Research security at Swinburne

Secure, compliant and globally responsible research at Swinburne

swinburne.edu.au/research/security

Swinburne University of Technology

Securing our research

Australia's research environment is increasingly shaped by national security, foreign interference and critical technology considerations. Swinburne operates within a complex and evolving regulatory landscape, with multiple frameworks including the University Foreign Interference Taskforce (UFIT) Guidelines, Defence Trade Controls Act, and Foreign Influence Transparency Scheme—requiring active management of research security risks.

In response, Swinburne has adopted a risk-based, proportionate approach to research security, balancing the benefits of international collaboration with the need to safeguard intellectual property, critical technologies and institutional integrity. This approach is embedded across the research lifecycle, including staff declarations, HDR students, grant submissions, partner due diligence, and oversight of visiting and adjunct researchers.

The Australian Research Council (ARC) Research Security Framework (2026) represents a step-change in expectations, with strengthened requirements for transparency, due diligence, and institutional accountability. Security assessments are now integrated into grant evaluation, with the potential for funding veto, additional conditions, or clawback where risks are identified. This is driving a significant increase in compliance obligations and scrutiny across the sector.

Swinburne has strengthened its capability through targeted tools and processes, including the Dimensions Research Security module and selective use of external intelligence sources such as the ASPI University Tracker. These support identification of potential risks in collaborations, affiliations and funding sources, although expert review remains essential.

A key area of focus is Defence Export Controls (DEC), which now apply broadly to research involving dual-use or sensitive technologies. These controls extend beyond physical exports to include data sharing, collaboration, and publication, with significant compliance obligations and penalties for breaches.

Ongoing staff awareness, targeted training, and sector engagement further strengthen the university's ability to manage evolving risks.

Overall, research security is now a core institutional requirement. Swinburne's approach positions it to support secure, ethical and globally engaged research, while meeting increasing government expectations and protecting Australia's national interest.

Professor Karen Hapgood
Deputy Vice-Chancellor, Research

Research security in Australia

Our research security obligations

Australia's research and innovation sector is globally recognised for its research excellence and makes a significant contribution to national prosperity and innovation. However, the Australian government continues to warn the sector that strategic rivals are targeting Australia's critical technology expertise where there are potential commercial or military applications.

Multiple Australian Government agencies are involved in maintaining research security. Swinburne University of Technology is responsible for safeguarding our research and complying with all regulatory requirements. Currently there are 11 different regulations, legislative requirements and frameworks to be considered:

- University Foreign Interference Taskforce Guidelines to Counter Foreign Interference in the Australian University Sector (Department of Home Affairs)
- Australian Research Council Research Security Framework (Department of Education)
- Autonomous Sanctions Act 2011 (Department of Foreign Affairs and Trade)
- Protecting Australia's Critical Technology regulations (Department of Home Affairs)
- Critical Technology Framework (Department of Industry, Science and Resources)
- Defence Trade Controls Act 2012 (Department of Defence)
- Defence Act 1903, including the Safeguarding Australia's Military Secrets (SAMS) amendments
- Defence Industry Security Program (Department of Defence)
- Defence Research, Innovation and Collaboration Security Program (Department of Defence)
- Australia's Foreign Relations (State and Territory Arrangements) Act 2020 (Department of Foreign Affairs and Trade)
- Security of Critical Infrastructure Act 2018 (Department of Home Affairs)
- Foreign Influence Transparency Scheme (Attorney-General's Department).

Frameworks also exist internationally that inform university research security responsibilities, such as autonomous sanctions lists of proscribed individuals and entities and the DHA Foreign County List (FCL) which lists countries where DEC permits are not required. Additional expectations may be outlined by the Department of Education on behalf of the Minister or other departments at any time.

Research security is part of our Countering Foreign Interference (CFI) obligations and is important across all areas and disciplines at Swinburne. This includes basic and fundamental research, applied research, industry research, innovation and commercialisation. The requirements are constantly changing and evolving in response to both changes in the geopolitical environment, and in response to improved research security understanding and skills across the Australian Government and university sector.

Critical technologies in the national interest

The List of Critical Technologies in the National Interest has been developed by the Dept Industry Science and Resources (DISR). The list identifies critical technology fields where Australia:

- has research, intellectual or industrial strengths
- national capabilities to be supported and championed
- needs uninterrupted access through trusted supply chains
- must retain strategic capability or maintain awareness.

The current list was updated in 2022 and identifies seven key enabling critical technology fields which have a high impact on Australia's national interest:

- advanced materials technologies
- Artificial intelligence (AI) technologies
- advanced information and communication technologies
- autonomous systems, robotics, positioning, timing and sensing
- biotechnologies
- quantum technologies
- clean energy generation and storage technologies.

For further details on the critical technology fields, explanations and examples, see www.industry.gov.au/publications/list-critical-technologies-national-interest#key-enabling-critical-technology-fields

This list is used by Department of Home Affairs for assessing research security for postgraduate research students study visa requests and any change of PhD topic requests.

National University Forums and Communities of Practice

DFAT have established forums for university representatives to be updated on matters related to research security and preventing foreign interference, including briefings on emerging risks. Swinburne ensures we have representatives attending these events.

Swinburne's risk based approach

Swinburne remains internationally connected, and values the broad expertise, experience and perspectives that our international collaborations – both institutional and researcher-led – bring to our research and innovation ecosystem.

In line with the UFIT Guidelines, Swinburne adopts a proportionate, risk-based approach to research security as summarised in Table 1.

Swinburne's research security tools

For support in understanding potential research security risks, Swinburne has purchased commercial programs and tools to provide up-to-date, open-source information similar to that used by the ARC and other agencies:

Dimensions Research Security Module

Dimensions Research Security module, which leverages the Dimensions database to help identify and manage potential risks related to research collaborations, critical technologies and geopolitical sensitivities. Dimensions Research Security combines open, licensed, and proprietary data to produce risk indicators. Access is limited to a few user licenses in the Research Portfolio. Information provided by this tool often requires further assessment by research or security experts for accuracy and for context. See www.dimensions.ai/sector/academic-institutions/research-security for more information.

ASPI University Tracker

The ASPI University Tracker is a database developed by the Australian Strategic Policy Institute that maps Chinese universities and research institutions linked to military, security and dual-use research, helping universities assess risks in international collaborations and partnerships.

Until mid-2025, the ASPI tracker was publicly available on the internet and was embedded in several research security processes at Swinburne, but was unexpectedly changed to be behind a paywall. This impacted the timeliness of risk assessments in the second half of the year. Swinburne has purchased three licenses which restore sufficient access to assess potential partnerships and collaborations, although the addition of the paywall has had an ongoing negative impact on the ability for individual staff and researchers to assess potential collaboration requests, PhD project proposals or visitor requests and improve general awareness.

Who can raise research security concerns?

Research security queries and due diligence concerns can be raised by the ARC (directly or via Commonwealth agencies); research integrity complaints; whistleblower complaints; investigative journalists; or staff and students.

Recent examples in Australia include Australian researchers allegedly collaborating with Iran on drone technology, a photonics researcher with Russian links, and multiple direct collaborations with Chinese defence universities.

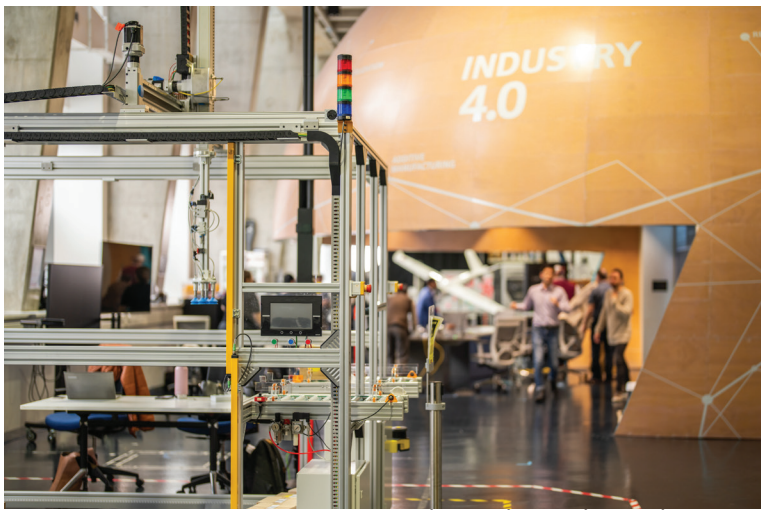

Table 1: Summary of Swinburne's risk-based approach to research security

Touch point	High level approach	Responsibility Lead
Swinburne researchers	• All research staff (including all T&R or RO academic staff and research office staff) are required to complete the annual Declaration of Interests and Probity (DOIP), with specific questions about foreign income and associations, other affiliations, outside employment, talent plans and any other potential conflicts of interest. This mirrors the requirements of the ARC and NHMRC declarations. • Ad-hoc reviews for selected potential recruits to Swinburne based on risk profile can be conducted using Dimensions Research Security (e.g. technology area or known past international collaborations) • Dimensions Research Security software (since 2025) • Documented risk assessments and conflict of interest management plans will be increasingly required to meet government expectations.	Research Services People & Culture Legal Risk & Compliance
Research HDR students	• Pre-offer risk checks for HDR candidates in sensitive research areas using the critical technology list. This applies to candidates located overseas as well as in Australia • Ongoing assessment if project scope, access or technology changes during candidature • International students with a postgraduate research student visa must obtain written approval from the Minister for Home Affairs before changing into a new critical technology-related course of study. Includes changes in proposed PhD thesis titles.	Graduate Research
Research grant proposals	• Research Services has a suite of additional due diligence checks in place for researchers submitting applications, including compliance checks on declared affiliations in the ARC submission portal compared to the staff members DOIP declarations and their Dimensions Research Security profile • The ARC requires this for all CIs on grants we are submitting • Additional assessment of proposed collaborators for proposals that include critical technology are also conducted.	Research Services
Partners due diligence	• Due diligence on new and existing partners (before commencement and throughout partnership based on risk) including foreign ownership checks. Checks apply prior to submission of grant proposals, CRC bids as well as to direct industry research contracts.	Research Services, Business Growth Services
Visiting and Adjunct Researchers	• All Visiting and Adjunct Researcher requests have a requirement for the School Executive Dean or equivalent and DVCR approval, to ensure CFI and research security requirements are considered before appointment.	DVCR and Deans
Sensitive research and technology	• Risk-based assessment based on government sensitive technology lists and risk management plans put in place as required • Defence Export Control assessments and permit requests if needed.	Research, researchers / line manager
Cybersecurity	• Enhance cybersecurity protections, knowledge sharing with sector and government agencies, particularly around data, commercial innovations, technical insights and IP.	Information Technology
Staff awareness and training	• Ongoing Information and awareness raising sessions with supervisors and HDR students are conducted at DVCR Research Forums and Graduate School communications • Targeted guidance and training on research security obligations • More specific and targeted awareness for researchers in defence or higher risk research areas (e.g. quantum, optics, AI, autonomous control etc) is conducted as needed by the Defence Engagement team including the Chief Security Officer and Security Officer, as per our DISP accreditation • Defence Export Controls Outreach information sessions for researchers and HDR students have been held in 2025/2026 and are available online via DEC website.	Swinburne Research
Partnered or Offshore PhD programs	• Due diligence on potential partnerships includes assessment for FITS notifications, autonomous sanctions, and critical technology • Proposed partnerships are reviewed by the Academic Partnerships Committee at the proposal stage as well as at periodic intervals within the partnership • Partnered PhD programs are also reviewed by RQPC and Academic Senate.	Graduate Research
Escalation path	• Each of the processes has an escalation path through to the DVCR, who may seek external or legal advice if required.	DVCR

Research funding and collaborations

Australian Research Council

The ARC issued a new ARC Research Security Framework v 1.0 in April 2026.

The ARC has defined four Research Security Principles (see Table 2) which apply across three focus domains: Security, Defence and International Relations (see Table 3).

- **Principle 1:** Advance Australia's national interest
- **Principle 2:** Research security is a shared responsibility
- **Principle 3:** Proportionate, risk-based decision-making
- **Principle 4:** National and global responsibility.

The ARC draws on open-source information (similar to Dimensions Research Security tool) to identify undeclared researcher affiliations and/or undeclared or concerning foreign research funding as their main risk indicators, mostly in critical technology fields.

Security checks are conducted by the ARC in parallel with peer review and grant assessment. The Minister has the power to veto research funding requests on national security grounds and recently exercised this power.

The ARC also has the power to add additional clauses to the funding conditions regarding national security, as well as to retrospectively withdraw and reclaim funding for grants in its National Competitive Grants Program where there are sufficient security concerns.

Administering organisations for ARC grants are now required to validate researcher affiliation and conflict of interest declarations and seek specific assurance on risk mitigations from all researchers on the grant, not just the researchers at the administering institution. This applies to the proposal stage as well as to any funded grants.

The scope of ARC due diligence requests is often wider than security frameworks suggest, including examining CIs and co-authors on previous papers which list ARC funding where the co-authors may have received defence or talent plan funding from a country that Australia does not have bilateral relations with. The acknowledgements sections of many papers acknowledge the funding sources for all the co-authors but do not always state which co-author received which funding.

Further, even if it is clear that the foreign/defence funding is connected to a co-author and not an ARC CI, the ARC requires additional assurances from Swinburne that the research security aspects of the project will be managed appropriately to prevent IP leakage via these collaborations. This type of concern is the hardest to address and resolve and a documented assessment process is now required.

New research security processes to enable Swinburne to address these new requirements will be developed in the second half of 2026.

NHMRC and other funding schemes

All Australian funding bodies will be required to implement research security measures similar to the ARC. Legislation to introduce requirements to the NHMRC are in progress, although the NHMRC may choose a different implementation approach to meet the requirements. Therefore, it is useful for all researchers to consider and actively manage research security, especially in fields connected to critical technologies.

Industry partners

All new and existing industry partners (including for-profit, not-for-profit, Australian and international companies) undergo routine due diligence checks as part of the proposal submission or contract review process – these include reputation, financial stability, source of funds, and compliance with regulatory requirements. Research security also requires checks on foreign ownership, source of funds, critical technology considerations and Defence Export Controls for example.

These checks apply prior to submission of grant proposals, CRC bids as well as to direct industry research proposals, tenders and contracts. They occur at the pre-award stage, but additional review can occur at any time throughout partnership based on changes in potential risk or research security requirements. These are a minor impact on grants and contracts processing time, unless potential research concerns are identified. This triggers a risk assessment and management plan, which requires careful consideration and may require Swinburne to seek additional advice and guidance.

ARC Research Security Principles

Table 2: Summary of Swinburne's risk based approach to research security

Principle 1: Advance Australia's national interest

- International research collaborations make significant contributions to the quality and impact of Australia's research sector by supporting access to world-leading expertise, shared resources and increased visibility. International collaboration will be supported where the associated risks are appropriately managed.
- ARC-funded research is expected to have a clear short or longer-term benefits to Australia and be consistent with Australian Government policy objectives, including those relating to security, defence and international relations.
- ARC funded research needs to be appropriately protected to ensure the Australian Government's investment in research and development aligns with Australia's national interest. This includes the management of intellectual property arising from ARC grant opportunities. Protections are particularly important within the context of research relating to critical technologies or with dual-use potential.
- Where risks to Australia's security, defence or international relations cannot be effectively mitigated, or where residual uncertainty remains material, the benefit of the doubt will be afforded to the national interest.

Principle 2: Research security is a shared responsibility

- Research security is a collective responsibility shared between individual researchers, universities and cross-government stakeholders.
- ARC research security activities complement risk mitigation efforts undertaken across the Australian Government and by Australian universities. The ARC's risk assessment processes are based on an understanding that other parts of the national research security ecosystem are operating effectively.
- University compliance with Australian Government policies, frameworks and programs designed to manage research security risks is assumed. Relevant frameworks include, but are not limited to, the University Foreign Interference Taskforce Guidelines, the Foreign Arrangements Scheme and the Defence Trade Controls Act 2012. ARC risk assessments are informed by advice from relevant parts of government, where required.
- Secure and open research depends on rigorous transparency from researchers, assessors and universities. Full and forthright declarations of foreign affiliations, associations and funding is foundational to the maintenance of trust in ARC processes and across Australia's research and innovation ecosystem.

Principle 3: Proportionate, risk-based decision-making

- Research security risks cannot be eliminated but must be managed in a manner proportionate to the potential threat. ARC risk assessments will involve a balanced consideration of ARC objectives to promote innovation and productivity against potential threats, with higher risk cases receiving greater scrutiny.
- ARC research funding is awarded to Australian universities for the purpose of early-stage research with research outcomes generally intended for open access publication. The nature, value, duration and scale of the project inform proportionate assessments of risk.
- ARC research security assessments are informed by available information and advice. Relevant government agencies may assist in providing case-specific or general advice related to their portfolio expertise to support decision-making.
- ARC risk assessment frameworks will be regularly reviewed to reflect emergent geopolitical threats, the evolving research and development landscape and changes to Australian Government advice.

Principle 4: National and global responsibility

- ARC funded research is expected to be consistent with Australia's status as a responsible global actor, including adherence to the highest ethical, legal and social standards.
- Aligning the Australian Government's investment in university research to the core values of a transparent and ethical global research ecosystem builds trust both domestically and internationally. Funded projects need to be safeguarded against misuse.
- Australia will continue to demonstrate international leadership by embedding global responsibility into ARC decision-making.

Source: ARC Research Security Framework Version 1.0 Effective April 2026. Revision June 2027

ARC Research Security Focus Domains

Table 3: Responsibility, risk indicators and focus domains that inform ARC risk assessments

Security domain

The protection of the nation's territory, institutions, and the safety of all Australians. This includes safeguarding against threats such as terrorism, foreign interference, espionage, cyberattacks, and harm to critical infrastructure.

Objectives:

- Transfers of intellectual property are appropriately regulated
- Covert influence of international actors on ARC research is minimised
- Academic freedom of enquiry and Australia's inclusive national identity built around our shared values are supported
- University critical infrastructure, resources and data are used appropriately.

Risk indicators may include, but are not limited to:

- The extent, nature and currency of affiliations with foreign institutions (e.g. appointments, talent plan participation, funding sources)
- The extent, nature and currency of collaboration networks (co-authors, recruitment, supervision)
- Relevance to critical technology, technological readiness level and the potential for unwanted transfers of research outcomes
- The accuracy, currency and completeness of information provided to the ARC in terms of international affiliations, associations and funding.

Defence domain

Strategic, military, industrial, and policy measures required to ensure Australia can resist coercion, contribute to regional stability, and, if necessary, conduct armed conflict in support of national objectives.

Objectives:

- Research with potential for dual-use is identified and managed appropriately.

Risk indicators may include, but are not limited to:

- Extent, nature and currency of affiliations with defence, military and/or intelligence linked institutions
- Research and funding history, such as previous projects involving funding from defence, security or military institutions
- Research that relates to defence-related outcomes or has dual-use potential.

International relations domain

Advancing Australia's interests globally through diplomacy, trade, development, security cooperation, and coordinated engagement with international partners.

Objectives:

- ARC funding arrangements support individuals, organisations and nations in a manner consistent with Australia's status as a responsible global actor
- ARC funded research and research partnerships are consistent with sanctions law and international agreements
- ARC funded research and research partnerships strengthen and protect Australia's bilateral relationships.

Risk indicators may include, but are not limited to:

- Extent, nature and currency of affiliations or collaboration networks with proximity to actors involved in human rights violations
- Extent, nature and currency of affiliations or collaboration networks with proximity to sanctioned activities, nations, organisations or individuals
- Extent, nature and currency of affiliations or collaboration networks with proximity to actors involved in foreign interference activities
- Potential for project participants and/or the research project to contribute to bilateral sensitivities.

Source: ARC Research Security Framework Version 1.0 Effective April 2026. Revision June 2027

Defence and security

Defence Industry Security Program (DISP)

Swinburne's defence collaborations are based around the "Detect and Protect" framework. DSTG and the Department of Defence require all universities conducting research and innovation in partnership with defence to be accredited under the DISP program.

Defence Export Controls

Australia's defence export controls regulate the transfer of certain goods, technologies and knowledge to ensure they are not used in ways that could harm national security or support military or weapons programs

These controls apply to items listed on the Defence and Strategic Goods List (DSGL), which includes both defence items and dual use technologies (i.e. civilian research with potential military application, such as AI, advanced materials or cryptography).

Export controls apply to more than physical exports, including:

- Sharing research data, software or technical know-how
- Providing access to controlled information (including in person, via email, cloud or collaboration tools)
- Working with international collaborators or students
- Publishing or presenting certain controlled technologies.

Under the Defence Trade Controls Act 2012, staff may need a permit from Defence Export Controls before:

- Sending controlled items overseas
- Sharing controlled technology with people outside Australia
- Providing access to certain controlled technologies to foreign nationals in Australia.

No DEC permit is required for researchers or staff working or supporting projects covered by the DSGL list who are:

a. Australian Citizens or Permanent Residents, or

b. citizens or permanent residents of the 31 countries listed on the Foreign Countries List (FCL), available at www.legislation.gov.au/F2024L01019/asmade/text

Recent DEC reforms have simplified some collaboration with the UK and US (AUKUS partners), while introducing new controls on sharing sensitive technologies, including within Australia.

It is important to note that DEC include sensible exemptions for fundamental research and most research that is intended for open publication and has no commercial or other restrictions.

Why DEC matters at Swinburne

Export controls now apply to routine research activities, not just defence projects. Non-compliance can lead to serious penalties for individuals and the university. Early identification of risks is essential—particularly in international collaborations and emerging technology fields.

What staff should do

- Consider whether your research involves dual use or sensitive technologies
- Seek advice before sharing controlled information internationally or with foreign nationals
- Engage with Swinburne's research security/compliance team when unsure.

Please ask us for advice rather than guess

Cybersecurity

Swinburne places a strong emphasis on cybersecurity and is committed to training and protecting its community against cyber threats. This is supported by a proactive monitoring approach, along with ongoing intelligence sharing with the Australian Cyber Security Centre and the broader university sector.

Examples of cyber threats may include:

- security issues with any Swinburne web sites, systems or data stores
- suspicious emails, phishing scams or other unsolicited messages
- suspicious software, spyware or malware on devices
- data breaches or leaks to personal information.

Swinburne enforces cybersecurity through strict IT acceptable use guidelines, including mandatory Multi-Factor Authentication (MFA) for system access and the requirement to report all security incidents. These policies are designed to protect personal information, monitor system usage, and prevent unauthorised software or malicious activity, ensuring that Swinburne's digital environments remain secure.

Emerging research security risks

Research security requirements will continue to evolve.

The ARC's new Research Security Framework means a significant increase in research security awareness and activity is required by the Australian university sector.

We anticipate further changes in the future, including new requirements being added by more funding bodies as well as iterative changes to the new ARC Research Security Framework, which is due for review in June 2027, Swinburne's processes will continue to become more formalised and integrated with BAU activities. Some areas where research security will need to be considered in future are outlined below

Researcher to researcher collaboration in sanctioned countries

Recent advice from the Department of Education to all universities regarding collaboration with specific sanctioned countries (Russia and Belarus, Iran and North Korea) extended the previous restrictions to researcher-to-researcher collaborations. This includes any work resulting in co-authoring papers with researchers or partners based in these countries. Limited collaboration via large multinational collaborations (eg WHO, UN, large scientific consortia) may be acceptable provided Swinburne has a documented assessment and risk management process for any papers. Swinburne will implement a process to request DVCR permission before collaborations commence.

International delegation visits

Swinburne often welcomes official delegations and visitors from international universities and governments to our campus to meet our researchers and see our facilities. Researchers also receive requests from delegations and individuals directly, including requests to visit after attending a conference etc. It is likely that research security and CFI will need to be considered more formally in future for delegations or visitors who are from countries that are not on the Foreign Country List (FCL), in order to comply with DEC.

ATEC requirements

In May 2026 the Minister for Education announced that Research Security expectations would be added to the ATEC or TEQSA regulations for all universities. Details of the exact requirements and obligations in the regulations are not yet available.

Glossary of acronyms

- ACSC – Australian Cyber Security Centre
- ARC – Australian Research Council
- ASPI – Australian Strategic Policy Institute
- AUKUS – Australia–United Kingdom–United States security partnership
- CFI – Countering Foreign Interference
- CI – Chief Investigator (on research grants)
- COI – Conflict of Interest
- DEC – Defence Export Controls
- DFAT – Department of Foreign Affairs and Trade
- DISP – Defence Industry Security Program
- DOIP - Declaration of Interests and Probity
- DSGL – Defence and Strategic Goods List
- DSTG – Defence Science and Technology Group
- DTCA – Defence Trade Controls Act 2012
- FITS – Foreign Influence Transparency Scheme
- FCL – Foreign Country List (published by DHA)
- HDR – Higher Degree by Research
- MFA – Multi-Factor Authentication
- NHMRC – National Health and Medical Research Council
- SAMS – Safeguarding Australia's Military Secrets
- UFIT – University Foreign Interference Taskforce.

Enabling safe and responsible collaboration

Research security at Swinburne is not about restricting collaboration—it is about supporting responsible, transparent and ethical research partnerships.

By embedding security considerations into standard research processes, Swinburne helps researchers:

- collaborate confidently with international partners;
- protect themselves and their work;
- meet funding and regulatory obligations; and
- contribute to Australia's research excellence and global engagement.

This balanced approach ensures Swinburne remains a trusted research partner—nationally and globally.

Further information

Email researchsecurity@swinburne.edu.au

Web swinburne.edu.au/research/security