Queen Mary
University of London

IT Services Policy

DG18 – Password Management Policy

Prepared by: < Shelim Miah>
Version: 2.0

Effective Date:	**20/06/18**	Review Date:	**20/06/2021**

Reviewers:	**Kathy Whelan, IT Service Desk Manager** **Konrad Dziedzic, Infrastructure Software Manager** **Amit Patel, Head of Service Management** **Martin Evans, Head of Data Centre Services** **David Boakes, Assistant Director Student & Staff Services**
Policy Owner:	
Name/Position	Rachel Bence, Chief Information Officer

Revision History			
Version	Description	Author	Date
1	Initial version.	William Mordaunt	28/05/2010
1.1	Annual Review – No Change	Ian Douglas	23/04/2014
1.2	Added admin change requirement in step 11	Ian Douglas	28/11/2014
2.0	Transfer onto new layout	Shelim Miah	10/11/2016
2.0	Review	Shelim Miah	10/07/2018
2.1	Updated 3.8	Kathryn Whelan	15/05/2020

Authorisation:	
Name / Position	**Rachel Bence, CIO**
Signature	**R.Bence**
Date	**15/05/20**

CONTENTS

1 Policy Statement

1.1 Staff and students use Queen Marys University of London's (QMUL) Systems and Services to access information. This information and any associated data must be protected and only accessible by those authorised to do so. Passwords and User names are issued to users to control access and protect information, whilst allowing authorised users to accesses information when required.

1.2 This Policy ensures that passwords are set and managed in accordance with best practise to prevent the misuse of the unauthorised access to information.

1.3 The Policy aims to:

- Outline the expectations of Users and guidelines for maintaining passwords.
- Ensure the security and protection of QMUL data.
- Implement controls to safeguard both users and support staff
- Outline roles & responsibilities
- Enhance communications

2 Scope

2.1 This policy is applicable to all IT account holders either studying or working at QMUL and any user who has been assigned a password in order to access data, system or services.

3 Policy Detail

3.1 All users must have a username and password for their personal and sole use for access to IT services. The username and password must not be shared or disclosed to anyone for any reason.

Refer to **Notes on Guidance on the Council Regulation Concerning Information Technology.**

3.2 Systems shall not be configured to allow users to login without a password. Exceptions shall be granted for specialised devices such as public access kiosks, when these devices are configured with public user accounts, they must have extremely restricted permissions (e.g. web only).

3.3 Systems must log the number of successful and failed attempts to a system and lock the account when a reasonable number of failed attempts has been reached such 5-10 failed attempts.

3.4 Where an account has been locked or disabled, the user must undergo a process of verification successfully before the account can be re-enabled.

3.5 Where operating systems dictate that system admin accounts require usernames and passwords to be shared between a group of people the following measures must be in place to reduce the risk of compromising the passwords:

- Whenever any member of the group leaves the group, even if it is to a different appointment in the University, the password must be changed.

- Whenever possible, systems administrators shall be assigned privileges to their personal usernames that are appropriate for their role and necessary for the specific tasks that need to be carried out. This is possible on all modern systems: UNIX/Linux and modern versions of Windows can all be operated in this way.
- Whenever possible, direct logins using the administrative accounts shall only be allowed from, a screen and keyboard directly attached to the system itself, and not via the network. The operating system shall be configured to prohibit network login attempts by any privileged account.
- No personal account shall have administrative level access rights, a separate admin account must exist and access to this account must be controlled at all times.

3.6 Users are required to maintain their own passwords. They shall be provided initially with a secure temporary password, which they are forced to change immediately.

3.7 Users shall use the QMUL password reset tool to manage central IT account passwords, all other passwords that are not integrated or linked to the central IT account must comply with this policy.

3.8 When choosing a password the user must ensure it is strong by, including, but not limited to, the following:

- Easy to remember
- Not based on anything that could be easily guessed using personal related information, e.g. names, telephone numbers, dates or birth, vehicle registrations, etc.
- Not consisting of a word included in a dictionary, or any of the obvious methods of manipulating dictionary words like replacing letters by digits
- Free of repeating identical all-numeric or all-alphabetic characters
- be at a minimum 12 characters or longer

3.9 Users must avoid keeping a record (e.g. paper or electronic) of passwords, where a record has been kept it must be destroyed immediately.

3.10 Users must not include passwords in any automated logon process (e.g. scripts, macros etc.).

3.11 Users must not use the same password for QMUL and personal purposes.

3.12 Users must avoid replicating the same password across several accounts, systems, services etc. As a compromise on one account will mean all accounts and services are compromised.

3.13 Users must verify their identity before being issued with a new or replacement password.

3.14 Passwords will be re-set in response to requests over the telephone only if there is no doubt as to the identity of the user making the request.

3.15 Temporary passwords must be unique and shall not be guessable.

3.16 Passwords must not be distributed via email except as part of an approved IT Services process.

3.17 Passwords must not be stored on computer systems in an unprotected form.

3.18 Default vendor passwords must be altered following installation of systems or software. Where possible Admin account names should also be changed.

3.19 IT support staff shall not request users to disclose their passwords when providing support or investigating problems

3.20 It is not mandatory that passwords be changed frequently. All users, however, must be required to change passwords whenever there is any indication of possible system or password compromise and to report such instances to IT Services.

4 Process and Procedures

4.1 The associated processes and guidance documents can be found by visiting the Password Reset Manager Tool webpage.

5 Monitoring

5.1 It is mandatory for anyone using an IT Account or wishes to gain access to QMUL data 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 IT Account and associated information system access being disabled.

5.2 Checks will be made by the Risk and Governance Manager and the findings will be reported to the IT Lead Team (ITLT) in the first instance for corrective actions to be issued.

5.3 The AD of IT Operations, in conjunction with the Risk & Governance Manager, is responsible for the monitoring, revision and updating.

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 IT Operations.

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

7 References

- DG 27 - IT Security Incident Management.
- SOP DG18 Password management

8 Appendix A

8.1 Definitions

Term	Meaning
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.
Strong Password	A strong password consists of at least twelve characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.). Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase.