UKRI policy fellowships 2027

Fellowship position

Fellowship title:

BIST research security for digital research infrastructure policy fellowship

Fellowship type:

Core policy fellowship

Host organisation:

Department for Business, Innovation, Science and Trade

Host team:

BIST Public Compute and AI for Science

Academic discipline/s:

HPC, engineering, research security, digital research infrastructure, data science, computer science

Summary:

An opportunity to support BIST to advance its understanding of research security within the digital research infrastructure research and innovation ecosystem.

Policy topic:

Research security in relation to digital research infrastructure (DRI).

Research career stage:

Open to early and mid-career researchers.

Fellowship structure

The fellowship is scheduled to begin on 1 October 2027 subject security clearance requirements. The fellowship will have three phases:

- inception: duration is 3 months at 0.4 FTE
- main placement: duration is 12 months at 0.6-1 FTE
- knowledge exchange: duration is 3 months at 0.4 FTE

Work arrangements

Location requirements:

The team is predominantly London based, with a presence in Edinburgh and Manchester. It would also be possible to work from Government offices in Darlington, Birmingham, Cardiff or Bristol. There would be some requirement to travel to London for key meetings and engagement with members of the wider team approximately six times a year.

Hybrid working:

We would be content for a minimum one day a week office attendance, at any location listed above, during the main placement phase. A laptop will be provided enabling work from home or other sites, providing access to host systems. In addition to office attendance, it would be useful to budget for travel to London around six times in the placement year and once in the inception phase. Eligible Travel and Subsistence costs are supported in the main UKRI grant. Please see full call text and guidance for more details.

Security clearance and nationality eligibility criteria:

Security Check (SC) clearance is required, which usually takes around eight to 12 weeks. We would expect the successful applicant to start the security clearance application process, with support from the host team, as soon as their fellowship has been confirmed by UKRI. Inception phase can begin before the security clearance process is completed but will be required for the main placement phase. The civil service also has nationality requirements that candidates would need to meet in order to take up the post. Please see civil service recruitment nationality rules for further information. Candidates should check these requirements before applying to ensure they meet the eligibility criteria

Successful applicants must also undergo a Baseline Personnel Security Standard (BPSS) check, which usually takes around 6 weeks.

Fellowship position description

This fellowship offers a unique opportunity to support BIST and UKRI to advance its understanding of research security within the digital research infrastructure research and innovation ecosystem. The UK's research and innovation system operates in an increasingly complex international environment, characterised by geopolitical competition, rapid technological development and evolving threats to knowledge, people, data, intellectual property and sensitive technologies. At the same time, international collaboration and the exchange of knowledge and expertise remain fundamental to UK research excellence, innovation and economic growth.

Research security builds trust in research by protecting it from theft, misuse and exploitation which could harm national or economic security. Achieving this requires government, funders, universities and research organisations to develop a shared understanding of risks, opportunities and proportionate mitigations.

Government holds strategic, policy and threat-related expertise, while researchers and organisations hold essential practical knowledge about how research security issues arise within disciplines and technology ecosystems. Existing engagement can be fragmented or dependent on individual relationships, limiting the systematic exchange of sector intelligence, lessons and emerging good practice.

Research security issues can also differ between technologies according to their maturity, applications, international connections, infrastructure, supply chains and routes to commercialisation. BIST therefore requires stronger technology-specific understanding of how risks are experienced and managed, where current arrangements work well and where more tailored policy, guidance or support could be beneficial.

The fellow will bring their expertise and experience into BIST to help translate academic knowledge, sector intelligence and practitioner experience into stronger policy understanding and practical approaches to delivery. They will act as a bridge between government and the wider research community, strengthening two-way knowledge exchange and helping ensure that policy remains grounded. The fellow will also work

closely with UKRI in their respective areas to help ensure effective connections between HMG policy and academic needs with funding approaches and strategic priorities.

The precise focus and approach will be co-designed by the fellow, based on their interests and expertise, and the host team, based on its strategic priorities, during the inception phase. Activities could include stakeholder engagement, evidence reviews, surveys, case studies, ecosystem mapping, quantitative and qualitative analysis, international comparison and horizon scanning. The primary purpose will be to inform policy development, improve understanding of the sector and strengthen practical research security capability.

Areas of interest could include:

- exploring how research security risks and opportunities arise across the research and innovation lifecycle, including partnerships, funding, access to infrastructure, researcher mobility, publication, intellectual property, commercialisation and routes to application;
- examining how researchers, universities, research organisations and businesses currently understand and manage research security considerations, including areas of uncertainty, capability gaps or practical barriers;
- informing research funding approaches and priorities to this research area to ensure they reflect good research security practice and are aligned with wider HMG needs and academic priorities;
- assessing how research security considerations vary across different forms of research, organisations, partnerships and applications, including differences associated with technology maturity, international connectivity and reliance on specialist knowledge, data, facilities or supply chains;
- examining how knowledge, data, intellectual property, people and specialist capabilities move through the ecosystem, and where information asymmetries, dependencies or vulnerabilities may arise;
- exploring how proportionate risk management can enable trusted domestic and international collaboration without creating unnecessary barriers to research and innovation;
- identifying effective mitigations, guidance, case studies, tools or capability-building activities that could support confident and consistent decisions across the research community;
- considering how scientific, technological, commercial and international developments may change the research security landscape and how horizon scanning could improve future preparedness.

The fellowship will help BIST and UKRI strengthen connections with the digital research infrastructure research community; bring academic and practitioner perspectives into policy development; identify emerging risks, implementation challenges and evidence gaps; develop proportionate approaches to protecting strategically important research and capabilities; and inform technology-specific policy, guidance, engagement and capability-building activity.

The fellow’s expertise could contribute through informing research security policy and guidance, shaping funding or sector interventions, identifying priorities for further analysis, developing practical tools and case studies, strengthening horizon scanning, and improving advice to senior officials and ministers.

The fellowship will provide the successful candidate with:

- the opportunity to co-design, produce and where appropriate, publish original analysis and research;
- the opportunity to inform BIST, UKRI and wider government policy in a strategically important technology area;
- full integration within the host team with a dedicated line manager and access to relevant meetings and policy processes as appropriate;
- opportunities to work with BIST research security, policy, analytical, technical and international specialists, as well as UKRI’s funding policy and programme leads in this area, to inform upcoming strategic priorities and funding activities;
- access to relevant evidence, systems and networks, subject to appropriate requirements;

- opportunities to engage with government, universities, research organisations, businesses and funders;
- access to policy roundtables, cross-government workshops and wider research security networks;
- opportunities to collaborate with fellows working across other strategically important technology areas

Person specification

Applications will be assessed by UKRI panel assessment against the following essential opportunity-specific requirements in addition to the generic eligibility and call criteria.

Essential criteria:

- a proven academic track record in digital research infrastructure, HPC or supercomputing.
- subject matter expertise in specific topics related to national security and cyber security.
- the ability to synthesise a range of quantitative and qualitative data and act on incomplete or uncertain information.

Applicants shortlisted from the panel assessment will be invited to a host led interview. At this stage the host will also take into account the following desirable fellowship-specific requirements

Desirable criteria:

- An interest and understanding in policy making, for example through work with or within a Government department or public agency.
- proven ability to use and communicate evidence in a fast-paced and reactive context
- awareness of the UK's existing digital research infrastructure landscape

Processing personal data

If applicants are shortlisted by the UKRI assessment panel UKRI will need to share the application and any personal information that it contains with the host for the host led interview selection process.

Your personal data will be handled in line with UK data protection legislation and managed securely. If you would like to know more, including how to exercise your Rights, please see the UKRI privacy notice.

Please see the hosts' privacy notice (BIST privacy notice) and they will delete your data at the end of the selection process unless you are successful, in which case we will retain your data as an independent data controller.