MRC Information Security Policy
(IT_pg_003)

Contents

MRC Information Security Policy

Version 4.0

Document Control Summary

Title	MRC Information Security Policy
Electronic file reference (network or intranet)	IT_pg_003
Status	Final
Version No.	4.0
Date of this document	18/12/2015
Policy author(s)	Gina Nason Head of IT
Approved by (Names, titles and date)	Operations Board, 8th December 2015
Next review date	December 2016
Equality Impact Assessment completed in	N/A

Policy statement

The confidentiality, security and accurate processing of data are matters of great importance to the Medical Research Council (MRC). Failure in any of these, or delays and disruption of computer processing, can result in disruption to the services the MRC provides, loss in public confidence, and financial or other material losses.

The objective of the Information Security Policy is to ensure business continuity and minimise business damage by preventing and minimising the impact of information security incidents.

The MRC is committed to good information security provision for its stakeholders and for its staff.

1. Key principles

1.1. Information security is an essential enabler. Security risks must be managed effectively, collectively and proportionately to achieve a secure and confident working environment.

1.2. Information and information systems are recognised as valuable assets that underpin the strategic goal of facilitating research, training and knowledge exchange.

1.3. The MRC must appropriately secure and protect its information assets against confidentiality breaches, loss of integrity and interruptions to availability.

1.4. Failure to protect information assets could lead to costly, time-consuming and damaging incidents which may harm the reputation of the MRC, its staff, third parties and the MRC's business.

1.5. This policy outlines the minimum information security principles that the MRC must comply with when using, storing, sharing or exchanging information.

1.6. The policy acts as a framework document and further detail about specific measures can be found in supplementary policies.

1.7. The MRC will comply with relevant legislation.

1.8. This policy complies with the UK Government Security Framework Policy (SFP) (see 16.1) which sets out the requirements placed on all Non-Departmental Public Bodies (NDPBs).

1.9. This policy aligns with the Research Council Information Security Policy.

1.10. This policy aligns with the International Standard on Information Security ISO27001: 2013 (see 16.2).

1.11. This policy applies to MRC Head Office and MRC Intramural Units (Establishments).

1.12. This policy relates to information security only. Physical and personnel security is dealt with by the MRC Security Policy (see 16.3) and MRC Baseline Security Policy (see 16.4).

1.13. The MRC is committed to implementing best practice for the management of information security.

1.14. MRC Establishments are expected to develop further controls to support the implementation of this policy.

1.15. For the purposes of this policy, the use of the word "staff" covers MRC employees on permanent or fixed term contracts as well as persons who are on secondment to the MRC and non-employees such as students, contractors and other persons carrying out work on MRC premises and/or on behalf of the MRC.

2. Scope

This policy applies to the following areas listed below.

2.1. All information owned by the MRC, independent of who processes the information.

2.2. Information and information systems in all forms, independent of the medium on which they are held (physical, electronic) or the form which they take (text, graphics, software, databases, multi-media).

2.3. All stages of the information lifecycle: creation, use, storage, disposal.

2.4. The transmission of information independent of means (post, electronic, oral).

2.5. All authorised users of MRC information and information systems, whether or not they are members of MRC staff.

2.6. With regards to electronic systems, this Policy applies to the use of MRC owned facilities and privately/externally owned systems when connected to any MRC network directly or indirectly. Owned is deemed to include leased, rented or loaned.

2.7. All MRC owned/licensed data and software, whether they are loaned or privately/externally owned systems, and to all data and software provided to the MRC by sponsors or external collaborators.

2.8. Equipment: computer processors of any size or used for any purpose; peripherals, workstation and terminal equipment; telecommunications and data communication cabling and equipment; LAN and WAN equipment.

2.9. Data: regardless of storage media (electronic or hard copy) and data in transit; information derived from any of the MRC's business processes

2.10. Software: operating system software and support programs, application software, application enabling software

2.11. Location: permanent or temporary offices, home/mobile working locations, institutes, establishments and laboratories operated by the MRC or wherever information associated with the MRC is located.

2.12. All MRC activities, worldwide.

2.13. This policy and associated policies, standards, guidelines and procedures are the minimum standard to be achieved by all establishments connected to shared systems and facilities. This minimum standard confers a level of "trust" to establishments to protect the assets of all participants. Any establishment not achieving this standard shall be regarded as "untrusted".

3. Purpose

3.1. The purpose of the information security policy is to protect the MRC, its stakeholders and staff from all information security threats, whether internal or external, deliberate or accidental. Information security is characterised as the preservation of:

3.1.1. Confidentiality: ensuring that information is accessible only to those authorised to have access

3.1.2. Integrity: safeguarding the accuracy and completeness of information and processing methods

3.1.3. Availability: ensuring that authorised users have access to information and associated assets when required

3.1.4. Regulatory compliance: ensuring that the MRC meets its regulatory and legislative requirements.

3.2. These preservation measures relate to both single records and aggregated records.

4. General considerations

4.1. MRC staff, contractors and third party users should be aware of information security threats, concerns and their responsibilities and liabilities. They should support the MRC's security policy and apply security measures in their day to day work to reduce the risk of human error.

4.2. Duties and responsibilities covering management and usage shall be segregated.

4.3. Ownership of information assets should be clearly defined and respected.

4.4. Information and information assets must not be used for inappropriate or illegal purposes.

4.5. Only appropriately licensed information assets will be used and usage must conform to the licence agreement.

4.6. MRC will classify information in accordance with the Government Classification Scheme (GCS). Sensitive information will be identified, marked and special arrangements made to ensure its confidentiality, integrity and availability (see 16.5). Information will be handling in line with legal requirements under Freedom of Information (FoI) and Data Protection Acts (DPA) (see 16.6 and 16.7 respectively).

4.7. Information and information assets will be disposed of according to the Records Management policy (see 16.8) and Government approved asset disposal mechanisms. Certificates of destruction must be obtained for hardware assets, certifying that the assets have been wiped, and the certificates kept on record.

5. Accessing information and information assets

5.1. Access to MRC information systems and assets will be appropriately controlled through a defined access control policy, covering user identification and authentication. This applies to users, networks, operating systems and applications.

5.2. Access is granted on a genuine "need to know" basis.

5.3. Where MRC contracts with, or grants access to, third parties, clear and contractually binding requirements will be agreed to ensure appropriate use and protection of information assets. Where this is not possible, the MRC may deny access to some or all of the shared information or information systems by informing the Security and Information Risk Owner (SIRO) (see 16.14). Formal exchange policies, procedures

and controls will be put in place to protect the exchange of information and/or software.

6. Technical aspects

6.1. All networks, systems (including storage) and infrastructure will be protected, managed and controlled in order to protect the systems from threats, interception, disruption and damage to maintain security for systems and applications. Example protection and control measures include:

6.1.1. Appropriate security, such as anti-virus, firewalls etc will be implemented to protect against malicious code.

6.1.2. To protect the MRC from virus infection, incident plans shall be developed for dealing with and recovering from virus attacks. Staff must be made aware of the standards, guidelines and procedures they must adhere to (see 16.9).

6.1.3. To protect against physical harm or direct access, security perimeters (eg card controlled entry points) shall be used to protect areas that contain information and information processing facilities.

6.1.4. Development, test and production applications shall be separated.

6.1.5. Security measures will be put in place to control the installation of software on operational systems.

6.1.6. Security must be considered at all stages of systems design, development and integration. Specific guidance on software development is available. Where mobile code is authorised, this must operate to a clearly defined security policy (see 16.11). Mobile code is defined as software that is transferred between systems. Examples include Javascript, Java applets, ActiveX controls, and macros embedded in Microsoft Office documents.

6.1.7. Changes to processing facilities and systems shall be controlled through the implementation of a change and configuration management process.

6.1.8. Specific control measures need to be applied to moveable media, eg laptops, mobile phones, memory sticks and external hard drives (see 16.11).

6.1.8.1. MRC data should only be stored on encrypted devices.

6.1.8.2. These encrypted devices must be provided by MRC.

6.1.8.3. A degree of pragmatism should be demonstrated when transferring data between devices in the same location. In these situations, the mobile device must not be removed from the Establishment building.

6.1.8.4. A sense check for all users is to ask whether they would be happy for that data to be published in the media. If they are not happy, then the data/device should be encrypted.

6.1.9. Only those devices that are supplied by MRC and are encrypted can be used for storing MRC data. See IT_pg_006 paragraph 7.6 for an exception to this (see 16.9).

6.1.10. Where IT services are provided by third party suppliers, security controls and resilience must be defined, implemented, operated and maintained by the third party. Reports and records shall be regularly reviewed and audits carried out. A basic/minimum question set has been developed regarding the use of external resources hosting MRC data/information (see 16.12).

6.1.11. Security implications in any service transition should be considered as a priority and a risk assessment carried out.

6.1.12. Where appropriate, multiple copies of data/information/software will be kept to protect against loss. These backups will be tested regularly.

6.1.13. Data and information must be stored on servers, where they will be backed up. No backups will be taken of workstation hard drives (C: or desktops).

6.1.14. Information assets will be protected by appropriate business continuity mechanisms, covering incident management and resilience configuration. Cause and impact assessment and restore plans (with timescales) will be developed, tested and maintained.

7. Use of personal devices

7.1. MRC does not advocate the use of personal devices to access MRC data, however we recognise that a flexible working environment means that personal devices will be used.

7.2. To facilitate this, staff must:

7.2.1. Ensure that their devices are password protected.

7.2.2. Ensure that their devices have the most up to date anti-virus software.

7.2.3. Passwords should not be saved and any auto-complete functionality must not be used.

7.2.4. MRC data on these devices is encrypted.

7.2.5. Accept that their devices should be wiped remotely if there is a potential security breach (ie if they lose the device). This means that appropriate remote wiping software must be downloaded.

7.3. When using webmail, users must not download attachments onto their personal devices.

8. Starting and ending work

8.1. All persons working with animals at/or for the MRC or who work in HR, IT, corporate and Head Office functions dealing with sensitive data will need to be checked for connection/affiliations to animal rights groups (see 16.4).

8.2. Animal Rights security checks also apply to suppliers and contractors who have access to MRC data.

8.3. The User Provisioning Leaver's process should ensure that all access rights are revoked and all assets returned on the termination of employment, contract or agreement.

9. Monitoring, recording and auditing

9.1. Compliance with this policy and its effectiveness will be reviewed and tested independently of those charged with its implementation, as part of the MRC's annual audit process.

9.2. An information asset register will be set up to identify all important assets, and assets containing personally identifiable data. Information asset owners will be identified and rules for acceptable use of such assets will be documented and developed. A "risk appetite" for these assets will also be identified and documented (see 16.13).

9.3. Appropriate, auditable records of access and use are to be maintained.

9.4. Monitoring will take place in order to:

9.4.1. ensure that only authorised individuals have access

9.4.2. ensure that MRC's IT systems are not used for inappropriate or illegal actively. This includes knowingly viewing, accessing, producing, storing, processing and/or distributing illegal/offensive materials (see 16.9).

9.5. It is required to identify and keep a record of all individuals who have access to, or are involved in handling and processing, MRC information. Responsibility will be clearly defined and where appropriate formally laid out in letters of appointment.

9.6. Audits will be carried out to determine compliance with the framework and associated policies. Additional audits on any IT-related matter can be commissioned and carried out by the RCUK internal audit department, the Audit and Assurance Services Group (AASG) and by suppliers (such as for compliance with software licences). Audits will be co-ordinated and communicated by the MRC's Head Office IT Service Delivery Team.

10. Roles and responsibilities

10.1. All individuals who use MRC information or information systems have a duty of care to protect the confidentially of information that is entrusted to them. The principal information security responsibilities for all are to:

10.1.1. Only use information and information systems that you have authorisation to use.

10.1.2. Follow all relevant instruction, procedures, guideline and codes of practice.

10.1.3. Report any real or suspect breaches of information security to your local Information Security Manager (ISM).

10.1.4. Not use, or attempt to use, any information or information system for illegal of inappropriate purposes (see 16.9).

10.2. Only one individual is required for each corporate security role. Numerous individuals may be required to fulfil the security roles at local level.

10.3. MRC Chief Executive

10.3.1. The MRC's Chief Executive is the Accountable Officer and has overall accountability and responsibility for ensuring that information risks are assessed and mitigated to an acceptable level within MRC.

10.3.2. The Chief Executive will ensure that arrangements to fulfil this responsibility are established, operated effectively, monitored and reviewed, and continually improved in light of internal and external best practice. The Chief Executive is also responsible for ensuring the provision of adequate resources to implement this Information Security Policy.

10.3.3. The Chief Executive shall appoint an MRC Director as Senior Information Risk Owner (SIRO).

10.3.4. As the Accounting Officer the Chief Executive will provide BIS with an annual statement on the Security Framework Policy (SFP) compliance (see 16.1).

10.4. Senior Information Risk Owner (SIRO)

10.4.1. The Senior Information Risk Owner is a Director familiar with general protective security and information risks. The SIRO acts as the champion for all security issues and factors information security into the MRC's business planning. The SIRO leads the MRC response to the SPF.

10.4.2. This is a mandatory role under SFP.

10.4.3. The SIRO has ultimate responsibility for security.

10.4.4. The SIRO owns the MRC's Information Risk Policy and Information Risk Assessment.

10.4.5. The SIRO will assure the Chief Executive that the MRC has the appropriate information security measures in place by:

10.4.5.1. Leading and fostering a culture that values, protects and uses information for the public good.

10.4.5.2. Ensuring the MRC's approach to information risk is effective in terms of resource, commitment, execution and is communicated to all staff.

10.4.5.3. Establishing appropriate responsibilities, boundaries and structures, including adequate resourcing for information security.

10.4.5.4. Taking responsibility for the overall information risk policy and risk assessment process, including policy development, action plans and annual risk reviews.

10.4.5.5. Presenting and promoting security policy and information risk management strategies to the CEO and Management Board.

10.4.5.6. Bringing to the CEO's attention the need for any action to improve information security, any security risks the MRC is facing and any incidents that have occurred.

10.4.5.7. Confirming that any significant security control weaknesses have been reflected in the Director's Annual Statement of Internal Control (DASIC).

10.4.5.8. Monitoring the implementation of this policy including the effectiveness of local procedures.

10.4.5.9. Providing a focal point for the resolution and/or discussion of information risk issues.

10.4.6. In relation to the Departmental Security Officer (DSO – see 9.6 below), the SIRO is expected to:

10.4.6.1. Act as a critical friend and carry out a challenge function.

10.4.6.2. Lend authority to security initiatives.

10.4.6.3. Provide support through appropriate resourcing.

10.4.6.4. Offer a strategic perspective and highlight issues and decisions that will impact on the DOS and protective security in general.

10.4.6.5. Initiate internal investigations.

10.4.7. Further information about the role of the SIRO is available in the guidance document (see 16.14)

10.5. Information Technology Security Officer (ITSO)

10.5.1. The ITSO is responsible for developing and implementing the Information Security Policy, IT standards and guidance and proceedings in accordance with the SFP. This must be undertaken in conjunction with the DSO, SIRO and those responsible for IT Service Delivery (including any outsourced service providers).

10.5.2. Only one member of MRC staff can be registered as the MRC ITSO at any point in time with the government security agencies.

10.6. Departmental Security Officer (DSO)

10.6.1. The DSO is the formal contact between MRC and the government security infrastructure and is the normal conduit for communication about threat levels, cross government responses, best practice advice and access to resources.

10.6.2. The DSO has no specific additional responsibilities in relation to information security.

10.6.3. Only one member of MRC staff can be registered as the DSO at any point in time with the government security agencies.

10.6.4. DSO is a mandatory role under SPF.

10.7. Information Asset Owners (IAO)

10.7.1. Information Asset Owners are senior individuals involved in running the MRC's business.

10.7.2. They are responsible and accountable for MRC owned information and specifically for protected personal data.

10.7.3. IAO is a mandatory role under SPF and is responsible to the SIRO for managing risks to the corporate information assets.

10.7.4. IAOs are named on the Information Asset Register.

10.7.5. To understand and address risk to the information assets they own and provide assurance to the SIRO and the security and use of these assets, the IAO must:

10.7.5.1. Know what information the asset holds and understand the nature and justification of information flows to and from the assets and minimise information transfers whilst achieving business purposes.

10.7.5.2. Know who has access and why and ensure their use is monitored and complies with this policy.

10.7.5.3. Ensure the confidentiality, integrity and availability of all information that their system creates, receives, maintains or transmits and protect against any reasonable anticipated threats or hazard to the security or integrity of such information, working with others where necessary.

10.7.5.4. Ensure impact assessments are carried out.

10.7.5.5. Understand and address risks to the asset and provide assurance to the SIRO.

10.7.5.6. Collate and manage their information asset register.

10.7.5.7. Ensure the asset is fully used to the benefit of the MRC.

10.7.5.8. Approve and oversee the disposal mechanisms when the information and/or asset is no longer needed.

10.8. MRC Unit Directors

10.8.1. MRC Unit Directors shall ensure that information security management is appropriately co-ordinated within their Unit in the context of this policy.

10.8.2. Directors will ensure that the confidentiality, integrity, availability and regulatory requirements for all their business systems are met.

10.8.3. Processes need to be in place for ensuring that:

10.8.3.1. Staff are fully informed of their obligations and responsibilities with regards to information security.

10.8.3.2. Policies are implemented through appropriate local guidelines and procedures.

10.8.3.3. Major threats to information assets are monitored.

10.8.3.4. Information security is enhanced and improved.

10.8.3.5. All breaches of information security, actual or intended, are reported, reviewed and monitored.

10.8.3.6. Complete the annual statement of internal control (DASIC).

10.9. Corporate Information Security Team

The responsibilities of the Corporate Information Security Team encompass:

10.9.1. Developing and maintaining the information security framework and associated policies.

10.9.2. Provide advice and guidance policy implementation.

10.9.3. Gain and maintain awareness of security threats being faced by the MRC.

10.9.4. Prepare a statement of applicability.

10.9.5. Monitor incidents, security status, and current threats, recommending safeguards.

10.10. Information Security Manager (ISM)

10.10.1. Each establishment shall appoint an information security manager responsible for the local management of information security, including policies and procedures.

10.10.2. Responsibilities include:

10.10.2.1. Establish and implement appropriate policies, standards, guidelines and procedures

10.10.2.2. Select the controls to be implemented

10.10.2.3. Define responsibilities for information security

10.10.2.4. Promote security awareness

10.10.2.5. Undertake risk assessments and manage risks

10.10.2.6. Carry out security reviews

10.10.2.7. Record security incidents

10.11. MRC Operations Board

10.11.1. Operations Board (Ops Board) is made up of representatives from Head Office and Unit Managers. Key responsibilities include:

10.11.1.1. Endorsing the information security policy.

10.11.1.2. Agreeing levels of risk and approving residual risk.

10.11.1.3. Receiving security reports at regular intervals covering the status of security implementation, update on threats, and the results of security reviews such as the Information Security Management System (ISMS) audit report.

11. Risk management

11.1. MRC will utilise its corporate risk systems, eg Easyrisk, to manage, monitor and report on its information risks.

11.2. Information risks will be handled in a similar manner to other major risks such as financial, legal and reputational risks.

11.3. Information assets will be risk-assessed to determine the degree of protection required.

11.4. MRC will assess it information risk annually, with internal reviews that assess the level of protection afforded to its information.

11.5. On the commencement of an IT project or programme, a risk assessment must be carried out if there is a significant change to existing IT systems.

11.6. A threat and impact assessment must be carried out to identify the impacts to the business if information risks are realised.

12. Training, education and awareness

12.1. Guidance is given to every individual that has access to MRC owned information.

12.2. Information risk awareness training is available for its Accounting Officer, SIRO and Information Asset Owners and members of the Audit Committee. Training must be conducted on appointment and individuals must demonstrate current awareness of potential threats.

12.3. Appropriate training will be provided to all individuals with specific information security responsibility.

12.4. Staff are required to receive information security awareness training and should be aware of the incident reporting procedures. If staff fail to successfully complete the training, then access to MRC systems and data must be withheld.

12.5. MRC will establish and maintain appropriate contact with other organisations, law enforcement authorities, regulatory bodies (including BIS) network and telecommunications operators in respect of this policy. This is not an exhaustive list of bodies.

12.6. MRC will actively review and monitor changes in government strategy and policy regarding information security and will disseminate any information to Unit IT Managers if relevant.

12. Breaches

12.1. Real or suspected breaches of this policy will be reported to the MRC's ITSO via your local ISM (see ref 16.15).

12.2. Breaches of this policy will be dealt with under MRC's disciplinary and/or criminal proceedings, as appropriate, or by equivalent sanction in the case of third parties.

12.3. All security breaches or suspected security incidents will be reported to the Corporate Information Security Team. The Corporate Information Security Team will determine whether the incident will be investigated locally or corporately. A separate process will then be followed (see 16.15). All reported incidents will be recorded.

13. Exceptions

13.1. Exceptions to this policy require approval by the SIRO. See separate Guidance note (see 16.16) regarding the process.

14. Effective date

14.1. This policy is effective from December 2015.

15. Review date

15.1. This policy will be formally reviewed in December 2016.

16. Related documents

16.1. Cabinet Office, (2014). HMG Security Framework Policy.
16.2. International Standards Organization, (2013). Information Security.
16.3. MRC Security Policy
16.4. MRC Baseline Security Policy
16.5. MRC Information Marking Guidance (IT_pg_012)
16.6. MRC Freedom of Information Handbook
16.7. MRC Data Protection Policy
16.8. MRC Records management policy
16.9. MRC Computer usage, email and internet monitoring policy (IT_pg_006)
16.10. MRC Software development controls guidance note (IT_pg_008)
16.11. MRC Mobile Device Security Policy (IT_pg_001)
16.12. MRC data hosting and security questionnaire (IT_pg_17)
16.13. Cabinet Office. *Information Risk Directive.* London: HMG, 2012
16.14. MRC SIRO role guidance (IT_pg_015)
16.15. MRC Security incident handling guidance note and associated COPs (IT_pg_002 and IT_COP_001-006).
16.16. MRC Exceptions to IT Policies guidance note IT_pg_016.

17. Amendment history

Version	Date	Comments/Changes
0.1	23.06.2011	Last updated 18.04.2008. Full review.
0.2	4.8.2011	Updated in response to comments from HR community and OB.
0.3	15.9.2011	Updated with further comments from OB.
2.0	Dec 2011	Updated with comments from TU side.
3.0	Dec 2014	Updated after full review from HO and OB
4.0	December 2015	Final version post scheduled review