Standard Operating Procedures (SOP) for:			
Contracting for IT Services			
SOP Number:	**DG04**	Version Number:	**1.1**
Effective Date:	**15 July 2014**	Review Date:	**07/07/2015**

Author: Reviewer:	**Gerry Leonard, Head of Research Resources** **Kris Bush, Head of Business Support Services**

Authorisation:	
Name / Position	**Chris Day, Director of IT Services**
Signature	**C Day**
Date	**15 July 2014**

Accountability:	
Position	Line Managers
Responsibility:	
Position	Procuring Officer Nominated IT Manager

Revision History			
Version	Description	Author	Date
1	Initial version.	Gerry Leonard	16/08/2010
1.1	Annual Review – Wording & terminology updates	Kris Bush	11/07/2014

Purpose and Objective:
The purpose of this SOP is to ensure that third party suppliers of services for the provision, maintenance or support of the College's IT systems are made aware of, and adhere to, the College's Information Security Policies and Standard Operating Procedures during the period when they have access to the College's IT systems.

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

SOP Text

	Responsibility	Activity
1.	Procuring Officer	Procuring Officer is the first point of contact with an external company that will be considered as a potential supplier of IT or other information related services to the College. The Procuring Officer shall ensure all procurement is undertaken in accordance

		with QMUL's Procurement Policies and alert the Procurement department to any requirement for confidentiality agreements.
2.	Procuring Officer	Procuring Officer shall, in the first instance, send to the external supplier, a copy of the standard Confidentiality Agreement (CDA) for signature (see SOP DG03 - Confidentiality Agreements). Only when a signed copy has been received shall the supplier be provided with a work specification/tender documentation or any details of the College's operating systems.
3.	Procuring Officer	If the service that is to be provided reaches the Official Journal of the European Union (OJEU) threshold, the Procuring Officer shall ensure that tender documents include a CDA, that must be returned immediately, and a copy of the College's Information Security Policies.
4.	Procuring Officer	Procuring Officer shall, as part of the procurement process, provide supplier with a copy of the College's Information Security Policies which shall form part of the contract for services that will be signed by the Supplier (see SOP DG07 - Purchasing IT Hardware and Software).
5.	Nominated IT Manager	Before a Supplier is provided with access to the College's IT System, a named IT Manager shall induct the Supplier into the College's operational environment, bringing to the attention of all 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 shall be made under SOP DG11 - System Access Controls to manage the Supplier's access.
6.	Nominated IT Manager	Shall arrange for the Supplier's staff to be provided with individual unique identifiers for accessing the College's IT systems. The Supplier's staff shall not share these identifiers between themselves or with any other third party. Refer to SOP DG17 – User Registration.
7.	Nominated IT Manager	Shall 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 College's Information Security Policies.
8.	Nominated IT Manager	Shall 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. Note: Continued non-compliance shall have contractual implications and be reported to the Queen Mary Procurement department. Suppliers shall be made aware that non-resolution will lead to contract termination.
9.	Nominated IT Manager	Shall, 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.