BBSRC, MRC and NERC Joint Security Policy

Contents

Policy statement

1. Principles
2. Perceived threats
3. Roles and responsibilities
4. Security planning
5. Local procedures
6. Risk assessments
7. Monitoring
8. Policy review
9. Amendment history
Policy Statement

The Research Council is committed to provide appropriate cost effective security measures for the protection of:

- Staff and others who may be affected by our activities, from security risks involving danger or threats
- Physical assets from theft, damage or other security risk
- Information from loss, corruption or compromise

To achieve this, the Research Council will set out clearly the security responsibilities of its employees and provide appropriate and sufficient information, training and support to enable them to discharge those responsibilities to the required standard.

This policy applies to all employees of BBSRC, MRC and NERC, including those employed on permanent or temporary contracts. The principles of the policy will also be applied, as far as reasonably practical to non-employees working at Council/establishment facilities (e.g. contractors)

The joint Security Policy has been agreed with the Trade Union Side and complies with statutory best practice.

The UK Shared Business Services (SBS) provides HR Services across the Research Councils. However some employees are deployed at establishments/facilities/ships that do not access services from the SBS. In these cases references to the SBS or system (Employee Self Service) will not apply and employees should refer to their Research Council HR team for assistance.
1. Principles

1.1 The Research Council recognises that as an employer it has a duty and right to both protect its workforce whilst engaged on Council/establishment business, and visitors on Council/establishment premises, and a need to strike a balance between the security of the individual and the requirement for research programmes to function efficiently.

1.2 To achieve this, establishments shall:

- Provide a cost and risk effective degree of security protection to staff whilst engaged on Council/establishment business
- Ensure that contractors and visitors will be afforded security protection appropriate to the stated purpose of their visit
- Ensure that the security measures applied take regard of Councils/establishments responsibilities under applicable health and safety legislation
- Conduct risk assessments to ensure that the appropriate level of security measures for the protection of staff and visitors is always in force
- Provide appropriate information, instruction and training to staff

1.3 The Government Security Secretariat (part of the Cabinet Office) has produced the Security Policy Framework (SPF) which is regularly updated and which underpins this policy.

2. Perceived threats

2.1 Perceived threats which could impact on the Research Council are considered to be:

- Terrorist Action
- Extremist Action
- Criminal Action
- Social Malcontent Action

2.2 This policy sets out the responsibilities and main factors involved in maintaining a level of security across the whole Research Council estate, which is commensurate with the current threat levels. It also includes those security measures which are considered relevant to the delivery and maintenance of practical, acceptable and effective security for the Research Council as a whole.
3. Roles and responsibilities

3.1 Security is the ultimate responsibility of Directors and Heads of establishments, (or equivalent). They should keep the level of security under regular review and revise arrangements in accordance with the perceived security risks.

3.2 Directors/Heads of establishments are required to ensure that:-

- Key personnel are appointed, (including Corporate and local Security Advisors)
- The roles and responsibilities of key personnel are clear
- There is a full exchange of relevant information between the parties
- Appropriate security measures are fully implemented (Appendix A9.5ii)

3.3 Everyone has a personal responsibility for the practical application of this policy in their day to day activities and must support the policy at all times. Any security incidents or concerns should be reported to local Management or a Security Advisor. Non-compliance will be treated as a serious issue and disciplinary action may result.

4. Security planning

4.1 The process of ensuring security at establishments can be supported through the application of the following basic principles:-

- Prevention of threat
- Detection of threat
- Response to threat

4.2 Prevention of threat

Prevention of threat can be aided by establishing a secure perimeter (with physical and procedural barriers to unauthorised entry), accompanied by a combination of access control, procedural control (for authorised entry), pre-employment screening and staff training.

4.3 Detection of threat

Through the use of surveillance systems, such as CCTV, communication channels with neighbouring security functions, search procedures, alarm systems and managing a culture of vigilance.

4.4 Response to threat

Response to threat should be managed through alert, escalation and lock-down principles, ensuring adequately resourced and trained emergency response functions, and robust communication with emergency services.
5. Local procedures

Appropriate training plans, recruitment and contracting procedures must be established locally and implemented. Establishments should carry out a local risk assessment to determine whether or not to conduct security screening for individuals who have access to sensitive material or sensitive areas. (Appendix A9.5iii)

All establishments should ensure that they have completed a security risk assessment for their premises, identifying and assessing the level of likely threat.

All establishments should ensure that they have identified the assets they need to protect (people, property, plant, data) and how these assets may be vulnerable to threat.

Preparedness is essential to mitigate incidents rapidly and effectively. All establishments should ensure that they have documented and tested a security plan detailing the hierarchy of control that has been implemented appropriate to the level of likely threat, including prevention, detection and response systems.

6. Risk assessments

6.1 Prevention must be the first priority. Threats analysis and risk assessments should be carried out on a regular basis. Risk assessments should be carried out against the following minimum criteria:-

- The experience of criminal acts on site, particularly vandalism, deliberate and opportunist theft
- The type of work being undertaken, e.g. work with animals, even the most benign, is a potential risk from animal rights groups
- Public concern about the nature of the scientific work being conducted
- The degree to which the establishment/site conducts high level 'commercial in confidence' work which may be open to commercial/ scientific/industrial espionage etc.
- The level of risk carried out by other establishments at the same site

Overseas operations should be risk assessed and a Security Policy for the overseas detachment produced at the time. Advice from the British Foreign and Commonwealth Office and other appropriate national bodies, for the country concerned will be sought and included as appropriate.

7. Monitoring of Security Arrangements

7.1 Directors should meet Security Advisors/Group regularly to discuss the implementation of this policy and to resolve any security issues. A formal annual report should be provided to be shared with the TUS.
8. Policy Review

This policy will be regularly reviewed to incorporate any legislation or regulatory changes. The TUS may request that a policy is reviewed.

9. Amendment history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments/Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>