IT Services Policy

DG04 – Contracting for IT Services Policy

Previously Known as: Confidentiality Agreement SOP
Prepared by: < Shelim Miah>
Version: 2.0
Effective Date: 20/02/2017  Status: Active

Reviewers: Kris Bush, Head of Business Support Services
            Henrick Brogger, Head of Service Delivery
            Amit Patel, Head of Service Management
            Bahar Shahin, Head of Procurement
            David Boakes, Assistant Director IT Operations

Policy Owner:
Name/Position Rhys Davies, Chief Information Officer

Previous name & number: DG03 Confidentially Agreement

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>Gerry Leonard</td>
<td>16/08/2010</td>
</tr>
<tr>
<td>2.0</td>
<td>Transferred onto a Policy Template</td>
<td>Shelim Miah</td>
<td>22/03/2016</td>
</tr>
<tr>
<td>2.0</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>24/05/2018</td>
</tr>
</tbody>
</table>

Authorisation:
Name / Position Rhys Davies, Chief Information Officer
Signature Rhys Davies
Date 28.05.18
1 Policy Statement

1.1 The purpose of this policy is to ensure that third party suppliers of services for the provision, maintenance or support of the QMUL’s IT systems are made aware of, and adhere to, the QMUL’s Policies, process and procedures during the period they have access to QMUL’s IT systems.

1.2 The Policy aims to:
- Outline the expectations of third party individuals and suppliers.
- Ensure the access of information is controlled and authorised.
- Ensure individuals and companies are held accountable for their actions.
- Outline roles & responsibilities.
- Enhance Communications.

2 Scope

2.1 The policy applies to all contractors, consultants and third party suppliers who have access to IT systems and the data held within them. This also applies to information that is held both electronic and on paper.

3 Policy Detail

3.1 The Procuring Officer must ensure all procurement is undertaken in accordance with QMUL’s Procurement Policies and alert the Procurement department to any requirement for confidentiality agreements.

3.2 Before any external supplier is given access to QMUL information, the Procuring Officer must ensure, a copy of the standard Confidentiality Agreement (CDA) is signed by the supplier and retained by the purchasing officer. (see SOP DG03 - Confidentiality Agreements). Only when a signed copy has been received can the supplier be provided with a work specification/tender documentation or any details of the QMUL’s operating systems.

3.3 Procuring officers must ensure as part of the procurement process, that a copy of QMUL’s Information Security Policies is provided to the supplier to sign as part of the contract for services. (see SOP DG07 - Purchasing IT Hardware and Software).

3.4 Where the procurement tender reaches the Official Journal of the European Union (OJEU) threshold, Procuring officers must ensure the CDA and the QMUL Information Security Policies are included as part of the tender documents. The CDA must be signed and returned immediately.

3.5 Where a Supplier has been selected, a suitable IT manager from QMUL must be appointed to oversee and manage the work of the individual.

3.6 Before a Supplier is provided access to QMUL’s IT Systems, the IT manager must induct the Supplier into QMUL’s operational environment, bringing to the attention of the Supplier’s relevant personnel the content of the IT Security Policies and what is expected of each employee in relation to their operations. Suitable arrangements must be made under SOP DG11 - System Access Controls to manage the Supplier’s access.
3.7 The IT manager must arrange for the Supplier’s staff to be provided with an individual unique credentials for accessing QMUL’s IT systems. The Supplier’s staff shall not share these credentials between themselves or with any other third party. Refer to SOP DG17 – User Registration.

3.8 The IT manager must monitor the supplier’s staff during the performance of their contract. Suppliers are expected, at all times, to be able to demonstrate their compliance with the QMUL’s Information Security Policies.

3.9 The IT manager must ensure that all instances of non-compliance are investigated and breaches dealt with in accordance with SOP DG05 -Information Security Incident Reporting. Such incidents shall be reported to the Suppliers contractual contact and dealt with according to the specified resolution procedures.

3.10 Note: Continued non-compliance will have contractual implications and be reported to the Queen Mary Procurement department. Suppliers will be made aware that non-resolution will lead to contract termination.

3.11 IT manager must, at the end or termination point of the contract, ensure all access rights, including physical and remote access, provided to the Supplier and its staff are removed.
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 responsible for initiating the review cycle for the document owner to carry out the review. The document owner will assess and incorporate appropriate comments/feedback received.

5.2 Once the document has been updated, the Risk and Governance Manager will request approval from the appropriate approval body. All approved documents are to be stored in a central repository and uploaded to the web where applicable.

6 Monitoring

6.1 It is mandatory for all contractors, consultants and third party suppliers to comply with this IT Policy and any associated procedure. 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 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 AD of IT Operations, in conjunction with 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 via the Assistant Director for IT Operations.

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 DG03 - Confidentiality Agreements
SOP DG05 - Information Security Incident Reporting
SOP DG07 - Purchasing IT Hardware and Software
SOP DG11 - System Access Controls
SOP DG17 - User Registration
QMUL’s published Procurement Policies
## 9 Appendix A

### 9.1 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Manager</td>
<td>Individual who oversees the work of a supplier, contractor or consultant</td>
</tr>
<tr>
<td>CDA</td>
<td>Confidentiality Agreement that outlines how QMUL data is to be treated</td>
</tr>
<tr>
<td>Supplier</td>
<td>A company or person from a company provides a services to QMUL, this also includes contractors and consultants</td>
</tr>
<tr>
<td>Procuring Officer</td>
<td>QMUL Staff member who is seeking the services of a consultant contractor</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>