



Information Security Policies

Version 6.1

Information Security Policies

Contents:

1. Information Security	page 3
2. Business Continuity	page 5
3. Compliance	page 6
4. Outsourcing and Third Party Access	page 7
5. Operations	page 8
6. Cryptography	page 11
7. Information Handling	page 12
8. User Management	page 14
9. Network, System and Software Management	page 15
10. Standard Operating Procedures (SOPs)	page 16

1. Information Security

- 1.1 It is Queen Mary's policy that the information it manages, in both electronic and hard copy, is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.
- 1.2 This information security policy provides management direction and support for information security across the organisation, in both electronic and hard copy. Specific, subsidiary information security policies are considered part of this information security policy and have equal standing.
- 1.3 This policy has been ratified by the organisation and forms part of its policies and procedures, including its Regulations for Conduct. It is applicable to and is communicated to staff, students and other relevant parties.
- 1.4 This policy will be reviewed every five years and updated, as applicable, to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.
- 1.5 To determine the appropriate levels of security measures applied to information systems, a process of risk assessment is carried out for each system to identify the probability and impact of security failures. (SOP DG01 – Information Risk Assessments).

The Information Services Board (ISB)

- 1.6 Queen Mary's Information Services Board (ISB) has been established to manage information services within the organisation, chaired by a senior College officer or an appointee of Council. The ISB is made up of appropriate senior organisational managers. It exists, in part, to:
 - Ensure that Queen Mary and its staff and students meet the requirements of extant UK legislation and regulations in relation to Information Security;
 - Ensure that there is clear direction and visible management support for security initiatives within the organisation;
 - Ensure that appropriate risk management assessments are resourced and undertaken; and
 - Promote security through appropriate commitment and adequate resourcing.

The Information Security Compliance Group

- 1.7 The Information Security Compliance Group, comprising management representatives from all relevant parts of the organisation, has also been created to devise and coordinate the implementation of information security controls.
- 1.8 Responsibility for ensuring the protection of information systems and ensuring that specific security processes are carried out lies with the Director of IT in collaboration with the heads of departments within Queen Mary who manage information systems.

- 1.9 Specialist advice on information security shall be made available throughout the organisation by the Director of IT.
- 1.10 The organisation will, under the direction of the Director of IT, establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.
- 1.11 The implementation of this Information Security Policy and its continued fitness for purpose will be reviewed and audited independently of those charged with its implementation, by the Queen Mary's internal auditors.

2. Business Continuity

- 2.1 Queen Mary's management team has in place processes to assess business continuity requirements and to identify appropriate areas for further action. This includes reliance on information resources, no matter whether they are electronic or hard copy, and whether those resources are provided within departments, by central Queen Mary services or services provided from outside Queen Mary. This accords with the Business Continuity Plan (SOP DG02 – Business Continuity).
- 2.2 A formal risk assessment exercise is conducted to classify all systems according to their level of criticality to Queen Mary and to determine where business continuity planning is needed (SOP DG01 – Information Risk Assessments – see para 1.5).
- 2.3 A business continuity plan will be developed for each system or activity. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates.
- 2.3 All business continuity plans will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether management and staff are able to put the plan into operation.
- 2.4 All staff will receive appropriate training to be able to carry out their roles with respect to business continuity plans. During an incident, staff may be required to carry out duties which are not part of their normal routine.
- 2.5 Each business continuity plan will be reviewed, and if necessary updated. The frequency of reviews will be as defined for the appropriate criticality level.

Backup and system

- 2.6 Information owners must ensure that appropriate backup and system recovery procedures are in place. Backup of the organisation's information assets and the ability to recover them is an important priority. Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business. (SOP DG27 – IT Security Incident Management and SOP DG02 – Business Continuity).

3. Compliance

- 3.1 The Terms and Conditions of Employment and the organisation's Code of Conduct set out all employees' responsibilities with respect to their use of computer systems and all sets of data, computer-based or otherwise. Line managers must provide specific guidance on legal compliance to any member of staff whose duties require it.
- 3.2 The student regulations incorporate the organisation's Code of Conduct which sets out all students' responsibilities with respect to their use of computer-based information systems and data.
- 3.3 All members of the organisation will comply with the Information Security Policy and any applicable laws. Where appropriate their compliance will be monitored. Failure to comply will be dealt with under the appropriate disciplinary procedure.
- 3.4 Before any new systems are introduced, a risk assessment process will be carried out which will include an assessment of the legal obligations that may arise from the use of the system. These legal obligations will be documented and a named system controller, with responsibility for updating that information, will be identified.
- 3.5 Queen Mary will ensure that documentation will be available to all members of Queen Mary on commonly encountered issues, including, but not restricted to:
- (i) The key aspects of the law of copyright, in so far as they relate to the use of information systems.
 - (ii) The key aspects of computer misuse and data protection legislation.
 - (iii) The organisation's Code of Conduct forbids the use of information systems to send or publish derogatory remarks about people or organisations.
 - (iv) The organisation's Records Retention Policy defines the appropriate length of time for different types of information to be held. Information will not be destroyed prior to the expiry of the relevant retention period and will not usually be retained beyond that period. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed.
 - (v) The organisation will only process personal data in accordance with the requirements of the data protection legislation. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so.
 - (vi) Where it is necessary to collect evidence from the information systems, it shall be collected and presented to conform to the relevant rules of evidence. Expert guidance will normally be sought.
 - (vii) All of the organisation's systems will be operated and administered in accordance with the documented procedures. Regular compliance checks will be carried out to verify this compliance.

4. Outsourcing and Third Party Access

- 4.1 All third parties who are given access to the organisation's information systems, whether suppliers, customers or otherwise, must agree to follow the organisation's information handling, retention and security policies. A copy of the information security policies and the third party's role in ensuring compliance will be provided to any such third party, prior to their being granted access.
- 4.2 The organisation will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the organisation will require external suppliers of services to sign a confidentiality agreement to protect its information assets. (SOP DG03 – Confidentiality Agreements).
- 4.3 Persons responsible for agreeing maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of the organisation's information security policies. (SOP DG04 – Contracting for IT Services).
- 4.4 All contracts with external suppliers for the supply of services to the organisation must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier. These must also state that information will be retained in line with Queen Mary's Records Retention Policy.
- 4.5 Any facilities management, outsourcing or similar company with which this organisation may do business must be able to demonstrate compliance with the organisation's information security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

5. Operations

- 5.1 This policy reflects the need to consider information security as a major component of staff duties and responsibilities. Managers within the organisation are charged with a duty to ensure, at local level, that adequate procedures are in place to protect the organisation's information assets and the information we receive for which we have a duty of care to protect. These policies apply to all information regardless of format.

Physical Access to information

- 5.2 Areas and offices where Confidential or Restricted information is processed shall be given an appropriate level of physical security and access control. Staff with authorisation to enter such areas are to be provided with information on the potential security risks in the area and the measures used to control them. (SOP DG24 – Working in Secure Areas).
- 5.3 Duties and areas of responsibility shall be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the organisation.

IT Operations

- 5.4 The procedures for the operation and administration of the organisation's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.
- 5.5 The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the Information Handling Policy, and a risk assessment undertaken to identify the probability and impact of security failure.
- 5.6 Procedures are in place to report security incidents and suspected security weaknesses in the organisation's business operations and information processing systems. The Director of IT is responsible for ensuring that an effective reporting system is maintained, together with detailed guidance on how to address identified weaknesses. (SOP DG05 – Information Security Incident Reporting and SOP DG27 – IT Security Incident Management).
- 5.7 Procedures will be established for the reporting of software malfunctions and faults in the organisation's information processing systems. Faults and malfunctions shall be logged by IT staff and monitored so that timely corrective action can be taken. (SOP DG06 – IT Malfunction Reporting).
- 5.8 Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have IT management approval. (SOP DG25 – Configuration Management and Change Control).

- 5.9 The implementation of new or upgraded software must be carefully planned and managed to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls. (SOP DG25 – Configuration Management and Change Control).
- 5.10 Development and testing facilities for business critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal change control procedures. (SOP DG25 – Configuration Management and Change Control).

Procurement

- 5.11 All computerised information technology systems must be purchased through Queen Mary's IT purchasing office. Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status in accordance with established change control processes. (SOP DG07 – Purchasing IT Hardware and Software)
- 5.12 Requests for new information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information and the Information Services Board. The business requirements of all authorised information systems must specify requirements for security controls.
- 5.13 Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the organisation must follow a formalised development process. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place and that systems are validated to ensure that they are fit for purpose. (SOP DG08 – Implementing IT Systems).
- 5.14 The security risks to the information assets of all system development projects shall be assessed and access to those assets shall be controlled by a centralised asset register, managed by the Director of IT. (SOP DG01 – Information Risk Assessments).

Disposal of Equipment and De-Commissioning Software

- 5.15 Obsolete equipment and software must be disposed of under the direction of the IT department. Devices containing Confidential or Restricted data will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the organisation and only be removed from site with the permission of the information asset owner. (SOP DG10 – IT Equipment Disposal).

System Control

- 5.16 Equipment supporting systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

- 5.17 Equipment supporting systems shall be given adequate protection from unauthorised access, environmental hazards and failures of electrical power or other utilities. (SOP DG23 – Computer Room Operation).
- 5.18 Access controls for all information and information systems are to be set at appropriate levels in accordance with the value and classification of the information assets being protected.
- 5.19 Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored. (SOP DG11 – System Access Controls).

6. Cryptography

- 6.1 The policy on cryptographic controls includes procedures to provide appropriate levels of protection to Confidential or Restricted information whilst ensuring compliance with statutory, regulatory and contractual requirements. (SOP DG12 – Cryptographic Controls).
- 6.2 Confidential or Restricted information shall only be imported to or taken for use away from the organisation in an encrypted form.
- 6.3 Authorised staff shall be able to gain access, when needed, to any relevant information held in encrypted form.
- 6.4 The confidentiality of information being imported or transferred on portable media or across networks must be protected by use of appropriate encryption techniques. Encryption shall be used whenever appropriate on all remote access connections to the organisation's network and resources.
- 6.5 A procedure for the management of electronic keys, to control both the encryption and decryption of Confidential or Restricted information is established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.

7. Information Handling

Information Inventory

- 7.1 An Information Inventory is maintained of all the organisation's major information assets and the ownership of each asset will be clearly stated.
- 7.2 Within the Information Inventory, each information asset is classified according to sensitivity using the organisation's agreed information classification scheme. Classified information and outputs from systems handling classified data must be appropriately labelled according to the output medium. (SOP DG09 – Information Classification).

Archiving

- 7.3 The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with the organisation's Retention Policy. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved or long-term access may be required. (SOP DG13 – Records Management)

Storage and deletion or destruction of information

- 7.4 All users of Queen Mary's information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files, records and information in a manner which safeguards and protects the confidentiality, integrity and availability of such files and with due regard to the defined procedures. (SOP DG14 – Storage of Information and SOP DG16 – Disposal of Information).

Off-site storage/removal

- 7.5 Removal off site of the organisation's Confidential or Restricted information assets, either printed or held on computer storage media, should be properly authorised by management. Prior to authorisation, a risk assessment based on the criticality of the information asset shall be carried out.

Confidential or Restricted material, handling

- 7.6 Confidential or Restricted information must be stored in a central storage file and not on portable media unless encrypted. Copies of such material must be protected and handled according to the distribution and authorisation levels specified for that information. All employees must be made aware of the risk of breaching confidentiality associated with the transfer, storage, and copying of information. (SOP DG15 – Handling Information).

Confidential or Restricted material, disposal

- 7.7 All information of a Confidential or Restricted nature is to be shredded or similarly destroyed when no longer required. The relevant information owner must authorise or initiate this destruction. Records must be disposed of in accordance with SOP DG16 – Disposal of Information.

System recovery

- 7.8 The Director of IT will ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files.

8. User Management

- 8.1 All users must be registered on a central database managed by the Director of IT. All users have one or more unique identifier(s) (user ID) for their personal and sole use for access to all the organisation's information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason whatsoever. (SOP DG17 – User Registration).
- 8.2 The Director of IT will ensure that a system for password management is maintained, to ensure the implementation of the requirements of the information security policies. (SOP DG18 – Password Management).
- 8.3 Access control standards are established for all information systems, at an appropriate level for each system, which minimises information security risks yet allows the organisation's business activities to be carried out without undue hindrance. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.
- 8.4 Access and removal of access to all systems will be managed by the Director of IT in line with SOP DG17 – User Registration, and must be authorised by the manager responsible for the system. A record must be maintained of such authorisations, including the appropriate access rights or privileges granted.
- 8.5 Persons accessing systems remotely to support business activities must be authorised to do so by an appropriate authority within the organisation. (SOP DG19 – Remote Access).
- 8.6 Access to Queen Mary's email system will be managed by the IT department and users will comply with SOP on using the system (SOP DG20 – Access to and Use of Email).

9. Network, System and Software Management

Queen Mary's network, systems and software is managed by the Director of IT under the oversight of the Information Services Board.

Network Management

Network segregation

- 9.1 The network must be segregated into separate logical domains with routing and access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting the organisation's business systems.

Remote access

- 9.2 Remote access to the network will be subject to robust authentication. Connections to the network are only permitted for authorised users ensuring that use is authenticated and data is encrypted during transit across the network. The implementation of new or upgraded software or firmware must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components.

Disconnection

- 9.3 Inactive connections to the organisation's business systems shall shut down after a defined period of inactivity to prevent access by unauthorised persons. (SOP DG21 – Disconnection from the System).

Open Access

- 9.4 Information systems purposely designed and constructed for open access may be operated without any requirement for users to identify themselves. Such systems will typically offer highly limited and restricted facilities and should permit access in read mode only, and then only to information which may legitimately be published without restriction.

Logs

- 9.5 Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff. (SOP DG22 – Maintenance of Security Logs).

10. Standard Operating Procedures (SOPs)

- DG01 Information Risk Assessments
- DG02 Business Continuity
- DG03 Confidentiality Agreements
- DG04 Contracting for IT Services
- DG05 Information Security Incident Reporting
- DG06 IT Malfunction Reporting
- DG07 Purchasing IT Hardware and Software
- DG08 Implementing IT Systems
- DG09 Information Classification
- DG10 IT Equipment Disposal
- DG11 System Access Controls
- DG12 Cryptographic Controls
- DG13 Records Management
- DG14 Storage of Information
- DG15 Handling Information
- DG16 Disposal of Information
- DG17 User Registration
- DG18 Password Management
- DG19 Remote Access
- DG20 Access to and use of Email
- DG21 Disconnection from the System
- DG22 Maintenance of Security Logs
- DG23 Computer Room Operation
- DG24 Working in Secure Areas
- DG25 Configuration Management and Change Control
- DG26 System Backup and Recovery
- DG27 IT Security Incident Management