IT Services Policy

DG27 – IT Security Incident Management

Prepared by: <Shelim Miah>
Version: 2.1
<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>08/12/2021</th>
<th>Review Date:</th>
<th>10/12/2022</th>
</tr>
</thead>
</table>

**Reviewers:**
- Henrik Brogger, Head of Service Delivery
- Jason Bunning, Head of Enterprise Systems
- 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>16/08/2010</td>
</tr>
<tr>
<td>1</td>
<td>Annual Review – No Change</td>
<td>Ian Douglas</td>
<td>23/06/2014</td>
</tr>
<tr>
<td>1.1</td>
<td>Transferred onto a Policy Template</td>
<td>Shelim Miah</td>
<td>22/03/2016</td>
</tr>
<tr>
<td>2.0</td>
<td>Finalised</td>
<td>Shelim Miah</td>
<td>22/03/2018</td>
</tr>
<tr>
<td>2.1</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>08/12/2021</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>10.12.2021</td>
</tr>
</tbody>
</table>
Contents

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

1.1 This policy ensures that IT security incidents are managed in accordance with industry best practice and that IT Security Incidents are reported and captured in order to react to incidents appropriately and timely.

1.2 The Policy aims to:
   - Outline how IT security incidents are managed.
   - Protect Queen Mary University of London’s (QM or QMUL) Assets
   - Implement appropriate measures to manage IT Security incidents.
   - Ensure a consistent approach to recording and maintaining IT security incidents.
   - Outline roles & responsibilities
   - Enhance Communications

2 Scope

2.1 The policy applies to all staff and students and may also apply to departments managing their own systems independent of ITS and any third party that wishes to access or use these systems.

3 Policy Detail

3.1 The Information Governance Group will maintain a register of computer systems holding data sets that contain information that is Restricted or above as defined by DG09 – Information Classification.

3.2 This register captures:
   - The details of the computer system(s) that holds information which is Restricted or above
   - The name of the person and their role within QM who is responsible for the operation of the computer system(s),
   - Any reference to dataset entries held by the QM Records and Information Compliance Manager
   - Information about the software used by those computer system(s).

3.3 The QMUL Records & Compliance Manager will also maintain a log of incidents where the computer systems holding information that is Restricted or above may have had any aspect of data security impinged.

3.4 Other incidents, for example, major incidents affecting the availability of computer systems, will also be recorded in the log.

3.5 The QMUL IT Security Team will provide advice and guidance to the QM Records & Information Compliance Manager regarding the degree of information required for logging different types of incidents. The QM Records & Information Compliance Manager will publish this guidance periodically to all members of QM.

3.6 Any person who may suspect a breach of the security of any computer system must report it to the IT Service desk or the team responsible for the computer system.
If any breach of physical or IT security is suspected or detected, the manager responsible for the area, the computer system(s) and peripherals must assign an Incident Manager.

Their role is to determine if any computer equipment, information records or user credentials have been compromised or stolen. Whether confirmed or suspected, this must be reported to the IT Security Team as well as the Estates security team as appropriate.

3.7 Any reports of IT-related security breaches must be investigated by the IT Security Team to determine the scope of the computer systems that may be at risk and inform both the overall Incident Manager and the QMUL Records & Information Compliance Manager of all data sets that may potentially be at risk.

3.8 A system investigator is to be appointed to report on the extent of the actual breach and inform the QM Records & Information Compliance Manager who shall notify the persons responsible for the data set as per DG05 – Information Security Incident Reporting.

3.9 Any disclosure of computer account credentials will be regarded as a breach of IT security and the standard notifications and actions taken. In this context, all systems to which the compromised account has access will be considered as potentially compromised.

3.10 The contents of the IT security incident log must be reviewed periodically, at least annually, and a report made to the Audit and Risk Committee.

3.11 Any incident deemed to be serious by the QM IT Security Team must be escalated to the Queen Mary Senior Executive team immediately, who will provide a report to the Audit and Risk Committee.

3.12 The IT Security Team will monitor the general IT threat landscape, especially for software used by its users, and notify the teams responsible for administering these systems to take the appropriate actions when significant threats have been identified.

3.13 Teams responsible for computer systems must also monitor the threat landscape of the software which they use and notify IT Security of any significant threats.

3.14 The IT Security Team must arrange periodic reviews, at least annually, of the information security requirements of each computer system in the register.

3.15 The QM Network Team must maintain a register of all (semi-) autonomous sub-networks connected to the QM network which will identify the network addresses used on that sub-network, the department or institute to which that sub-network belongs, and the person or role responsible for managing that sub-network.

3.16 If any computer system is determined to be at risk in any specific incident, both the person identified in this register and the local Information Security Manager for the department responsible for the network connection used by that computer must be included in the list of people to whom reports are made about the incident.

3.17 If a sub-network is determined to be a source or relay of any malware or network traffic causing other problems, the offending material or traffic must be blocked.
4 Process and Procedures

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

5 Roles & Responsibility

5.1 The Risk and Governance Manager will be responsible for initiating the review cycle for the policy. The Document owner will assess and incorporate any comments or feedback received.

5.2 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.

5.3 It is the responsibility of all staff and students to report any potential or actual breaches of both physical and virtual IT security.

5.4 The team responsible for the breached computer system are responsible for assigning the Incident manager who will determine if any computer equipment or records of computer access credentials might have been accessed and, if so, report it as a possible breach of IT security to the IT Security Team.

5.5 The IT Security Team shall determine the scope of the computer systems that might be placed at risk and any data sets that may have potentially been placed at risk and appoint a system investigator either from the IT Security team or from the team responsible for the Computer system.

5.6 The System Investigator must determine if any breach of the IT Security of the system actually occurred and report the actual extent of the breach to the overall Incident Manager and the IT Security Team. If Highly Confidential, Confidential or Restricted data has been put at risk the IT Security Team shall inform the QM Records & Information Compliance Manager who shall notify the persons responsible for the data set.

6 Monitoring

6.1 Compliance with this Policy is mandatory for all QMUL Staff. Where non-compliance is identified, ITS will take appropriate action, which may result in escalation to senior management for action to be taken.

6.2 Checks may be made by the Risk and Governance Manager and the findings may 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 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 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 DG05 – Information Security Incident Reporting
SOP DG09 – Information Classification
SOP DG13 – Records Management
## 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</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>sub-network</td>
<td>A subnetwork or subnet is a logical subdivision of an IP network.</td>
</tr>
<tr>
<td>Malware</td>
<td>short for malicious software, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising</td>
</tr>
</tbody>
</table>