Queen Mary
University of London

IT Services Policy

DG19 – Remote Access

Prepared by: < Shelim Miah>
Version: 2.0

Description & Target Audience: This document outlines the use of remote access for IT Support activities and users who may wish to work remotely. This document is aimed at all Staff and 3rd Party Vendors.			
Effective Date:	**31/03/2017**	Review Date:	**31/03/2018**

Reviewers:	**Craig Walker, IT Service Desk Manager** **Ian Douglas, Head of Information Security** **Henrick Brogger, Head of Student & Staff Support Services** **Amit Patel, Head of Service Management** **Martin Evans, Head of Data Centre Services** **Paul Gallagher, Interim Assistant Director Applications** **Johnathan O'Reagan, Assistant Director Infrastructure** **David Boakes, Assistant Director Student & Staff Services**
Policy Owner:	
Name/Position	Katie Friis, Interim Deputy Director IT Services

Revision History			
Version	Description	Author	Date
1	Initial version.	David Pick	01/06/2010
1	Annual Review – No Change	Ian Douglas	23/04/2014
1.1	Section on Remote Vendor access added	Ian Douglas	16/01/2015
1.2	Additional Clauses added	Ian Douglas	29/05/2015
1.3	Updated to Policy template & reviewed	Shelim Miah	28/11/2016
1.4	Reviewed with David Boakes	Shelim Miah	16/03/2017
2.0	Finalised	Shelim Miah	31/03/2017

Authorisation:	
Name / Position	**Katie Friis Interim Deputy Director of IT services**
Signature	**Katie Friis**
Date	**31/03/2017**

CONTENTS

1 Policy Statement

1.1 IT Services (ITS) provides a remote access solution to support students and staff who may work from remote locations. In offering this service ITS must ensure that support is available should users require it. This enables Queen Marys University of London (QMUL) users to benefit from flexible working practises, distance learning and enhances communications. This policy ensures that remote access is managed and information and IT services are protected.

1.2 The policy aims to:

- Outline the expectations of remote access users.
- Ensure appropriate controls are in place to protect QMUL data.
- Ensure access to remote services are managed
- Outline roles & responsibilities
- Enhance communications

2 Scope

2.1 The policy applies to all users accessing IT services and QMUL data from remote locations. It also applies to 3rd party suppliers and IT staff who wish to access users' desktop terminals or IT systems to carry out remedial work.

2.2 The phrase "remote access" covers both "mobile users" and "teleworkers". Mobile users work casually from a number of remote locations, using equipment that is either their own or supplied by 3rd parties; the equipment may be a mobile device (smart-phone, PDA, etc.) or a standard computer. Teleworkers have a much more formal arrangement, usually with QMUL-supplied equipment, to work remotely; the more formal arrangement means that the management of the remote equipment is under QMULs control.

3 Policy Detail

3.1 Any Remote Access Solution (RAS) used to access Central IT Systems and user terminals must be approved by IT Security and the Domain Team Leads (DTL) group.

3.2 Whilst evaluating the RAS solution the group must consider any potential risk of data being compromised, for example data may be stored locally on a public computer. The decision must then be documented whether approved or rejected.

3.3 Remote access credentials such as a username and password must not be transferred across a network without encryption, especially the general Internet. They must not be stored "in clear text". Refer to DG12 – Cryptographic Controls and DG18 – Password Management.

3.4 Remote access must have enhanced authentication whether a Virtual Private Network (VPN) or remote session access (e.g. VDI, Thin Linc, RDP etc.) from any non QMUL or untrusted network.

3.5 When remote assistance is required for example when someone is connecting to a device as a local user to resolve or demonstrate the use of an application;

3.6 The following four controls must be in place:

- The local user has to take a positive action to enable the remote session
- The local user must be able to view the actions taken by the remotee
- The local user must be able to terminate the session at any time
- Business processes must be in place that reminds the local user to close any application showing sensitive data prior to the remote session being established

3.7 Where a 3rd party vendor requires access in order to provide support to QMUL as part of a support contract the following controls must also be in place:

- Access to the system or application must be controlled by QMUL. A member of QMUL must take a positive action to enable the access
- All vendor access must be pre-arranged with QMUL and fall under appropriate change control
- Access must be for a defined time period only and is not open access
- Access must be limited to the system or application that the vendor is supporting

3.8 Any device that intends to be used for remote access must have a suitable anti-virus with the latest definition updates installed and protected with a Firewall.

3.9 ITS must periodically, as technology changes, review and advise on new RAS and the preferred technology strategies for remote access.

4 Process and Procedures

4.1 The associated processes and guidance documents can be found by visiting the ITS webpage, some pages maybe restricted to IT staff.

5 Monitoring

5.1 All RAS that require access to the central IT Systems or used to provide technical support to users must comply with this policy. Where non-compliance is identified, ITS will take appropriate action.

5.2 The Information Security Manager will make checks and report the findings to the IT Lead Team (ITLT) in the first instance for corrective actions to be issued.

5.3 The AD of Student and Staff Support Services, in conjunction with the Risk & Governance Manager, is responsible for the; monitoring, revision and updating of this policy.

6 Exceptions

6.1 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 Student & Staff Services.

6.2 The ITLT will then make a decision or refer this to the IT Strategy Board (ITSB) for further guidance if necessary.

6.1 Where compliance to this policy is not possible due to technical, financial or regulative reasons, an exception must be raised to the appropriate group for approval so that it can be recorded as being granted exception to the policy.

6.2 It is acknowledged that some remote access in the application space do not comply with the enhanced authentication requirement due to the technical infrastructure place.

7 References

SOP DG09 – Information Classification
SOP DG12 – Cryptographic Controls
SOP DG15 – Handling Information
SOP DG18 – Password Management
SOP DG19 – Remote Access

8 Appendix A – Definitions

Term	Meaning
QMUL	Queen Mary University of London
JANET	Joint Academic Network, the organisation the provides QMUL with Internet connectivity
ITS	IT Services
RAS	Remote Access Solution
Remotee	Individual who access the device of a user to provide technical support. This individual can be QMUL support staff or a 3rd party vendor or in some cases this can be a user.
BYOD	Bring Your Own Device refers to users using their own device (which is not owned or provided to you by QMUL) to access and store QMUL information, whether at the place of work or remotely, typically connecting to the QMUL's Wireless Service.
Data Controller	The Data Controller is a person, group or organisation (in this case QMUL) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
User	A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL's systems.
ITLT	IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.
ITSB	IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.
Account Sponsor	Can be a line manager or person of authority that is responsible and accountable for an IT Account that has been issued.
Policy	A set of rules or framework that outlines the boundaries in which to operate.
Process	A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs
SOP	Standard Operating Procedure is a documented high level step-by-step sequence of Operational activities for adhering to policies that can be replicated across several departments and team.
Procedural Document	A set of low level detailed instruction that specify exactly what steps to follow to carry out an activity. E.g. instructions on how to print.
SPOC	Single Point of Contact; a person that acts the coordinator or focal point of information concerning an activity or program