Standard Operating Procedures (SOP) for:			
System Access Controls			
SOP Number:	**DG11**	Version Number:	**1**
Effective Date:	**7 Dec 2015**	Review Date:	**07/12/2018**

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

Authorisation:	
Name / Position	**IT Services Lead Team**
Signature	**C Day**
Date	**23 November 2015**

Accountability:	
Position	Line Managers
Responsibility:	
Position	Director of IT Services Heads of Department Application Administrators

Revision History			
Version	Description	Author	Date
1	Initial version.	William Mordaunt	26/05/2010
1	Annual Review – no changes	Ian Douglas	23/06/2014
1	Annual Review No Change	Ian Douglas	21/07/2015

Purpose and Objective:
To prevent unauthorized access to information systems. To prevent unauthorized access to information held in application systems.

References:
SOP DG09 – Information Classification SOP DG17 – User Registration SOP DG27 – IT Security Incident Management Guidelines on the Right to Privacy and the Monitoring of Data

SOP Text

	Responsibility	Activity
1.	IT Services & Departments which operate their own IT systems	Log-on screens shall include, where possible, a general notice warning that the system should be accessed only by authorised users, with a brief description of the criteria by which they are identified (e.g. employees, contract staff, suppliers or students of QMUL).

2.	IT Services & Departments which operate their own IT systems	Log-on screens shall include a general notice warning that systems may be monitored and that unauthorised access or use may result in disciplinary proceedings and that evidence collected may be passed on to law enforcement agencies. Refer to Guidelines on the Right to Privacy and the Monitoring of Data
3.	IT Services & Departments which operate their own IT systems	Where possible, log-on screens shall not display any system or application identifiers until the log-on process has been successfully completed. The screen shall not provide help messages during the log-on, particularly not warnings about how many incorrect entries are allowed.
4.	IT Services & Departments which operate their own IT systems	Password characters shall be hidden during log-on and encrypted prior to being sent across the network.
5.	IT Services & Departments which operate their own IT systems	The system shall validate the log-on data only on completion of input and then, if there is an error, the system shall not explain which part of the data is incorrect but simply require the user to try again.
6.	IT Services & Departments which operate their own IT systems	The system shall automatically record unsuccessful logon attempts and limit the number of consecutive unsuccessful log-on attempts. After the limit has been reached the system shall reject further attempts and log-on shall be automatically disabled for the account for a pre-defined period of time.
7.	IT Services & Departments which operate their own IT systems	Where possible, the system shall limit the maximum time allowed for log-on attempts in order to avoid providing attackers with time to guess correct details.
8.	IT Services & Departments which operate their own IT systems	After successful log-on, the system shall display, where possible, details of the date and time of the last successful log-on. This will enable an authorised user to check whether the previous log-on was performed by someone else and report an IT security incident if necessary, as per SOP DG27 IT Security Incident Management.
9.	IT Services & Departments which operate their own IT systems	Users' access rights to systems shall be limited to those systems that they are authorised to use. Access rights shall initially be granted as part of the user registration process, but may be extended or revoked as the user changes their role. Refer to SOP DG17 User Registration.
10.	Application Administrator	Access to functions within applications shall be restricted by the use of menus and the security features of the applications themselves. Application security shall be controlled by an Application Administrator.

11.	Application Administrator	Users' access rights within systems shall take account of the functions that they need to perform such as read, write, delete, and execute.
12.	Application Administrator	Wherever possible, application systems that include audit trail capabilities shall have such capabilities enabled if the systems contain Confidential or Restricted data, as defined in SOP DG09 – Information Classification.