Queen Mary
University of London

IT Services Policy

DG28 – Network Management

Prepared by: < Shelim Miah>
Version: 2.0

Description & Target Audience: This document outlines how the network is to be managed and the security precaution that must be in place. This document is aimed at all IT Staff who are in anyway involved in managing, operating, maintaining and supporting the IT Network in Queen Marys University (QMUL).			
Effective Date:	**31/03/2017**	Review Date:	**31/03/2018**

Reviewers:	**Ian Douglas, Head of Information Security** **Tavinder Jandu, Head of Network Services** **Amit Patel, Head Service Management** **David Boakes, Assistant Director Student & Staff Services**		
Policy Owner:			
Name/Position	Katie Friis, Interim Deputy Director of IT Services		
Revision History			
Version	Description	Author	Date
0.1	Initial version.	Shelim Miah	10/06/2015
0.2	Review	Ian Douglas	20/07/2015
0.3	Change to section 5, comments from Tavinder	Shelim	10/08/2015
1.0	Finalised	Shelim	10/08/2015
1.1	Update template to policy and review	Shelim Miah	16/02/2017
1.2	Review with David Boakes	Shelim Miah	13/03/2017
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 Queen Marys University of London (QMUL) networks are an essential enabler to the day-to-day operational needs. This means that the security of the IT networks is paramount to protecting QMULs systems and its data.

1.2 This policy outlines the terms and conditions for the management and use of QMUL's IT Network to protect the IT resiliency and the university from disruption to its services.

1.3 The policy aims to:

- Outline the expectations of network administrators and managers
- Ensure the security and protection of QMUL data.
- Implement controls to safeguard the IT Network
- Outline roles & responsibilities
- Enhance communications

2 Scope

2.1 This policy is applicable to the central IT Network, any device or application that connects to or uses the central IT Network must adhere to this policy, including e-mail and internet services.

3 Policy Detail

3.1 The IT Network, policies, processes and procedures must be compliant with external providers such as JANET.

3.2 The IT Network design must cater for the different levels of security requirements within QMUL.

3.3 New connections (wired or wireless) of equipment to QMUL Networks may only be made by, or with the authority of, the ITS Infrastructure team.

NB Authority is assumed granted when following a standard process, for instance attaching a BYOD to the network.

3.4 Network connections (including the dual-homing of systems) between QMUL networks, external networks or network domain must only be made by, or with the authority of, the ITS Infrastructure team.

Network Architecture

3.5 The network must be segregated into separate logical trust domain determined by data confidentiality classification, intended user location and business criticality.

3.6 There must be appropriate routing and access controls operating between the domains.

3.7 Appropriately, configured firewalls shall be used to protect the networks supporting the organisations business systems.

3.8 The QMUL Network is divided into Security Domains with network traffic to and from a domain mediated by a Firewall. Security Domains must be designed to provide appropriate levels of security to the data held within them. Restricted or Confidential data must be held in Security Domains that have been approved by IT Security to hold that level of data.

Network Security

3.9 Configuration access to QMUL network equipment must be controlled; authorised staff must use access credentials that uniquely identify them.

3.10 Shared accounts for managing network equipment are prohibited.

3.11 All IP addresses in use must be registered with an appropriate entry in the Domain Name System and this registration must be kept up-to-date.

3.12 Appropriate logs must be kept so that it is always possible to determine who/what was using a particular IP address at a particular time. Logs should be retained in line with the Universities retention policy.

3.13 Network equipment must be configured to drop any protocols unless they are explicitly allowed. The ITS Network team with oversight from IT Security have the responsibility of determining what protocols are allowed.

3.14 Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

3.15 Network security configurations such as firewall rules etc. must be documented in order to provide security assurance and auditability.

3.16 All network monitoring must be done in full compliance with QMUL Monitoring Policy. IT must monitor for and manage network security incidents.

Wireless

3.17 All wireless access to QMUL networks must be centrally managed and monitored by, or with the authority of, IT.

3.18 All wireless networks must be secured to prevent open access. Wireless access to the QMUL network must be authenticated and logged.

3.19 The use of a wireless access point must be compatible with the security category of the network domain it gives access to.

4 Process and Procedures

4.1 The associated processes and guidance documents can be found by visiting the IT Services webpage.

5 Monitoring

5.1 It is mandatory for anyone using or connecting to the central IT Network to comply with the IT Policies and any associated procedures. Where non-compliance is identified, ITS will take appropriate action, which may result in the access to the central Network being denied.

5.2 Where breaches of IT security and or policies are suspected or detected they are to be reported to IT Security via the Service Desk.

5.3 The AD Infrastructure, in conjunction with the Risk & Governance Manager, is responsible for the; monitoring, revision and updating of this document.

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 IT Lead Team (ITLT) for a decision 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 guidance.

6.3 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.

6.4 It has been acknowledged that there are some parts of the Network configuration, which were undocumented during the commissioning of the new network, and not all IP address usages are logged.

7 References

- SOP DG28 – Network Management
- JANET Acceptable Use Policy

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
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