IT Services Policy

DG24 – Working in Secure Areas

Prepared by: <Shelim Miah>
Version: 2.1
1 Policy Statement

1.1 To ensure that QMUL staff are able to undertake sensitive and critical work in designated secure and protected work areas that have a higher level of security.

1.2 The Policy aims to:

- Ensure that work in secure areas is managed in accordance with industry best practice.
- Ensure the security and protection of QMUL data.
- Implement controls to safeguard QMUL staff
- Outline roles & responsibilities
- Enhance communications

2 Scope

2.1 This policy is applicable to all QMUL Staff, requiring a secure work area space to carry out their research or testing.

3 Policy Detail

3.1 Work areas that require secure environments must be located in physically secure areas, protected by a physically sound security perimeter. All doors and windows must be suitably protected against unauthorised access. Secure areas shall be located to avoid access or even visibility by the public.

3.2 Access to secure areas shall be by authorised personnel only. Entry control mechanisms shall be used to ensure that only authorised personnel are allowed access and that all accesses are logged.

3.3 Access control shall require multiple authentication mechanisms such as Pin and swipe access.

3.4 Employees, contractors and third parties should only be aware of the existence of, or activities within, a secure work area on a need to know basis.

3.5 Personnel of contracted third-party service providers shall be given restricted access to secure areas and this shall be under supervision.

3.6 Unsupervised work in secure areas shall be avoided for safety reasons and to prevent opportunities for malicious activities.

3.7 Local procedures must be in place to ensure sufficient training and access protocols are in place which must be followed by staff entering these work areas.

3.8 Vacant secure areas shall be physically locked and periodically checked.

3.9 Secure areas shall be monitored by intruder detection systems and, where practical, CCTV, monitored by security staff.

3.10 Visitors to secure areas shall be accompanied at all times unless their access has been previously approved. A record shall be maintained of the arrival and departure times of all visitors.
3.11 All staff and visitors requiring access to secure areas shall be made aware of the security requirements outlined in this procedure and of emergency procedures.

3.12 No photographic, video, audio or other recording shall be permitted in secure areas without the prior approval of the appropriate director, head of department or institute manager.

### 4 Roles & Responsibility

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 Monitoring

5.1 It is mandatory for anyone carrying out sensitive work in these areas to comply with this policy and any associated procedures.

5.2 IT Services may request checks to be carried out as part of internal audits, any findings will reported to the IT Lead Team (ITLT) for any corrective actions to be issued.

5.3 Where non-compliance is identified and the corrective actions have not been implemented, ITS will take appropriate action, which may result in escalation to senior management.

### 6 Exceptions

6.1 In the event of an exception that is not addressed by this policy, the matter will be firstly referred to the ITLT.

6.2 The ITLT will then make a decision or refer this to the IT Strategy Board (ITSB) for a decision
## Appendix A

### 7.1 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Controller</td>
<td>The Data Controller is a person, group or organisation (in this case QMUL) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.</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>
</tbody>
</table>