MRC Security Policy
Policy

It is Medical Research Council (MRC) policy 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.

NB. Information Technology Security is covered in a separate policy document issued by Head Office, **MRC Information Security Policy**.

Personnel Security is covered in a separate policy document issued by Head Office, **MRC Baseline Security Policy**

The Cabinet Office has issued a Security Policy Framework (SPF) (latest revision May 2011) which sets out the mandatory minimum requirements against which all departments will be required to provide annual assurance. The SPF provides the standard to which this policy has been written.

The Medical Research Council recognises that as an employer it has a duty and right to protect its workforce whilst engaged on Council business, and visitors whilst on Council premises. Within this policy Council recognises a need to strike a balance between the security of the individual and the needs of research programmes to function efficiently.

To achieve this, establishments shall;

- Provide a cost and risk effective degree of security protection to staff whilst engaged on Council business;
- Ensure that contractors and visitors to Council premises will be afforded security protection appropriate to the stated purpose of their visit;
- Ensure that the security measures applied take regard of Council’s 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.

The application of this policy and guidance will aid the achievement of MRC standards and help to ensure that the MRC meets all related legal requirements.

**Roles and responsibilities**

The MRC is committed to set out clearly the security responsibilities of its employees and to provide appropriate and sufficient information, training and support to enable them to discharge those responsibilities to the required standard.

Directors are required to ensure that:

- Key personnel are appointed
- The roles and responsibilities of key personnel are clear
- There is a full exchange of relevant information between parties
- Appropriate security measures are fully implemented
Key Personnel

A suitable person should be identified to be responsible for Security, with appropriate experience and/or qualification, and provided adequate resource to ensure cost effective security measures can be implemented.

Guidance Note 1 – Security Planning
Guidance Note 2 – Access Control
Guidance Note 3 – Surveillance
Guidance Note 4 – Manned Guarding
Guidance Note 5 – Third-Party management
Guidance Note 6 – Emergency preparedness
Guidance Note 7 – Off-site and personal security

Corporate Safety Security and Resilience Section
Version 1.0 2011
Guidance Note 1 – Security Planning

Introduction

The process of ensuring security at establishments can be aided through the application of three basic principles, following “Defence in Depth”.

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

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.

Detection of threat

Detection of threat can be aided 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.

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.

Approach

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

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

All units should ensure that they have documented 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.

Responsibilities

Each Unit should appoint the following persons:

Security Co-ordinator, responsible for:
- Producing a risk assessment with appropriate control
- Producing and maintaining contingency plans
- Deciding appropriate action in the event of an incident
- Deciding on reoccupation of a building after an evacuation
- Liaising with police and emergency services
- Arranging training, communications and testing

Security Sponsor
- Senior management representative who will “champion” security
• Has overall responsibility for planning and the authority to authorise appropriate expenditure for protective measures
• Provide adequate resource to the security co-ordinator to ensure appropriate and cost effective security measures can be implemented
Guidance Note 2 – Access Control

In addition to physical barrier systems and perimeter fencing, maintaining a secure perimeter can be aided through restriction of access and procedural control.

Access restriction

Automated Access Control Systems (AACS) are readily available on the market. When installing and implementing an AACS system, the following principles should be followed:

Authorisation – access should only be granted/ altered once authorisation against defined criteria has been received (e.g. access is only authorised when security screening has been completed). Authorisation should come from one designated person or office, and the number of authorisers should be kept to a minimum.

Control – the means of access (access card, key fob, etc) should only be issued/ altered from one central point, once authorisation is received. Note, that the person/office issuing access should be different from the person/office issuing authorisation.

Process – all users should be aware of their responsibility to keep their access card, pass or fob safe and secure, to report any losses immediately, and to not lend their card, pass or fob to other people. There should be processes in place to monitor unusual access, for example to restricted areas, or during silent hours.

Procedural control

Units should have procedures in place for:
- Initiation of security screening
- Feeding the results of security screening to the person responsible for authorising access (Access controller)
- Authorising access (in conjunction with other stakeholders)
- Removing access (e.g. for leavers)
- Controlling the issue of new access devices
- Logging non-conformances (e.g. lost passes)

Responsible persons

Units should appoint the following:

Access controller, responsible for:
- Verifying access requests against relevant permits and clearances
- Developing procedural control
- Authorising access requests
- Monitoring access trends
- Implementing corrective action against non-conformances

Access control officers, responsible for:
- Operation of access control systems
- Issuing access control items (key fobs, cards etc)
- Maintaining inventory of access control items
- Logging non-conformances
Guidance Note 3 – Detection

Surveillance can assist with early detection of potential threat, and is important both within and without the perimeter. Surveillance can be undertaken manually, through the use of patrols (if manned guarding is in place), or electronically through the use of CCTV and PIDS.

PIDS (Perimeter Intrusion Detection Systems)

PIDS architectures may involve the following items:
- Sensors
- CCTV
- Alarm systems
- Data communication

The most widely used aspect of PIDS systems within MRC units is CCTV, but it is worth noting that data communication systems should comply with MRC Information Security policies and procedures.

Sensors

Units considering sensors as part of their security risk assessment and plan should consider the following types of sensors:
- Barrier sensors – dual purpose systems that provide a physical barrier to intrusion, and a sensor for detection
- Volumetric – a detection field that locates and tracks intruders within a secure zone
- Fence-mounted – detect vibration on an existing physical fence, triggering an alarm when activated

CCTV (Closed Circuit Television)

Managing data

Data should be recorded and viewed only on equipment that is secure and restricted from the view of those not involved in the management of the system. Data should be stored securely in a manner that preserves image integrity, and deleted/destroyed once there is no further use for images.

Disclosure of images should be procedurally restricted, and records kept of all disclosures, including the purpose. The method of disclosure should be secure. Units should have procedures in place for enforcement agency data requests (e.g. police) and subject access requests (people requesting images of themselves) Data management should be periodically audited to ensure compliance.

The appropriate standard for CCTV is BS 7958: 2005 *Code of Practice for the management and operation of closed-circuit television (CCTV)*, and all systems should be installed in compliance with the Data Protection Act 1998

Coverage and signage

The installation of CCTV should ensure adequate coverage of vulnerable areas. The areas for consideration should be defined through risk assessment. In a high-risk establishment, total coverage may be necessary.
The technical specification of cameras and their location should reflect the environment, the image quality (size, resolution and frame rate) that is required, and when installed, should be adequately protected from vandalism.

The purpose of the CCTV system (monitoring, detection, recognition or identification) should be documented in the Security plan.

Wherever CCTV is in use, signage should be in place to inform people that surveillance is in place.

**Training**

All staff who use CCTV should be trained in the following:
- MRC Policies and procedures for image recording retention
- How to recognise and handle requests for images
- How to handle and store images securely

**Responsibilities**

Units should appoint the following:

**CCTV Manager**
- A manager responsible for the whole CCTV system, including implementation of policies and procedures

**CCTV Operators**
- Persons responsible for day-to-day operation of the CCTV system
- These persons should ensure that logs of operation, responsibility, maintenance and repairs are maintained

**Alarm systems**

Alarm systems may be used for detection of intruders in an area, or to detect the breach of a physical barrier. With a secure zone equipped with a number of control measures as part of an overall system, an intrusion may result in several alarms being triggered, and it is important that response personnel are adequately trained to recognise when unauthorised changes in the system are made, and to understand the meaning of alarms within their jurisdiction.
Guidance Note 4 – Manned Guarding

Manned guarding is a complementary layer of security and should be considered in conjunction with automated and procedural control. It is important to note that a physical presence can act as a deterrent to threat.

Selection of staff

Staff selection should be completed before employment to ensure that security staff have been security screened. Screening should be compliant with BS 7858:2006 Code of Practice for security screening of personnel employed in a security environment. Staff should be selected for their abilities to be vigilant and observant, and to keep up with developments in the security industry.

Training and CPD

All security personnel at MRC Units should be trained to the same (or better) standard that the private sector equivalent standard (e.g. SIA, NVQ Level 2), and undertake continuing professional development as supervised by the Unit Security Co-ordinator.

Health and Safety Management for shift workers

All shift patterns must be fully compliant with HSG 256, Managing Shift Work, and working time legislation. The Unit Security Co-ordinator should ensure that risk assessments are carried out with respect to lone working and night working (if applicable), stress and violence, as well as routine operations, such as patrolling and search routines.

Randomised procedures

All routine operations that involve staff movement, such as patrols, should be randomised in terms of route taken, duration, and the time of day that they are undertaken to avoid observable gaps in security presence. However, the possible routes and durations should be considered as part of an overall risk assessment to ensure that at all times of day, weather conditions (if external patrols are required) and duration of search (lengthy searches may result in unmanned areas of vulnerability) staff safety can be maintained. Where applicable, BS 7499:2007 Code of Practice for static site guarding, mobile patrol services should be considered.
Guidance note 5 – Third Party Management

Contractors

Contractors working on premises may need to enter and exit secure doorways more often than regular staff, without necessarily having the training or commitment to the MRC to maintain the security of MRC premises. All regular contractors (i.e. not supervised by an MRC employee) should be security screened, undergo a health, safety and security induction, and be informed of local security rules that they must abide by during their time on the premises. Compliance should be monitored by the host, and non-compliances taken up with the contractor. When dealing with contractors who have need to have access to restricted information (for example, plans of buildings), commercial confidentiality and document security should be ensured through contract terms, not only for the contractor, but also for the terms of any subcontract that may be necessary for the dissemination of project information.

Visitors

All visitors to MRC establishments should be escorted by a host, not only for security reasons, but also for their health and safety. Depending on the nature of the facility, it may be necessary to search the bags or vehicles of visitors.

All visitors should be informed in advance of arriving that they are visiting a secure facility, and should only be allowed entry if they are expected by a named host. Candidates for interview should not be informed of the names of those that will form the interview panel, and only titles should be used on recruitment communication. Interview candidates should be supervised at all times, and staff who are taking copies of identification documents, or giving site tours should be vigilant to disclosure of information about physical security.

Neighbours

Communications about security risk and initiatives should be maintained with neighbours, and where necessary, reciprocal arrangements should be sought to ensure vigilance can be maintained.

Unwelcome visitors

Procedures should be in place for lockdown and escalation in case of intruders. Escalation should be to emergency services, and both an agreement and a familiarisation visit should be arranged with local emergency services to foster a good working relationship and facilitate response in the event of an incident.

Handling phone calls

All staff should be aware of the potential for receiving phone calls that may be fishing for personal data. Telephone calls may come in from a variety of sources, asking for a particular post title, or job title, with the caller having no knowledge of the person’s name, phone number or other details. In these cases, calls should be treated as suspicious, the caller’s details taken, and passed to the Unit Security Co-ordinator without giving the caller any of the details of any MRC employee.
Guidance note 6 – Emergency preparedness

Emergency plans should be developed in the following categories as appropriate to the unit:

- Adverse publicity
- Demonstrations
- Telephone threats
- Delivered items
- Bomb on the premises

Adverse publicity

Adverse publicity could occur against an individual or the company. All examples of media interest should be referred to the MRC Press Office.

Demonstrations

All units should assess the risk of pre-planned and spontaneous demonstration

Pre-planned demonstrations

Notice of pre-planned demonstrations may come from a variety of media and intelligence sources. When doing this risk assessment, units should also consider the remote or central location of site, ease of transport links, and the activities of neighbouring businesses. Units should consider likely locations for a demonstration, and develop procedures for all staff to follow in the event that a demonstration occurs. Typical procedures may involve dressing down or avoiding the unit and awaiting further instructions.

Spontaneous demonstrations

For spontaneous demonstrations, the procedures already in place for planned demonstrations and research continuity plans may assist in contacting all staff and confirming action.

Handling the media

All media enquiries should be forwarded to a member of the MRC Press Office.

Telephone threats

Nuisance, abusive or threatening calls

Any member of staff receiving a phone call that they consider threatening, abusive or a nuisance call should record the call details and report it to their line manager in the first instance.

The line manager should assess the threat from the call, and the need for further action.

The Unit Security Co-ordinator should ensure procedures are in place on a unit level to:

- Communicate with telephone service providers to trace phone calls if necessary,
- To report threatening phone calls received at the home/mobile telephone numbers of staff to the police.
Telephone bomb threats

Planning

Units should have a bomb threat pro-forma, which helps record available details about the threat call. Staff who are likely to be the recipients of incoming calls (receptionists, security guards, administrators) should be appropriately trained in their responsibilities, escalation procedures, call handling and using the pro-forma. Units should have an up-to-date inventory and location for all hazardous substances and/or agents that may pose additional danger if a threat was received to their locations.

Escalation

Units should collect the details of emergency services, corporate contacts, and other relevant stakeholders who may need to be notified in case a bomb threat is realised. Cascade lists and emergency contacts should be stored in an alternative location to ensure accessibility in the event of a threat being received.

Delivered items

Units should assess the risk from delivered items being/containing:
- Explosive
- Incendiary
- Physically dangerous (e.g. sharp)
- Chemical, radiological or biological agents

Any device that has already been through the potentially rough handling of the postal system (with the exception of those items that arrive via courier) are unlikely to contain timing devices, so are likely to contain trigger mechanisms.

All staff who receive post should be trained to recognise indicators or suspicious items. Indicators may include:
- Excessive sealing that encourages opening from a particular end
- Items addressed to a title rather than a person
- Items with unusual post marks
- Unusual smell/odour
- Greasy/oily stains
- Small holes in envelope/packaging
- Powders/liquids emanating from package

Bomb on the premises

In the event of an incident, an assessment should be made by a competent person as to whether the incident is a hoax or involves a real explosive device.

In the event that there is not a named competent person available at the unit, escalation procedures should be in place for:
- Notifying police
- Evacuation/invacuation, considering the use of alternative alarms and alternative assembly points
- Ensuring availability of witnesses (such as the recipient of the threat call, security staff, delivery staff, goods-in staff).
Guidance note 7 – Off site and personal security

Personal security when working away from MRC premises plays a key part in ensuring your health and safety.

Working in the community

When working in the community, staff should follow the MRC guidance note: A practical guide for research involving the public, 2004.

Your personal life

Social networks

Social networking privacy is an increasingly controversial subject, and there are simple steps you can take to ensure that you cannot be personally associated with your work. All staff should ensure that they do not reference their employer as the MRC on Facebook and other social networks, and avoid participating in discussions about animal research on networks like Twitter.

Socialising with friends

In public locations, it is not always possible to know who may be listening in to conversations. When in a public place, staff should avoid discussing the work of, and their affiliation with the Medical Research Council.

Precautionary measures

The measures above are to prevent activists from linking personal lives of staff to MRC operations. Staff may also wish to remove their details from www.192.com.