IT Services Policy

DG05 – Information Security Incident Reporting

Previously Known as: IS Incident Reporting SOP
Prepared by: <Shelim Miah>
Version: 2.2
Effective Date: 02.02.2023  Review Date: 02.02.2024

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>David Pick</td>
<td>12/04/2010</td>
</tr>
<tr>
<td>1</td>
<td>Annual review - No change</td>
<td>Paul Smallcombe</td>
<td>04/03/2014</td>
</tr>
<tr>
<td>1.1</td>
<td>Annual Review - Minor updates</td>
<td>Paul Smallcombe</td>
<td>29/05/2015</td>
</tr>
<tr>
<td>1.2</td>
<td>Transferred onto a Policy Template</td>
<td>Shelim Miah</td>
<td>22/03/2016</td>
</tr>
<tr>
<td>1.3</td>
<td>Updates</td>
<td>Paul Smallcombe</td>
<td>17/05/2017</td>
</tr>
<tr>
<td>1.4</td>
<td>Draft Finalised</td>
<td>Shelim Miah</td>
<td>12/06/2017</td>
</tr>
<tr>
<td>1.4</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>24/05/2018</td>
</tr>
<tr>
<td>2.1</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>10/12/2021</td>
</tr>
<tr>
<td>2.3</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>02/02/2023</td>
</tr>
</tbody>
</table>

Authorisation:

<table>
<thead>
<tr>
<th>Name / Position</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Lead Team</td>
<td>IT Lead Team</td>
<td>02.02.2023</td>
</tr>
</tbody>
</table>
## CONTENTS

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

1.1 One of the most valuable assets that Queen Mary University of London (QM or QMUL) has is information, it is important to capture and store this information in line with QM information governance and retention Policies. QM has a legal obligation to protect this information against loss and unauthorised disclosure. In order to meet these obligations and protect this asset, it is important that information is managed so that it is classified, stored, handled and disposed of accordingly.

1.2 This policy ensures that information security incidents are managed in accordance with industry best practice and that all Information Security (IS) incidents are reported and captured in order to help bring the incident to a resolution.

1.3 The Policy aims to:
   - Outline the expectations of Information owners.
   - Ensure information security breaches are reported and managed
   - Minimise information loss and breaches
   - Outline roles & responsibilities
   - Enhance Communications

2 Scope

2.1 This policy applies to all staff, contractors, third party suppliers, visitors and students who may encounter or identify a potential IS incident. IS incidents may involve the loss or theft of physical and/or electronic information assets or damage to these. The process for managing IT security incidents is described in DG27 – IT Security Incident Management.

3 Policy Detail

3.1 Queen Mary must maintain an Information asset register that contains Highly Confidential, Confidential or Restricted information together with the name and role of the information asset owner and details of the organisation (internal or external) they work for. Refer to DG13 – Records Management Policy.

3.2 It is the responsibility of each Director/Head of Department to inform the Queen Mary Records & Information Compliance Manager of the existence of any data sets within their areas of responsibility containing Highly Confidential, Confidential or Restricted information as defined by DG09 – Information Classification Policy.

3.3 A log of all incidents that may impinge on any aspect of information security including, but not limited to, the confidentiality and integrity of the data, must be kept. Refer to DG13 – Records Management.

3.4 The QM Records & Information Compliance Manager is to make entries in the log of incidents. If any of the data sets are classified as Highly Confidential, Confidential or Restricted, the data owner must be notified.

3.5 The contents of the incident log are to be reviewed periodically, and in any case at least annually, and a report made to the Information Governance Group.
3.6 Queen Mary shall publish guidance about which types of data set or incident needs to be recorded in these registers or logs. Refer to DG09 – Information Classification. Queen Mary shall publicise this guidance periodically to all staff members of Queen Mary.

3.7 When an information security incident is detected, the appropriate line manager must assign a member of staff to act as an Incident Manager. An information security incident could be triggered as a result of a breach of physical security or a staff member reporting the loss or theft of information, or the discovery of information that Queen Mary is not legally entitled to hold.

3.8 The Incident Manager is to determine if any computer equipment may have been accessed, if so, report it as a possible breach of IT security to the IT Security Team, as per DG27 – IT Security Incident Management. The Incident Manager is to make a list of all non-computer-based information possibly placed at risk and report this to the QM Records & Information Compliance Manager.

3.9 If a risk to Highly Confidential, Confidential or Restricted information is identified it shall be reported to the QM Records & Information Compliance Manager who shall determine from the register the data owner responsible for the information at risk. The data owner shall assign an Incident Manager who shall determine the remedial action that must be taken.

3.10 In the event that a breach of IT security is detected it shall be investigated by a technically competent person. The investigator shall make a list of all computer-based information possibly placed at risk and report this to the QM Records & Information Compliance Manager.

3.11 Any disclosure of computer account credentials shall be regarded as a breach of IT security and must be handled as per SOP DG27 – IT Security Incident Management.

3.12 Whenever any data owner listed in the register of Highly Confidential, Confidential or Restricted information is notified of a possible breach of security, they shall determine the nature of the risk and take remedial action. This may include notifying all individual persons identified in the data set of the possible breach, what information was at what risk, and what action is being taken.

3.13 If the data owner is Barts Health NHS Trust (BH) then the BH Information Governance Team must be informed.

3.14 Any incident deemed to be serious by the QM Records & Information Compliance Manager shall be escalated to the Queen Mary Senior Executive team immediately, who will provide a report to the Audit and Risk Committee.

4 Process and Procedures

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

5 Roles & Responsibility

5.1 The Risk and Governance Manager will be the custodian of the document and manage its review and update. All approved documentation are to be stored in a central repository and uploaded to the web where applicable.

5.2 The QM Records & Information Compliance Manager is to make entries in the log of incidents. If any of the data sets are in the register of Highly Confidential, Confidential or Restricted data the data owner must be notified.
6 Monitoring

6.1 It is mandatory for all information asset owned or held by QM to comply with this Policy and any associated procedure. Where non-compliance is identified, appropriate action will be taken, which may result in escalation to senior management for action to be taken.

6.2 Checks will be made by the Risk and Governance Manager and the findings will be reported to the IT Lead Team (ITLT) in the first instance for corrective actions to be issued.

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

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 ITLT.

7.2 The ITLT will then make a decision or refer this to the IT Strategy Board (ITSB) for further guidance as necessary.

8 References

SOP DG09 – Information Classification
SOP DG13 – Records Management
SOP DG27 – IT Security Incident Management

9 Appendix A - Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Asset</td>
<td>Where valuable information or data that can be sensitive is captured and stored, this can be systems, physical paper, CD and mobile devices such as SD cards, pen drives etc.</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>A Risk can be anything (an action, event or set of circumstances) that can adversely or beneficially affect QM’s ability to achieve its current or future objectives</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><strong>User</strong></td>
<td>A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QM’s systems.</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ITLT</strong></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><strong>ITSB</strong></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><strong>IGG</strong></td>
<td>Information Governance Group – provide assurance and guidance on information governance across QM.</td>
</tr>
<tr>
<td><strong>QMSE</strong></td>
<td>Queen Mary Senior Executive (QMSE) 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-Principals and the Senior Officers in Professional Services</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QM’s systems.</td>
</tr>
</tbody>
</table>