1E03

# Institutional Leadership Challenges in Research Integrity and Research Security: Emerging institutional responsibilities in higher education research

○Takehito Kamata (Sophia University)
takehitokamata@sophia.ac.jp

## 1. Introduction

In the realm of research integrity and security, each nation has established frameworks aligned with national priorities and governance structures. Policymakers and leaders at the national level have collectively developed a consensus on research integrity and security. To adhere to this international consensus, institutional leaders such as university presidents, provosts, and research vice presidents are expected to address the harmonization of international standards. This involves moving beyond policy statements to practical coordination mechanisms that encompass both traditional research integrity principles and emerging security threats, thereby maintaining the credibility of research communities.

University presidents, provosts, and research vice presidents encounter complex strategic challenges that require integrating openness and security. These leaders must reconcile the aspirations of open science with security measures such as export restrictions, partner due diligence requirements, and disclosure obligations. Effective responses require the development of new competencies across diverse stakeholder groups. Institutional leaders must possess strategic risk management skills, cross-departmental coordination capabilities, and crisis management expertise.

In this study, I investigate the convergence of integrity and security challenges, highlighting how universities balance academic openness and protection requirements while navigating evolving policy landscapes. The primary objective is to provide academic policymakers, university administrators, and researchers with insights into the integration of ongoing research integrity initiatives and forthcoming research security endeavors. This information will serve as a guiding framework for policy implementation at the institutional level. I also seek to identify the roles universities have adopted and the knowledge and skills university leaders need to facilitate the integration of research integrity and security, with emphasis on research security.

## 2. Historical Background

National policymakers and leaders at the national and international levels have initiated cross-border efforts to transform the research policy framework. This transformation entails moving from compliance-based models to governance systems that integrate research security with traditional research integrity challenges. Implementation of these changes progressed between 2019 and 2025. Notably, concerns raised in a 2018 letter by Dr. Francis Collins, director of the National Institutes of Health, regarding unexpected foreign influences on government and federally funded research in the United States, garnered attention from both the domestic and international research communities [1].

Following Dr. Collins's letter, institutions faced an unprecedented convergence of challenges and were compelled to safeguard against misconduct, foreign interference, and cyber threats while preserving the openness indispensable for scientific advancement. Regulatory inconsistencies across jurisdictions created challenges for policymakers, necessitating cooperation and compliance. They engaged in discussions and negotiations to address research policy gaps and establish a common consensus on definitions of research integrity and security, grounded in diverse national and legal frameworks [2, 3, 4].

The G7 Security and Integrity Working Group, established in 2021, published *Common Values and Principles on Research Security and Research Integrity* (2022) and *Best Practices for Secure and Open Research* (2023) [5, 6]. These publications emphasized that openness and security are mutually reinforcing rather than contradictory; however, this approach sometimes undermined the

stability of international research collaboration. In addition to international consensus, policymakers and national leaders developed and implemented research security policies tailored to national interests. The following sections present national approaches by the United States, Canada, and Japan.

The United States led with National Security Presidential Memorandum 33 (NSPM-33) in January 2021. This memorandum established mandatory requirements for institutions receiving more than $50 million in federal research funding. Its four core elements are cybersecurity, foreign travel security, insider threat awareness and identification, and export control training [7]. Institutions created centralized structures requiring the appointment of research security officers, directly accountable to senior leadership, typically the chief research officer or the vice provost for research. The primary responsibility of these positions was to coordinate multidisciplinary workgroups that included representatives from sponsored projects, IT security, legal affairs, and compliance. For example, in anticipation of these requirements, Northwestern University and the University of Maryland launched detailed research security training programs in 2025. These programs include scenario-based learning on foreign travel precautions, data protection, and insider threat awareness [8, 9].

Canada established the Tri-Agency Framework in May 2024 through coordinated policies from the Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council, and Social Sciences and Humanities Research Council. The Policy on Sensitive Technology Research and Affiliations of Concern prohibited funding when researchers maintained affiliations with organizations connected to foreign military entities [10]. This policy was based on Canada's 2021 National Security Guidelines for Research Partnerships, which required funded projects with private partners to undergo national security risk assessments [11]. Canadian universities operated under coordinated tri-agency frameworks, integrating research security functions through existing vice presidents' research offices rather than by creating separate positions. In addition, the U15 group of research-intensive universities collaborated with the federal government to address research security and published *Safeguarding Research in Canada: A Guide for University Policies and Practices*, a national framework harmonizing open science with security [12].

Japan's Economic Security Promotion Act of 2022 supported private sector economic security management through the development of critical technologies. The act identified 25 critical technology fields requiring enhanced due diligence and outlined 50 key technology areas across maritime, space, aviation, cyberspace, and biotechnology sectors [13]. Approximately $3.5 billion was allocated for research and development in these areas. Although primarily targeting the private sector, the act indirectly influenced academic policy development in these areas. Additionally, the University Research Security and Integrity Consortium, "Team Japan," formed by university leaders in Japan [14], made progress in knowledge sharing among the member institutions. Drawing on insights and lessons from policymakers and university leaders in Canada and the United States, Japanese leaders advanced research security and promoted research integrity.

The convergence of national frameworks through initiatives such as the G7 Virtual Academy and toolkit systems exemplifies recognition that research security challenges transcend borders. Universities must develop integrated competency frameworks addressing both compliance requirements and collaborative research needs. Institutional leaders, researchers, and support professionals should use resources from the G7 Virtual Academy and toolkit systems to understand ongoing and emerging concerns at their institutions [15].

## 3. Challenges and Policy Gaps on Research Integrity

Beyond traditional research integrity challenges aimed at preventing misconduct and questionable practices, institutions have faced growing risks from foreign interference and cybersecurity threats, particularly state-sponsored activity and unauthorized information transfer since 2018. The absence of standardized due diligence protocols and risk screening created vulnerabilities that eroded trust among collaborators at individual, institutional, sectoral, and national levels.

Data protection and export control regulations posed compliance challenges for researchers and

stakeholders [16]. High-profile retractions underscored the need for greater oversight and transparency in research publishing [17]. Simultaneously, weak conflict-of-interest management systems and limited information sharing between institutions and government agencies hindered effective management of research integrity challenges.

## 4. Challenges and Policy Gaps on Research Security

Growing awareness of foreign interference in academic research has elevated research security to a critical concern. The OECD's 2022 report, *Integrity and Security in the Global Research Ecosystem*, identified fragmented coordination frameworks as major obstacles to research security. The field involves stakeholders across civil security, cybersecurity, defense, education, and international affairs. These groups highlighted institutional gaps, especially weak due diligence for assessing foreign interference risks and poor risk identification for critical assets and vulnerabilities. Universities often lacked monitoring systems for international collaborations, limiting their ability to detect evolving risks. Smaller teaching-focused institutions faced resource challenges, resulting in insufficient personnel and funding for comprehensive security programs.

## 5. Essential Knowledge and Skills for Research Integrity

Institutional leaders recognized the need for personnel to understand research integrity principles, national regulations, and institutional policies to address inconsistencies across organizations—such as conflict-of-interest management, definitions of misconduct, and due diligence processes [18]. The most successful institutions created research integrity officer positions with leadership responsibilities for oversight, policy implementation, and misconduct investigations. These officers also address broader concerns, including authorship disputes, questionable research practices, and misconduct allegations. Scholars increasingly view integrating research integrity and research security as an institutional responsibility essential for collaborative research across institutions and nations [19].

A comprehensive understanding of regulatory and policy frameworks is critical. Personnel must define misconduct, understand national and international codes of conduct, and navigate requirements such as conflict-of-interest regulations and data management mandates. For example, familiarity with the U.S. Office of Research Integrity guidelines and the European Code of Conduct is a vital asset for researchers, research support professionals, and institutional leaders globally [20, 21].

## 6. Essential Knowledge and Skills for Research Security

In this section, I will outline the required knowledge and skills for academic leaders at higher education institutions. These elements are essential for institutional leaders and research security professionals in academia [2, 15, 19].

### *Engaged Leadership and Governance Within and Beyond the Academic Sphere*

Executive-level coordination, cross-departmental integration, and the ability to establish security-conscious cultures while preserving institutional autonomy will be crucial. Individuals capable of developing institutional policies; integrating security into governance; and leading cultural change, grounded in strategic thinking, are essential. They should understand research security, research integrity, compliance, and academic freedom.

### *Risk Assessment and Due Diligence Through a Global Perspective*

Systematic evaluation of international and domestic partners and projects is paramount for promoting research security. Individuals with knowledge of research support services, due diligence procedures, intelligence gathering, and identification of potential threats across nations are indispensable.

### *Cybersecurity and Data Protection*

Personnel should have the technical expertise to implement advanced cybersecurity measures and ensure compliance with data and information protection regulations, including data governance requirements, cross-border transfer rules, secure data-sharing platforms, and international privacy laws. Advanced procedures such as multifactor authentication, real-time threat detection, and incident response planning should be implemented at all universities [16].

*Legal and Regulatory Compliance Across Multiple Jurisdictions*

Individuals should understand relevant laws and regulations, including export control regimes, sanctions lists, and sponsor requirements. This knowledge is crucial for managing conflict-of-interest disclosure and ensuring institutional compliance across jurisdictions. Leaders in research security must be proficient in disclosure management, conflict-of-interest identification, and transparent reporting mechanisms based on research integrity principles.

## 7. Conclusion

To maintain institutional credibility and cultivate trust within global research communities, engaged leadership and governance commitment within and beyond academia are essential. This commitment requires broad perspectives on risk assessment and due diligence, a strong understanding of cybersecurity and data protection, and knowledge of legal and regulatory compliance across jurisdictions.

## References


[1] F. Collins, Letter (Dear Colleagues:), National Institutes of Health, Department of Health and Human Services, The United States, (2018). https://www.insidehighered.com/sites/default/files/media/NIH%20Foreign%20Influence%20Letter%20to%20Grantees%2008-20-18.pdf

[2] Organisation for Economic Co-operation and Development, Integrity and security in the global research ecosystem, OECD Publishing, (2022). https://doi.org/10.1787/1c416f43-en

[3] G7 Science and Technology Ministers' Communique, G7 Science and Technology Ministers' Communique, Cabinet Office, Government of Japan, (2023). https://www8.cao.go.jp/cstp/kokusaiteki/g7_2023/230513_g7_communique.pdf

[4] G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, G7 Best practices for secure and open research, G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, (2024). https://science.gc.ca/site/science/sites/default/files/documents/1136-g7-best-practices-for-secure-and-open-research-february-2024.pdf

[5] G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, G7 Common Values and Principles on Research Security and Research Integrity, G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, (2022). https://www8.cao.go.jp/cstp/kokusaiteki/integrity/g7_sigre_values_en.pdf

[6] G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, G7 Best practices for secure and open research, G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, (2023). https://www8.cao.go.jp/cstp/kokusaiteki/g7_2023/2023_bestpracticepaper.pdf

[7] The White House, National Security Presidential Memorandum 33: U.S. Government-supported research and development [Memorandum], The White House, (2021). https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

[8] Northwestern University. Research security training plan – Standard operating procedure (v. Aug 2025). Northwestern University, (2025). https://researchsecurity.northwestern.edu/docs/research-security_sop_082725.pdf

[9] University of Maryland. Research security training. Research and Development, University of Maryland, (2025). https://www.umaryland.edu/ord/umb-research-security-program/research-security-training/

[10] Government of Canada, Policy on Sensitive Technology Research and Affiliations of Concern, Minister of Innovation, Science and Economic Development Canada, Government of Canada, (2024). https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern

[11] Government of Canada, National Security Guidelines for Research Partnerships, Minister of Innovation, Science and Economic Development Canada, Government of Canada, (2024).

https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships
[12] U15 Canada, Safeguarding Research in Canada: A Guide for University Policies and Practices, Government of Canada, (2023). https://science.ised-isde.canada.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/guidance-research-organizations-funders-and-universities/safeguarding-research-canada-guide-university-policies-and-practices
[13]. S, Nagino and B, Glosserman, PacNet #34 – Japan sets the pace for private sector economic security management, Pacific Forum. https://pacforum.org/publications/pacnet-34-japan-sets-the-pace-for-private-sector-economic-security-management/
[14] Institute for Future Initiatives, The University of Tokyo, U.S.-Canada-Japan International Workshop on Research Security and Integrity (※By invitation only), Institute for Future Initiatives, The University of Tokyo, (2025). https://ifi.u-tokyo.ac.jp/en/event/13105/
[15] G7 Security and Integrity of the Global Research Ecosystem (SIGRE), G7 Virtual Academy on Research Security and Integrity, G7 Security and Integrity of the Global Research Ecosystem (SIGRE), (2025). https://europa.eu/sinapse/sinapse/community/0505f60a-287b-11ed-b6d0-0050568bf5be/login
[16] B. Wolford, What is GDPR, the EU's new data protection law?, GDPR.EU, (2025). https://gdpr.eu/what-is-gdpr/
[17] R. V. Noorden, More than 10,000 research papers were retracted in 2023 — a new record, Nature, 624, 479-481 (2023). https://doi.org/10.1038/d41586-023-03974-8
[18] J. L. Briskin and C.K. Gunsalus, Fostering Accountability: How Institutions Can Promote Research Integrity with Practical Tools and Knowledge, The Journal of Law, Medicine & Ethics, 53(1), 67–73, (2025). https://doi.org/10.1017/jme.2025.40
[19] K. R. Gamache, B. Applewhite, J. Bruegger, E. Carlisle, T. Clark, D. Gifford, B. Kozisek and P. C. Nunn, Safeguarding Research Integrity and Security in the Global Research Ecosystem (Final Report), Bush School of Government & Public Service, Texas A&M University, (2025). https://bush.tamu.edu/wp-content/uploads/2025/06/Gamache_EMPSA-Final-Report_Safeguarding-Research-Integrity-Security_24-25.pdf
[20] Office of Research Integrity, Department of Health and Human Services, The United States, Guidance Documents, Office of Research Integrity, Department of Health and Human Services, The United States, (2025). https://ori.hhs.gov/guidance-documents
[21] ALLEA: All European Academies, European Code of Conduct for Research Integrity – Revised Edition 2023, ALLEA: All European Academies, (2023). https://www.eua.eu/news/member-and-partner-news/european-code-of-conduct-for-research-integrity-revised-edition-2023.html