IT Services Policy/Policy Document

DG12 - Cryptographic Controls - Policy

Prepared by: <Shelim Miah>
Version: 2.1
**Effective Date:** 16/12/2021  
**Next Review:** 16/12/2022

**Reviewers:**  
- Paul Smallcombe, Records & Information Compliance Manager  
- Rhianne Short, Information Security Manager  
- Shelim Miah, Risk & Governance Manager

**Policy Owner:**  
Name/Position: Rachel Bence, Chief Information Officer

**Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial version.</td>
<td>Benjamin Roberts</td>
<td>21/04/2010</td>
</tr>
<tr>
<td>1.1</td>
<td>Update paragraph 13</td>
<td>Ian Douglas</td>
<td>29/05/2015</td>
</tr>
<tr>
<td>1.2</td>
<td>Update</td>
<td>Shelim Miah</td>
<td>11/05/2017</td>
</tr>
<tr>
<td>1.3</td>
<td>Update</td>
<td>Paul Smallcombe</td>
<td>22/05/2017</td>
</tr>
<tr>
<td>1.4</td>
<td>Draft Finalised</td>
<td>Shelim Miah</td>
<td>12/06/2017</td>
</tr>
<tr>
<td>2.0</td>
<td>Final version</td>
<td>Shelim Miah</td>
<td>28/05/2018</td>
</tr>
<tr>
<td>2.1</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>16/12/2021</td>
</tr>
</tbody>
</table>

**Authorisation:**

Name / Position: Information Governance Group  
Signature: Information Governance Group  
Date: 16.12.2021
Contents

1. POLICY STATEMENT .................................................................................................................. 4
2. SCOPE ....................................................................................................................................... 4
3. POLICY DETAIL .......................................................................................................................... 4
4. ROLES & RESPONSIBILITIES .................................................................................................... 5
5. PROCESS AND PROCEDURES ................................................................................................. 5
6. MONITORING ............................................................................................................................. 5
7. EXCEPTIONS ............................................................................................................................... 5
8. REFERENCES ............................................................................................................................... 6
9. APPENDIX A - DEFINITIONS .................................................................................................... 6
1. **Policy Statement**

1.1 This policy ensures that the confidentiality, authenticity and integrity of information is protected at all times, by the use of Cryptographic controls when transmitting and storing data.

1.2 The Policy aims to:

- Outline the expectations of those who handle data/information.
- Ensure the security and protection of QMUL data/information.
- Sufficient controls are in place to minimise the risk of compromising data
- Implement controls to safeguard against misuse
- Outline roles & responsibilities
- Enhance Communications

2. **Scope**

2.1 This policy applies to all staff who have access to or wish to have access to data/information that is of a sensitive nature, including any third party who store or hold data for QMUL.

3. **Policy Detail**

3.1. Each organisational unit of the College shall have an Information Security Manager. One responsibility of the Information Security Manager is to advise members of that organisational unit about the use of encryption technology.

3.2. The Information Security Manager shall identify the appropriate level of encryption protection in a given security situation.

3.3. The Information Security Manager shall ensure that secret keys are securely recorded and stored so that encrypted data can be accessed by authorised persons if a key’s owner is unavailable.

3.4. Where secret key encryption is used it is the responsibility of the user, or group of users, to keep the key secret. Secret keys shall only be given to users who are authorised to have access to the information.

3.5. Where public key encryption is used users shall not share their private key.

3.6. Secret and private keys shall only be stored in an unencrypted form if there are both pressing operational requirements that dictate this (for example the need to allow equipment to restart unattended) and if increased care is taken to protect access to the storage medium.

3.7. Where a secret key has been compromised, the information shall be decrypted using the compromised key and immediately encrypted using a new key. All on-line data encrypted using the old key shall be re-encrypted using the new key. Off-line encrypted data held securely shall not be decrypted and re-encrypted.

3.8. Arrangements shall be made to ensure that any encrypted copies of business critical information must be recoverable after a disaster. Possible techniques may include, but are not limited to, the use of protected backups of the keys or the use of a key-escrow technique.
3.9. Mobile devices (e.g. laptops, mobile phones, PDAs, etc.) shall all be encrypted. Removable media (e.g. USB sticks, DVDs, etc.) containing Confidential or Restricted data must be encrypted.

3.10. Standalone computers, and networked PCs storing data locally, that contain Confidential or Restricted data (see SOP DG09 - Information Classification) must be encrypted.

3.11. Encryption must be used for remote access connections to QM information assets. Refer to DG19 - Remote Access

3.12. Where a member of staff is uncertain whether a cryptographic solution is appropriate this decision will be referred to the Information Security Manager.

3.13. Information must be encrypted using the current best practise encryption technique, for advice contact the QMUL IT Security Team.

4. Roles & Responsibilities

4.1. The Risk and Governance Manager will be responsible for initiating the review cycle for the policy, process document owner to carry out the review. The Document owner will assess and incorporate any comments or feedback received.

4.2. Once the document has been updated, the Risk and Governance Manager will take the document to the appropriate board for approval. All approved documentation are to be stored in a central repository and uploaded to the web where applicable.

5. Process and Procedures

5.1. The associated processes and guidance documents can be found by visiting the ITS webpage.

6. Monitoring

6.1. It is mandatory for anyone using an IT Account to comply with the IT Policies and any associated procedures. Where non-compliance is identified, ITS will take appropriate action, which may result in the IT Account and associated information system access being disabled.

6.2. Where breaches of IT Security and or Policies are suspected or detected they are to be reported to IT Security via the Service Desk.

6.3. The Risk & Governance Manager, is responsible for the; monitoring, revision and updating of this document.

7. Exceptions

7.1. In the event of an exception that is not addressed by this Policy. The matter will be firstly referred to the IT Lead Team (ITLT) for a decision.

7.2. The ITLT will then make a decision or refer this to the IT Strategy Board (ITSB) for guidance.
8. References
SOP DG09 – Information Classification
SOP DG19 – Remote Access

9. Appendix A - Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Asset</td>
<td>A piece of information such as a document, record or report that holds data that is valuable and can be sensitive.</td>
</tr>
<tr>
<td>Data Sets</td>
<td>A collection of data or information that could be contents of a database or a project file</td>
</tr>
<tr>
<td>Risk</td>
<td>An uncertain event or circumstance that, if it occurs, will affect the outcome of an objective</td>
</tr>
<tr>
<td>Process</td>
<td>A series of actions or steps taken in order to achieve a particular outcome</td>
</tr>
<tr>
<td>User</td>
<td>A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL’s systems.</td>
</tr>
<tr>
<td>ITLT</td>
<td>IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.</td>
</tr>
<tr>
<td>ITSB</td>
<td>IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.</td>
</tr>
<tr>
<td>IGG</td>
<td>Information Governance Group – provide assurance and guidance on information governance across QMUL.</td>
</tr>
<tr>
<td>QMSE (SET)</td>
<td>Queen Mary Senior Executive (QMSE or SET) is Queen Mary’s senior management team who advise the Principal on the management of day-to-day business as well as its long-term future. The group comprises the Principal, Vice-Principal and the Senior Officers in Professional Services</td>
</tr>
<tr>
<td>User</td>
<td>A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL’s systems.</td>
</tr>
</tbody>
</table>