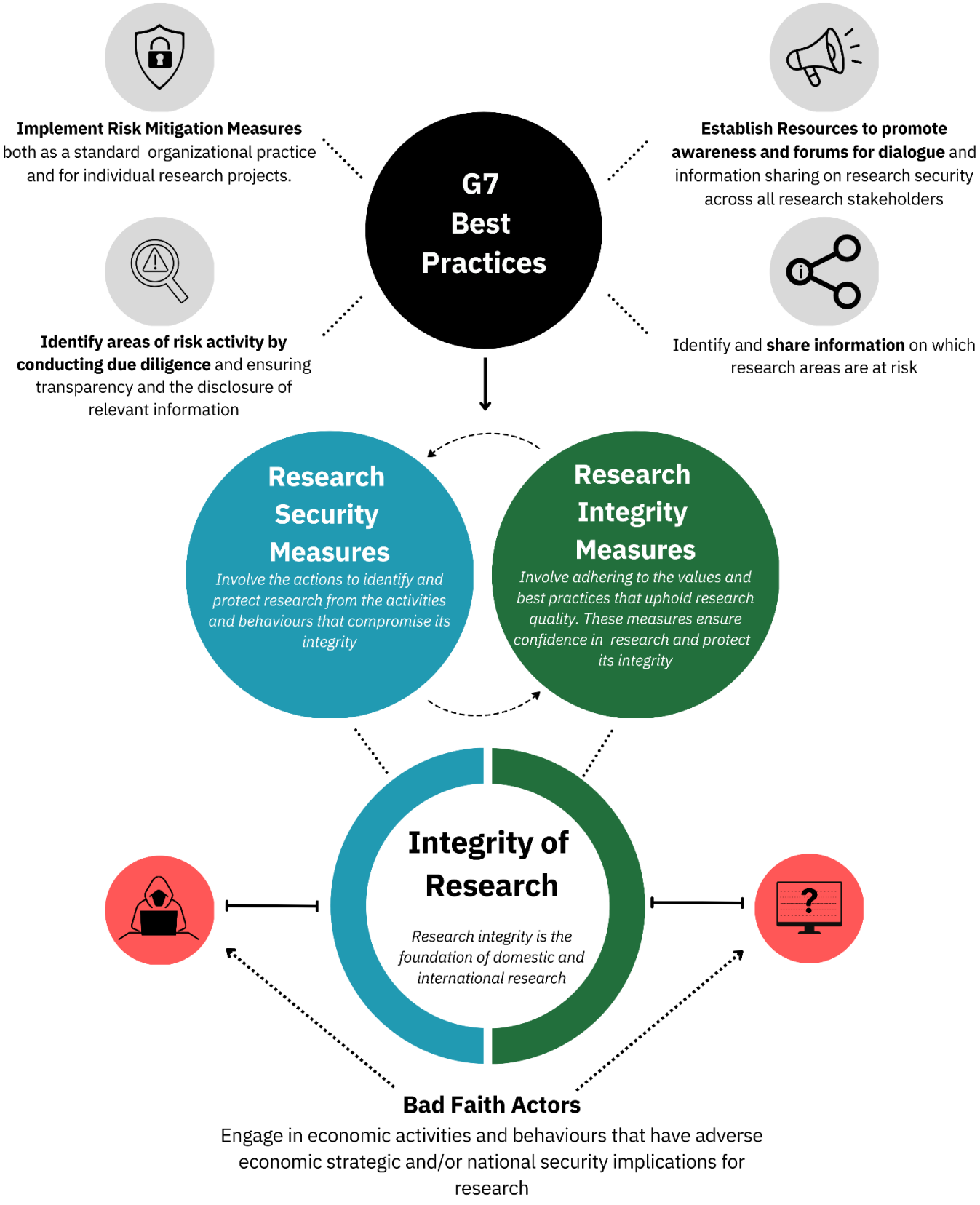


Figure 1: *A graphic depicting how the G7 Best Practices support both research security and research integrity.*

1. Establish resources to promote awareness and forums for dialogue and information sharing on research security and integrity across all research stakeholders.

Research security is an emerging area of national security concern and may be a new risk topic for many individuals and institutions. Ongoing dialogues between stakeholders in the research community, both bilaterally and multilaterally, are important to maintain active and ongoing sharing of information and to raise awareness. Information sharing can be accomplished through the provision of resources (i.e. online databases, training, etc.), and through the establishment of taskforces or working groups to discuss current and future needs of the research community, informed by an understanding of the broader conduct of research.

All stakeholders, including governments, research funders, research institutions and researchers should take care to avoid targeting specific individuals or communities when raising awareness of or discussing security risks. The lexicon and language that is used in such dialogues is critical to ensuring freedom from discrimination, harassment, and coercion that is foundational to the success of research.

Governments: Establishing forums for dialogue and information sharing between a government and the various stakeholders in their research community can help all partners better understand the research environment and its security risks. These dialogues can serve many purposes, including sharing information on current and emerging risks, identifying the needs of the research community to build resources, and supporting policies on research security and integrity. For example, a government may be able to share unclassified information to inform funders, institutions and researchers of new risks or practices. Similarly, information can flow back from the research community to government to ensure governments have sufficient knowledge of the research culture and processes to develop research appropriate risk information and policies.

Governments may also want to consider creating a central resource for members of the research community to obtain information from and build awareness. Such a central resource could include current information on current and evolving risks, and be a source of information for resources that can help implement some of the best practices identified here.

Research Funders: Research funders can engage regularly with the government bodies which set expectations for research funding and programs and to help shape broader policies which relate to research security and integrity. Similarly, research funders' engagement with research institutions and researchers is critical to understand emerging issues and unmet needs. Research funders may also aid in the dissemination and promotion of resources to aid in building awareness.

Research Institutions: Research institutions play a critical role in identifying the needs of the researchers. By establishing active dialogues with an institution's researchers, tools and resources can be developed to close gaps in understanding of risk, and provide relevant, up to date information on the current risk environment, tailored to specific organizational contexts and processes. Research institutions may train and update staff regularly on areas of potential risk and how to mitigate them to ensure they stay current with existing threats. They may wish to disseminate resources to researchers to build awareness of risk within their research community.

Researchers: By engaging in effective awareness raising and information sharing, researchers can be empowered to protect their research and, in doing so, the integrity of their domestic and international research ecosystems. Researchers also have a role to play in contributing to dialogues at all levels to ensure their needs are well articulated and understood, so that they can be addressed by governments, research funders, and research institutions.

Policy In Action

In 2019, the United Kingdom launched the Trusted Research campaign to address the need for an enhanced understanding of research security in the UK research and innovation sector, in light of the increasingly collaborative and out-ward facing stance within UK academia.

2. Identify and share information on which research areas are at risk.

Outside of regular sharing of information on research security and integrity broadly, it is important to provide risk-targeted information, which means identifying research areas more likely to be targeted and how. The identification of more at risk research areas promotes a *risk-proportionate* approach to research security, still supporting international collaboration and open science but recognizing that some research areas warrant a greater level of security than those at lower risk. Research areas which are more prone to security and integrity risks should be consistently reviewed and updated to maintain relevancy and respond to changes in science and the risk environment.

Governments: Governments should work in collaboration with funders, institutions, and researchers to ensure the identification of at-risk areas is accurate and delivers on the needs of the research sector. Governments have a role to play in helping their country's research community in understanding the risks in certain subject matter areas, including providing information on at risk areas such as:

- Areas with a clear link to advancing military or intelligence capabilities;

- Areas which are dual use in that they have military/intelligence and civilian application;
- Areas with the potential for significant economic benefits;
- Areas with potential access to sensitive personal data or large data sets that may be sensitive in the aggregate form;
- Areas of critical infrastructure including those processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of a country's citizens and the effective functioning of government; and
- Areas aligned to priority national economic and/or strategic interests.

Research Funders: Research funders should implement research security and integrity requirements in a targeted way that focuses on research areas of the highest risk. Funders should also engage with researchers to ensure they have a complete understanding of a project and the potential risks.

Research Institutions: Research institutions should know what research activities are carried out within themselves in the research areas which the government views as sensitive. They can in turn help researchers to identify that their research is of higher risk and provide support to them through the sharing of information.

Researchers: Researchers have the most insight into their own research and the environment in which it is developed. Researchers should consider ways in which their work could be appropriated and misused, follow any existing government guidance to determine whether their research may be considered sensitive, and utilize any tools provided by governments, funders or research institutions to conduct due diligence activities on their research.

Policy In Action

In June 2023, the United States Department of Defense (DoD) introduced a Department-wide policy on reviewing fundamental research projects for conflicts of interest arising from foreign influence. DoD will follow these policies for risk-based security reviews of fundamental research project proposals to mitigate potential research security risks.

3. Identify areas of risk activity by conducting due diligence and ensuring transparency and the disclosure of relevant information.

Risk can originate from a variety of sources and it is critical to establish where threats are most likely to stem from to develop risk mitigation measures in response. By defining the key means of risk, other best practices such as the implementation of risk mitigation measures can be better implemented.

Governments: Together with their respective research communities, governments should take responsibility for the development of policy frameworks which set the due diligence and transparency requirements for research funders, institutions, and researchers. These frameworks should balance national and global interests, promoting research, science, and innovation while putting in place safeguards to protect research from identified risks.

Governments and national security agencies should also provide guidance to research institutions and researchers as to the most current risks to the research community, regularly assessing the threat environment to ensure the research community is equipped to identify risk and that frameworks are consistent in safeguarding research. Through regular assessment, policy frameworks can be reviewed to consider whether they are still meeting the needs of the research community and objectives of research security and integrity. Governments have more insight into trends in risk and may share this information to aid in risk identification when possible. Furthermore, governments should monitor for any unintended adverse impacts of any policy framework that is established to ensure that the principle of maintaining academic freedom and avoiding discrimination and harassment is maintained.

Research Funders: Research funders are responsible for implementing policy frameworks established by governments to meet the objective of identifying, assessing and mitigating areas of risk in research projects. Applications for funding should transparently demonstrate the due diligence that has been undertaken to identify risk and the disclosure of relevant potential risks. To aid in this identification, funders should utilize either government established or their own guidance and approaches for applicants to disclose and identify risk. Such approaches should allow researchers to easily and transparently demonstrate their disclosure and assessment of risk. When reviewing applications, funders are responsible for weighing any risks against the scientific merit and benefits of a proposal.

This can include for example, assessing of any project partners or disclosure of any conflicts of interest or affiliations. Foreign governments, militaries, their proxies, and other organizations may seek to facilitate unauthorized knowledge transfer through the use of partnerships or researchers or members of the research community to access research information (e.g., data), research knowledge, and the resulting intellectual property and technology. To reduce these risks, funders should have an

understanding of who is involved in a research project, and their associations. Individuals could be knowingly or unknowingly co-opted or coerced to facilitate unwanted knowledge transfer in a manner that could harm national security.

Funders could consider requiring the transparency and disclosure of information related to potential conflicts of interests and standardizing such requirements by including these requirements in funding application forms. This can include disclosure of information related to the individuals involved on a project (organizational affiliations, appointments, paid consulting activities) or on other sources of funding of the research (in-kind, personnel, or cash contributions) including from foreign governments.

To ensure that the principle of safeguarding research freedom and avoiding discrimination and harassment is maintained, research funders should monitor for any unintended adverse impacts in the implementation of research security and integrity programming, and take action to ensure that discrimination and harassment is not accepted within their research funding programs.

Research Institutions: Research institutions can establish capacity to assist their researchers in identifying and evaluating risks, and ensuring transparency in the disclosure of information. Research institutions may wish to consider identifying a lead at the senior leadership level to take responsibility for matters regarding research security and integrity and to help ensure a uniform approach. Research security risks could for example, be integrated into an organization's risk framework or risk registry, or in the institutional framework for research integrity. Reputational, ethical, and national security risks related to research projects should be regularly discussed at the senior leadership level to allow institutions to quickly respond and adapt to emerging concerns. Research institutions should ensure that those responsible for risk management decision making clearly understand the scope of their responsibilities and have appropriate support to identify where decisions should be considered for escalation to a more senior level.

In addition, institutions should have responsibility for identifying and evaluating institutional-based risks, that can apply to multiple projects or research disciplines. For example, identifying infrastructure-based risks – both physical and digital – would generally be an institutional level responsibility, with physical access controls and cyber security controls often put in place at the institutional level, rather than by individual researchers for specific projects. In addition, institutions should review the language of research agreements to ensure the outcomes are transparently documented and favourable to all parties.

To ensure that the principle of maintaining research freedom and avoiding discrimination and harassment is maintained, research institutions should monitor for any adverse impacts in the implementation of research security and integrity initiatives and report any such findings to the relevant research funders or governments so that such occurrences can immediately be addressed.

Policy In Action

In July 2021, the Government of Canada introduced the National Security Guidelines for Research Partnerships (the Guidelines) to integrate national security considerations into the development, evaluation and funding of research partnerships. Applicants to research funding programs where the Guidelines apply must submit a Risk Assessment Form, including a risk mitigation plan.

Researchers: As has been stated previously, researchers know their research domain and the work they are completing best, and - as a result - are frequently best placed to identify areas of potential risk activity, including specifically in relation to partnerships and people; supported by risk information provided by governments and other credible sources. To aid in identifying risk, researchers should also commit to identifying, evaluating and mitigating potential risks to the integrity and security of their research. This includes appropriate information disclosure to their research institutions and research funder(s), which may have knowledge on broader emerging risk trends which may not be immediately evident to a researcher. This allows researchers to stay abreast of the broader risk context or changes in risk.

Understanding the motivations and interests of partners and team members can help in identifying potential areas of risk. By completing due diligence reviews, risk indicators may be observed suggesting that an individual's autonomy may be compromised; indications of connections to foreign governments; military or security services on sensitive research areas; information that shows your partner operates in countries known to access and/or steal IP from researchers; or any information that suggests lack of transparency. Learning more about those involved in a project and understanding their motivations and goals will aid in identifying and mitigating potential risks. Regardless of the degree of formality of the partnership, knowing who is involved in the project – and having clear, shared and documented processes to guide the collaboration - is beneficial and supports the integrity of the research. This will allow researchers to proceed with confidence knowing that potential risks have been identified and transparently addressed.

Researchers need to understand that research security and integrity measures should not target any specific individuals or communities, and should identify to their institutions, funders or governments any instances of discrimination or harassment so that such occurrences can be immediately addressed.

4. Implement risk mitigation measures, both as standard organizational practice and for individual research projects.

After establishing *where* risk exists and its magnitude, members of the research community are generally better positioned to address and mitigate against it. Risk mitigation aims to reduce the likelihood and impact of risks to a level that is acceptable to the researcher, their institution, the research funder, and the respective government. Risk mitigation measures can be implemented at an organizational level, creating standards that are expected to be followed, and at a project specific level where a more tailored approach to mitigating risk may be appropriate for projects with unique characteristics that may elevate their level of risk. Mitigation measures should be proportionate to the level of risk in order to ensure both secure and open research. Mitigation measures may need to be adapted over time as risks change and will benefit from periodic review to determine if they are still appropriately addressing current risks, or if changes are necessary to respond to new concerns.

Stakeholders such as research funders and research institutions may also wish to consider implementing risk governance both at the organizational and project level. Having in place organizational policies and processes to assess and mitigate risks associated with organizational risks as well as with individual research projects is critical to ensuring consistency in the decision-making process.

Governments: Governments have a valuable role to play in providing guidance on risk mitigation. Governments can develop resources and information sharing mechanisms to help other members of the research community with this best practice.

Research Funders: Research funders may wish to consider implementing specific requirements within their application process related to research security and integrity, or set policies or conditions that certain risk mitigation measures be a standard expectation for funding. Funders may wish to consider encouraging or requiring applicants to ensure that participants on a specific program meet certain training requirements in relation to securing their research, have cybersecurity plans in place, and control measures for the management of data, in accordance with existing and evolving research community best practices. In addition, by virtue of being in receipt of research proposals submitted by applicants, research funders are likely able to identify and develop broad risk mitigation best practices. In turn, they can circulate guidance on risk mitigation measures broadly across the research community (in conjunction with governments).

Research Institutions: Research institutions can consider implementing a variety of measures to protect themselves and their researchers. For example, institutions may consider employing appropriate cyber security practices, physical access controls, ensuring adherence to the relevant legal obligations of their country, and developing protections for intellectual property.

To encourage strong research security and integrity practices, a research institution can also establish a code of conduct on research security and integrity for its researchers. A code of conduct can set standards broadly for researchers within the institution. This can also set expectations for how researchers should react when faced with instances of unauthorized access, malicious interference or coercion. Having in place appropriate policies and processes for staff to report issues or concerns will support information sharing, identification and mitigation of risks.

Institutions can also consider providing training on standards for good cyber security and physical security practices. If staff are travelling or sharing information internationally, they should be briefed, trained and equipped to be knowledgeable on how to keep themselves and their sensitive information secure.

Policy In Action

More than 120 research institutions, organizations and professional societies in Germany have installed local Committees for Ethics in Security-Relevant Research to advise researchers and research institutions on questions concerning security-relevant aspects of their research. The committees were established in accordance with the "Recommendations for Handling of Security-Relevant Research", which were introduced in 2014 by the German National Academy of Science Leopoldina and the German Research Foundation, and updated in 2022.

Researchers: To implement risk mitigation measures, researchers can develop risk mitigation plans with clear risk reduction steps. Ideally, risk mitigation plans would be developed with the support of a researcher's institution and/or funder, in order to address risks identified through an earlier review of potential areas of concern. A researcher's chosen risk mitigation strategy should balance the benefits and risks and not inhibit their ability to collaborate, attract international talent, or create sustainable funding. Risk mitigation plans should aim to be as specific as possible and may vary in what they cover depending on the types of risks identified.

These risks mitigations can be integrated into existing research hygiene practices, with documented measures and procedures shared with all members of a research project, and implemented and tracked to ensure they are being followed. Members should familiarize themselves with controls that are implemented. Training and onboarding procedures should be established to ensure that, both at the onset and throughout the life of the project, risks are managed appropriately. Such research security and integrity practices can be most effective when they are integrated into general research practices.

Conclusion

Open and collaborative research allows us to respond to some of the world's most challenging issues. Research integrity acts as the base from which researchers are able to operate in our global research environment. To support research integrity, the above best practices are meant to help research communities establish and improve processes and efforts to protect their respective research and enable the operation and continuation of a collaborative research system on a reciprocal trust basis. These practices have been developed to support research by following many key research integrity principles, such as academic freedom; open science; transparency, disclosure and honesty; freedom from discrimination, harassment, and coercion; fostering public trust; and institutional autonomy.

Research security remains an emerging area for research communities around the globe and is therefore a concept that will continue to evolve over time. These practices should continue to be adapted to address new and emerging risks, to ensure responses are proportionate and appropriate.

Annex A - Common Values of Research Integrity

Academic Freedom: The freedom to teach, conduct, and publish research in an academic environment with an emphasis on enabling the participation of all is a fundamental tenet of research. It is fundamental to the mandate of research institutions to pursue truth, provide education to students, and disseminate knowledge and understanding. Academic freedom requires an environment of enabled autonomy and job security where researchers are free from undue external influence or limitations on scholarly inquiry.

Freedom from Discrimination, Harassment, and Coercion: Freedom from discrimination, harassment, and coercion is a value that is foundational to the success of research. All members of the research community should be free from discrimination, harassment, bullying, coercion, or threats to their personal or family safety. Discrimination, harassment, and coercion can be by an individual, a group, an institution, or a government. This includes instances whereby entities may coerce and harass individuals to act in unethical and dishonest ways – counter to their will or interest – to support an entity's own objectives, interests, and directives.

Equity, Diversity, and Inclusion: Equity, diversity, and inclusion (EDI) is the active promotion of the principles of access, diversity, and non-discrimination in all research activities – including recruitment procedures and career prospects. These are necessary for all aspects of research. EDI contributes to the diversity of identity and thought, with room for a variety of ideas, cultures, and views. Ensuring that everyone is able to freely participate in the research community, ecosystem, or enterprise will help to build an innovative, prosperous, and inclusive world.

Institutional Autonomy: Research institutions can only fulfill their missions to students, faculty, staff, and society if they are free to pursue and disseminate knowledge based on evidence, data, and peer review. Institutions should be free to pursue their own missions. These missions can be based on the oversight and direction of their governance, or can be to meet community and local needs. Regardless, institutional autonomy requires a safe and secure environment in which all individuals and institutions are free and protected from unwanted external influence.

Open Science and Access to Research: All members of the research community should actively support the open sharing and exchange of research results, data, methods, and inputs, while preserving the incentives for innovation. Open science – the practice of making science and research inputs, outputs, and processes available to all with minimal restrictions – should be practiced in full respect of privacy, security, and ethical considerations, as well as appropriate protection of ideas, research outcomes, and intellectual property. Enabling all members of society to build on previously validated research, open science helps to speed up the pace of new discoveries, bettering the lives of others and our societies and contributes to research quality.

Fostering Public Trust: Conducting and pursuing research in a way that maintains the trust of the public and all those involved in research is vital to the continued success of science and research efforts. As contributors to integrity, all entities engaged in science and research activities should strive to demonstrate that they can meet the expectations of trust when accessing sensitive data or research. This requires deliberate, clear, and shared understandings across all partners of the purpose, use, and ownership of research results. This understanding should be upheld and respected across all stages of the research and in all jurisdictions. Maintaining this public trust also necessitates stewardship, which entails reflecting proper oversight and management at all levels. Governments and funding agencies have stewardship responsibilities over their decision-making and over their relationships with post-secondary institutions and research institutions. Post-secondary institutions and research institutions have stewardship responsibilities in their relationships with their employees and students, and in their communications with their sponsors.

Transparency, Disclosure, and Honesty: Fully transparent and reciprocal sharing of the methods, data, and outcomes of unclassified research – while maintaining confidentiality when appropriate – is crucial to research collaboration, integrity, and the free flow of ideas and information. Transparency in disclosing researcher affiliations, competing or conflicting interests, and sources of funding is also important to ensure the integrity of the research being conducted. Transparency requires honesty. As a complementary value, honesty entails being straightforward and free of fraud and deception when proposing, developing, undertaking, reviewing, reporting, and communicating research. This extends to all aspects of research and includes the acknowledgement of the work of others and making justifiable claims or sensible interpretations based on research findings.

Annex B – G7 Principles on Research Security

Balancing National and Global Interests: Funding for scientific and research partnerships should continue to be guided primarily by scientific merit assessments and excellence, and take appropriate and proportionate consideration and mitigation of risks to national and/or economic security where necessary.

Maintaining Openness and Research Security: Open science should not be an afterthought and governments should commit to making research accessible when there is no justification for it to remain closed. It is recognized that openness should have limits and cannot override obligations to maintain safeguards over research that could have adverse ethical, geopolitical, or national security implications should it be disseminated.

Collaboration and Dialogue: All entities involved in research should strive to support and engage with one another in the pursuit of a community that upholds security alongside openness. Governments should commit to engaging in meaningful information sharing about the nature of the risks, with the goal of addressing common risks alongside researchers and benefiting from shared approaches.

Proactive Efforts: Governments should strive to take proactive and preventative measures that manage and reduce research security and research integrity risks based on lessons-learned and best practices.

Risk Proportionality: Responses to risks should be proportionate and appropriately scaled. Risk-appropriate responses to research security should take into account the potential for misuse of the research and the aggregate level of risk, among other factors.

Shared Responsibilities: To address dynamic and changing research risks, all members of the research community should acknowledge and understand their distinct roles and responsibilities with respect to addressing and managing risks to research security and research integrity.

Accountability and Responsibility: Individuals and organizations should be held accountable for all their actions, including when their behaviours deviate from accepted standards.

Adaptability: There should be commitment to dynamic research security measures, acknowledging that overly rigid approaches run the risk of delaying beneficial research. Static and unwavering approaches can lead to significant research disincentives and do not account for new and emerging risks.

Annex C - Examples of Best Practices

European Commission - Standard Operating Procedures for Research Integrity

Each example of the EU Standard Operating Procedures for Research Integrity reflects one of the above described best practices.

1. The SOPs4RI (Standard Operating Procedures for Research Integrity) is a four-year (2019-2022) multi-partner project funded by the European Commission. SOPs4RI aims to stimulate transformational processes across European Research Performing Organisations and Research Funding Organisations (RPOs and RFOs).

2. SOPs4RI will deliver an online, freely accessible and easy-to-use 'toolbox' that can help RPOs and RFOs cultivate research integrity and reduce detrimental practice. SOPs4RI will establish an inventory of relevant Standard Operating Procedures (SOPs) and Guidelines that RPOs and RFOs can draw on when developing governance arrangements promoting strong research integrity cultures.

3. The European Commission has found that serious violations of good research practices such as Falsification, Fabrication and Plagiarism (FFP) are relatively rare, with an estimated 1% to 2% of scientists engaged in such practices. However, less serious issues, known as Questionable Research Practices (QRP), such as bad research design, methodology and analyses are much more frequent. Thus, providing intuitive guides for researchers to follow and to better structure their research is integral to the European Commission's approach to ensuring a sound research environment.

4. Studies from different disciplinary fields have shown that it is often difficult to reproduce previous studies' findings. Selective reporting, inadequate description of methods and other such QRPs are often considered to be the cause of replication problems. Replication issues and inefficient research environments can not only slow down research, but obfuscate the process and hold up resources or distract those such as supervisory bodies from other areas of a research network. This can create opportunities and blind spots which can be exploited to compromise research security.

United Kingdom – Trusted Research Portal

(1) Establish resources to promote awareness and forums for dialogue and information sharing on research security and integrity across all research stakeholders

The UK has a thriving research and innovation sector that attracts investment from across the world. More than half of UK research benefits from international partnerships. The National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC) Trusted Research campaign was launched in 2019 to address

the need for an enhanced understanding of research security in the UK research and innovation sector, in light of the increasingly collaborative and outward-facing stance within UK academia.

Trusted Research aims to support the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector. It is particularly relevant to researchers in science, technology, engineering and mathematics (STEM) subjects, dual-use technologies, emerging technologies and commercially sensitive research areas. The advice has been produced in consultation with the research and university community and is designed to help the UK's world-leading research and innovation sector get the most out of international scientific collaboration whilst protecting intellectual property, sensitive research and personal information.

Trusted Research:

- Outlines the potential risks to UK research and innovation.
- Helps researchers, UK universities and industry partners to have confidence in international collaboration and make informed decisions around those potential risks.
- Explains how to protect research and staff from potential theft, misuse or exploitation.

In addition to the Trusted Research for Academia guidance the UK has produced Trusted Research for Senior Leaders, which outlines some key considerations for leaders in academia, Trusted Research Countries & Conferences, which provides threat information and practical mitigations to implement when travelling overseas, alongside a Trusted Research checklist for use by researchers at the outset of any collaboration.

United States – Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education

(2) Identify and share information on which research areas are at risk

In June 2023, the United States Department of Defense (DoD) introduced a Department-wide policy on reviewing fundamental research projects for conflicts of interest arising from foreign influence. The policy is accompanied by two documents:

- The "Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions" and
- The "Fiscal Year 2022 Lists Published in Response to Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 as amended."
    - Includes lists which identify foreign institutions that have been confirmed as engaging in problematic activity, and foreign talent programs that have been confirmed as posing a threat to the national security interests of the United States.

DoD will follow these policies for risk-based security reviews of fundamental research project proposals to mitigate potential research security risks. DoD's goals in conducting risk-based security reviews of fundamental research project proposals are:

- To ensure the security of DoD-funded fundamental research;
- To ensure that covered individuals fully disclose information that can reveal potential conflicts of interest and conflicts of commitment; and,
- To provide clear messaging to those conducting fundamental research on acceptable and encouraged behaviors as well as activities that may lead to challenges in securing DoD research funding.

Risk-based security reviews will be conducted, at a minimum, on all fundamental research projects proposals that are selected for award based on technical merit.

France – Protection of the Scientific and Technical Potential of the Nation

(2) Identify and share information on which research areas are at risk

The nation's scientific and technical resources comprise all the tangible and intangible assets required for scientific activity (fundamental or applied) and technological development. The essential elements of these resources form an integral part of the nation's fundamental interests, as defined in article 410-1 of the French Criminal Code.

The system for the Protection of the Scientific and Technical Potential of the Nation (PPST) aims to protect the most "sensitive" knowledge, expertise and technologies of public and private establishments (research laboratories, companies, etc.) located on national territory, the misappropriation or capture of which could :

- Harm the nation's economic interests;
- Strengthen foreign military arsenals or weaken French defense capabilities;
- Contribute to the proliferation of weapons of mass destruction and their means of delivery;
- Be used for terrorist purposes in France or abroad.

This system is based on article 413-7 of the French Criminal Code, and is organized around three main implementing texts:

- Decree no. 2011-1425 of November 2, 2011 ;
- The Prime Minister's order of July 3, 2012;
- An interministerial circular dated November 7, 2012.

In concrete terms, the PPST offers legal and administrative protection to covered entities, and enables them to :

- control physical and logical access to certain areas, known as "restricted zones" (ZRR), by seeking the opinion of the relevant ministry;
- provide legal protection against malicious acts affecting the entity's reputation and competitiveness (fraudulent use of information, theft or capture of

sensitive data, anti-competitive practices, intrusion into information systems, etc.);
- benefit from government support in raising the entity's level of security;
- build a responsible work team aware of protection issues;
- be part of a trusted community that encourages research and industrial partnerships.

The PPST is a living system that adapts to contemporary concerns. Two decrees, published in March 2022, will further optimize the processing of requests for access in ZRRs, in order to reduce the time required to process notices relating to requests for access, without compromising the necessary vigilance.

In this way, the PPST contributes to the protection of the nation's fundamental interests, and is also a tool at the service of the establishments concerned, to protect their sensitive knowledge and know-how.

Canada – The National Security Guidelines for Research Partnerships

(3) Identify areas of risk activity by conducting due diligence and ensuring transparency and the disclosure of relevant information

In July 2021, the Government of Canada introduced the National Security Guidelines for Research Partnerships (the Guidelines) to integrate national security considerations into the development, evaluation and funding of research partnerships. The Guidelines were developed in consultation with university representatives and better position the research community to undertake consistent, risk-targeted due diligence on risks to research security.

Applicants to research funding programs where the Guidelines apply must submit a Risk Assessment Form, including a risk mitigation plan. Applicants are required to be transparent in assessing:
- whether their research area has the potential for both military and civilian applications (i.e., is dual-use) or could be targeted by foreign governments, militaries their proxies or other actors to advance their national security capabilities and interests; and
- whether the proposed research partner poses a risk to national security.

National security risks may be described as, but not limited to, potential instances of foreign interference, espionage, intellectual property theft or unauthorized knowledge transfer that:
- contribute to the advancement of military, security, and intelligence capabilities of states or groups that pose a threat to Canada; or
- disrupt the development of Canadian research, weaken the resiliency of critical infrastructure, or jeopardize the protection of sensitive data of Canadians.

Funders conduct an administrative risk validation using open-source information to ensure application accuracy, and where necessary, refer applications to national security departments and agencies for risk assessment and advice. Recognizing that

security risks evolve and can come from anywhere in the world, the Guidelines are country-and company-agnostic with risk assessments conducted on a case-by-case basis.

The Guidelines work to ensure Canadian research is as open as possible and as secure as necessary, and recognize the shared responsibility of due diligence amongst researchers, research institutions, funders and government. Applications for research partnerships that are assessed to present an unacceptable risk to national security or where risks cannot be appropriately mitigated, are not funded.

Japan - Checklist for New Risks Associated with Increasing Internationalization and Openness of Research

(3) Identify areas of risk activity by conducting due diligence and ensuring transparency and the disclosure of relevant information

In recent years, there have been concerns of damage to the values, such as openness and transparency, which form the base of the research environment, and the danger of researchers unintentionally falling into conflicts of interest and commitment due to the new risks associated with internationalization and increasing openness of research activities. Under such circumstances, the Policy Directions for Ensuring Research Integrity in Response to New Risks Associated with Increasing Internationalization and Openness of Research Activities was released at the Integrated Innovation Strategy Promotion Council on April 27, 2021, as government measures related to ensuring research integrity.

Based on the Policy Directions, the Cabinet Office created a checklist template for researchers and a checklist template for universities and research institutes in December 2021, which can be used for training and other purposes to raise awareness among researchers, universities and research institutions.

Checklist templates consist of questions to ensure the management of the following, from the standpoints of researchers as well as universities and research institutions:

- Risks including mismanagement of conflicts of interest and commitment, risks leading to technology outflows and information leaks, and deteriorating trust,
- Procedures for collaboration and agreement with foreign organizations or universities and offering of compensations and goods from foreign countries, and;
- Risks related to counterparts of collaborations and agreements with foreign organizations or universities.

Subsequently, the checklist template for universities and research institutes was revised in June 2023, following an incident of alleged violation of the Unfair Competition Prevention Act.

It is desirable that universities and research institutes use the templates to create their own, accommodating their specific requirements and circumstances.

Italy - National Research Programme: National Plan for Open Science

(4) Implement risk mitigation measures, both as standard organizational practice and for individual research projects.

In June 2022, the Italian Government published the "National Plan on Open Science" (*Piano Nazionale Scienza Aperta*), as a reference document in support of efforts that the Italian scientific community has been deploying in this domain over the past years, such as:

- Multiple Italian universities joining the EU's Coalition on Advancing Research Assessment (CoARA). The Agreement on Reforming Research Assessment sets a shared direction for changes in assessment practices for research, researchers and research performing organisations, with the overarching goal to maximise the quality and impact of research.
- CoARA; focus groups were launched by the permanent conference of the Italian university principals.
- The "Italian Reproducibility Network" was launched in early 2023. This non-profit organization aims to promote, support and guard open science practices through a number of outreach and educational activities.

The National Plan on Open Science makes up several components of the Open Science approach, such as:

- No-paywalls for accessing academic papers,
- Accessible data and code,
- An evaluation system of the Italian universities, and;
- Ensuring the security and integrity of the research ecosystem.

The document sets a clear direction, while leaving room for the community to devise systems of rules and incentives that would comply with the approach. From this perspective, the National Plan is only a first step, and much work is still necessary to promote and adopt the necessary changes towards a transparent, trustable and fair research community.

Germany

(4) Implement risk mitigation measures, both as standard organizational practice and for individual research projects.

More than 120 research institutions, organizations and professional societies in Germany have installed local Committees for Ethics in Security-Relevant Research (KEFs, German acronym) to advise researchers and research institutions on questions concerning security-relevant aspects of their research. The committees were established in accordance with the "Recommendations for Handling of Security-Relevant Research", which were introduced in 2014 by the German National Academy of Science Leopoldina and the German Research Foundation (DFG), and updated in 2022. The recommendations are meant to strengthen awareness in the academic sector and the self-governance of science regarding security-relevant research issues. According to the recommendations, security-relevant research includes

scientific work that has the potential to produce knowledge, products or technologies that can be misused by third parties to harm human dignity, life, health, freedom, property, the environment or peaceful coexistence. This kind of research is designated as "of concern", if the misuse can be immediate and the potential damage is significant.

Since KEFs are usually interdisciplinary, they contribute with relevant expertise, such as from ethics, law and the humanities, in weighing risks and benefits in security-relevant research questions. They raise the researchers' awareness on security-relevant aspects of their work, for instance by offering advice and regular events on research areas at risk of misuse. They are an important instrument for strengthening researchers' responsibility in dealing with risks of misuse in their research and mitigating these risks, e.g., through counseling and competence building. Furthermore, they help to contextualize research projects ethically and thus contribute to a better reviewing of funding applications in research areas that are particularly at risk of abuse. Moreover, KEFs can legitimize security-relevant research through ethical evaluations as part of their consultations. By providing transparency and promoting ethical reflection, KEFs help strengthen public confidence in research as well.

The establishment and work of the KEFs is supported by the Joint Committee on the Handling of Security-Relevant Research, an advisory body established by the DFG and the Leopoldina in 2015. The joint committee hosts regular events to promote exchange among the KEFs, build their competences and raise awareness on current research area of high risk.