Standard Operating Procedures (SOP) for:			
IT Security Incident Management			
SOP Number:	**DG27**	Version Number:	**1**
Effective Date:	**15 July 2014**	Review Date:	**23/06/2015**

Author: Reviewer:	**David Pick, IT Services Security** **Paul Smallcombe, Records & Information Compliance Manager**

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

Accountability:	
Position	Line Managers
Responsibility:	
Position	Directors/ Heads of Department QM IT Security Team QM Records & Information Compliance Manager QM Central Network Team All members of the College

Revision History			
Version	Description	Author	Date
1	Initial version.	David Pick	16/08/2010
1	Annual Review – No Change	Ian Douglas	23/06/2014

Purpose and Objective:
To ensure that information technology security incidents are handled in accordance with industry best practice.

References:
SOP DG05 – Information Security Incident Reporting SOP DG09 – Information Classification SOP DG13 – Records Management

SOP Text

	Responsibility	Activity
1.	Directors/ Heads of Department	Each Director/ Head of Department shall inform the IT Security Team of the existence of any computer systems within their areas of responsibility containing Confidential or Restricted information as defined by SOP DG09 – Information Classification.
2.	QM IT Security Team	Queen Mary shall maintain a register of computer systems holding data sets held that contain Confidential or Restricted information as defined by SOP DG09 – Information Classification. This register shall identify the computer systems, the person or role within Queen Mary responsible for the operation of those

		computer systems, reference to the entries in the register of data sets held by the QM Records and Information Compliance Manager, and information about the software used by those computer systems. Refer to SOP DG13 – Records Management.
3.	QM IT Security Team	Queen Mary shall maintain a log of incidents that may impinge on any aspect of data security for the computer systems holding Confidential or Restricted information including, but not limited to, the confidentiality and integrity of the data. Other incidents, for example, major incidents affecting the availability of computer systems, shall also be recorded in the log. Refer to SOP DG13 – Records Management.
4.	QM IT Security Team QM Records & Information Compliance Manager	The QM IT Security Team will advise the QM Records & Information Compliance Manager about any information or guidance they receive or generate about the degree of logging required for different types of incident. The QM Records & Information Compliance Manager shall publish this guidance periodically to all members of Queen Mary.
5.	Incident Manager	Where a breach of physical security is detected an Incident Manager shall be assigned. The Incident Manager of that physical breach shall 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.
6.	Any person aware of a potential breach of IT Security	Where a suspicion of any breach of the security of any computer system registered with the IT Security Team is raised it shall be reported to the IT Security Team. If there is any doubt about it, it shall be reported.
7.	QM IT Security Team	When it receives a report of a potential or actual breach of IT security, the IT Security Team shall determine the scope of the computer systems that might be placed at risk. The IT Security Team shall consult its registers and inform both the overall Incident Manager and the QM Records & Information Compliance Manager of all data sets that may have potentially been placed at risk.
8.	QM IT Security Team	The IT Security Team shall consult with the person or team responsible for each computer system possibly involved and appoint a technically-competent System Investigator for that particular breach, either from the IT Security Team or from the team responsible for the computer system(s) involved.
9.	System Investigator QM Records & Information Compliance Manager	The System Investigator shall determine if any breach of the IT Security of that system actually occurred and report the actual extent of the breach to the overall Incident Manager and the IT Security Team. If 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 as per SOP DG05 – Information Security Incident Reporting.
10.	All Members of Queen Mary	Any disclosure of computer account credentials shall 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 shall be considered as potentially compromised.

11.	QM IT Security Team	The contents of the IT security incident log shall be reviewed periodically, and in any case at least annually, and a report made to the Audit and Compliance Committee.
12.	QM IT Security Team	Any incident deemed to be serious by the QM IT Security Team shall be escalated to the Queen Mary Senior Executive immediately, who will provide a report to the Audit and Compliance Committee.
13.	QM IT Security Team Any person responsible for a computer system used for handling Confidential or Restricted data	The IT Security Team shall monitor the general IT threat landscape, especially for software used by any computer system registered with it, and notify the teams responsible for computer systems handling Confidential or Restricted data of significant threats. The team responsible for any computer system shall also monitor the threat landscape of the software which they use and notify the IT Security Team of any significant threats. The IT Security Team shall arrange periodic reviews, at least annually, of the information security requirements of each computer system in the register.
14.	QM Central Network Team	The QM Network Team shall maintain a register of all (semi-) autonomous sub-networks connected to the College 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.
15.	Any person conducting any part of an IT Security Incident investigation	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 shall be included in the list of people to whom reports are made about the incident.
16.	QM Central Network Team	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 shall be blocked.