Standard Operating Procedures (SOP) for:			
Maintenance of Security Logs			
SOP Number:	**DG22**	Version Number:	**1**
Effective Date:	**15 July 2014**	Review Date:	**23/06/2015**

Author: Reviewer:	**William Mordaunt, IT Services Project Manager** **Ian Douglas, Head of IT Security**

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

Accountability:	
Position	Directors/ Heads of Department
Responsibility:	
Position	Directors/ Heads of Department

Revision History			
Version	Description	Author	Date
1	Initial version.	William Mordaunt	26/04/2010
1	Annual Review – No Change	Ian Douglas	23/06/2014

Purpose and Objective:
To detect and record unauthorized information processing activities.

References:
QMUL Records Retention Policy and Schedule

SOP Text

	Responsibility	Activity
1.	IT Services / Departments Operating Computer Systems	Audit logs recording user activities, exceptions, and information security events shall be produced and retained for an agreed period, defined in the Records Retention Schedule, to assist in future investigations and access control monitoring.
2.	IT Services / Departments Operating Computer Systems	Audit logs shall include: User IDs Dates, times, and details of key events, e.g. log-on, log-off Workstation identity or location where possible any network addresses available, especially IP or MAC addresses
3.	IT Services / Departments Operating Computer Systems	Logging facilities and log information shall be protected against tampering and unauthorised access.

4.	IT Services / Departments Operating Computer Systems	The implementation of logging facilities shall take into account the risk of the storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.
5.	IT Services / Departments Operating Computer Systems	The clocks of all relevant information processing systems shall be synchronised with an accurate time source to ensure the accuracy of audit logs which may be required for investigations or as evidence in legal or disciplinary cases.
6.	IT Services / Departments Operating Computer Systems	Audit logs shall be reviewed periodically and corrective measures taken.