

4. Scope

The Policy covers any activity impacting on the assets of the e-Science Programme: infrastructure, code-base, datasets, and its good name. Specifically it applies to all projects, personnel and facilities funded via an e-Science programme grant, and to all core facilities in the UK academic and research community recognised as contributing services to the programme. It also deals with their protection against external threats.

5. Responsibilities

Ultimate responsibility for this Policy rests with the Director General of the Research Councils, but effective management responsibility is exercised on the Director General's authority by the UK e-Science Core Programme Directorate.

The Directorate is supported by a Grid Operations Security Team who will review the security of the e-Science Programme, including this policy and its supporting documentation, and make recommendations to the Directorate on any policy actions or initiatives that are needed.

Although in a strict sense the grant holding institution carries the legal responsibility for a given project, for practical purposes a project's Principal Investigator (PI) will be held accountable for its security. The PI must identify through the project's organisational structure other persons with security-related roles, and should nominate a point of liaison for operational matters, ensuring that cover for this rôle is provided in case of holiday or sickness of the regular technical contact.

Security incidents should be reported to the Grid Security Operations Team. In most cases, contact will be through a host institution's local CERT.

6. Practices

Projects must adopt processes that lead to secure solutions commensurate with the risks they face. When a project is proposed, its case for support must explain how this will be achieved. The e-Science programme will provide suitable training in this area. Proposals should anticipate, where possible, the training and consultancy needs of the project.

Grant-awarding panels may call upon specialist referees to evaluate the security features of a project proposal. On the advice of those referees or otherwise, they may decide to attach security-related requirements to a grant offer. These may include

- Funding for relevant training for project staff, to enable secure processes to be adopted, and secure features designed from the outset of the project;
- A requirement to undertake a detailed threat and risk analysis in the early stages of the project;
- A requirement to produce a detailed draft project security policy in advance, perhaps with an external review of that policy;
- Specific points at which a project security audit will be required, and funding to facilitate that audit;
- Specific conditions relating to access to facilities, data sets, etc.;

- Requirements to keep up-to-date with ongoing developments in particular security technologies;
- Sanctions to be applied if these requirements are not followed.

All funded projects will require a security policy, informed by a risk analysis. A security policy for a project will usually describe how the following will be taken into account:

- Policies and guidance from the e-Science programme, including this policy;
- Legal obligations, such as health and safety, and data protection;
- Ethical frameworks that constrain the project or the use of any associated capability;
- Specific concerns or risks arising from the nature of the project, including those of industrial partners and international collaborators;
- Established and evolving security practice in Grid-based environments;
- Actions to be taken upon detection of a breach of policy, whether by project staff or administrators, or by external persons.

Project security policies should be appropriate to the academic/research community and the specifics of the research project.

Industrial partners and international collaborators are similarly encouraged to adopt best practice, and are obliged to follow this policy when accessing assets of the e-Science programme.

In due course projects may be audited. The project security policy and its associated risk analysis will be the basis of the audit. The audit will look for evidence that risks have been adequately addressed in the policy and that processes are in place to support the security policy.

7. Sanctions

Notwithstanding the intention to be supportive to projects where security is concerned, this policy provides for sanctions in the event that a project wilfully or through negligence puts its own and others' security at risk; e.g. in the event that a project fails to follow the security requirements set out in its offer letter, and/or to adopt appropriate security processes relative to the risks that it faces. The sanctions will generally match the nature of the failure, and may range from denial of access to shared e-Science facilities to withholding of grant resource.

The Directorate will recommend the appropriate sanction or sanctions, although sanctions if confirmed will be applied by the relevant authority (e.g. funding body or facility operator).

The addition of e-Science sanctions does not alter the existing right of the JANET-CERT or the local institution's IT Services to apply sanctions of their own, if the wider community is put at risk by the actions of an e-Science project.

8. Further Information

Further information and guidance will be developed to support this policy and assist projects and project staff in applying it. All such advice will be made available via the National e-Science Centre web site, <http://www.nesc.ac.uk/>.

Last updated 15 April 2004 by Alan Robiette, <a.robiette@jisc.ac.uk>