IT Services Policy

DG21 – Disconnection from Systems

Prepared by: <Shelim Miah>
Version: 2.1
Effective Date: 03/12/2021  
Review Date: 03/12/2022

Reviewers: Rhianne Short, Information Security Manager  
Shelim Miah, Risk & Governance Manager

Policy Owner: Rachel Bence, Chief Information Officer

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial version.</td>
<td>William Mordaunt</td>
<td>26/04/2010</td>
</tr>
<tr>
<td>1</td>
<td>Annual Review – No Change</td>
<td>Ian Douglas</td>
<td>23/06/2014</td>
</tr>
<tr>
<td>1.1</td>
<td>Annual Review – Point 3 added</td>
<td>Ian Douglas</td>
<td>21/07/2015</td>
</tr>
<tr>
<td>1.2</td>
<td>Review and update of template</td>
<td>Shelim Miah</td>
<td>20/02/2017</td>
</tr>
<tr>
<td>1.3</td>
<td>Review DIB</td>
<td>DIB</td>
<td>12/10/2018</td>
</tr>
<tr>
<td>2.0</td>
<td>Finalised</td>
<td>ITLT</td>
<td>29/10/2018</td>
</tr>
<tr>
<td>2.1</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>08/12/2021</td>
</tr>
</tbody>
</table>

Authorisation:  

<table>
<thead>
<tr>
<th>Name / Position</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Lead Team</td>
<td>IT lead Team</td>
<td>08/12/2021</td>
</tr>
</tbody>
</table>
# CONTENTS

1 POLICY STATEMENT .................................................................4
2 SCOPE ..................................................................................4
3 POLICY DETAIL .....................................................................4
4 PROCESS AND PROCEDURES ...............................................5
5 MONITORING .........................................................................5
6 EXCEPTIONS ...........................................................................5
7 REFERENCES ...........................................................................5
8 APPENDIX A ...........................................................................6
   8.1 DEFINITIONS .....................................................................6
1 Policy Statement

1.1 Queen Mary University of London (QMUL) networks and systems are an essential enabler to the day-to-day business of the organisation. The security of the networks is paramount to protecting the systems and data of QMUL. This document ensures that users are disconnected from QMUL network and systems after a period of inactivity to protect QMUL systems and data.

1.2 The policy aims to:

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

2 Scope

2.1 This policy is applicable to all QMUL central IT Network and systems, any device or application that connects to or uses the central IT Network and systems.

3 Policy Detail

3.1 QMUL centrally managed PCs, Laptops and workstations shall have password-enabled screen savers configured so that the screen content is no longer visible and the device secured against unauthorised access after a defined period of inactivity.

3.2 Systems that are accessed using thin-client or web-based interfaces shall have session timeouts configured so that the session is automatically disconnected after a defined period of inactivity. The actual timeout periods will be agreed between the system owners and IT Services, or the department operating the system, according to the sensitivity of the data being accessed.

3.3 IT Services (ITS) will disconnect systems from the QMUL central network if they are posing a risk to other systems or information.
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 and systems 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 and systems 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 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.

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

7 References

- SOP DG21 – Disconnection from the System
## 8 Appendix A

### 8.1 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>QMUL</td>
<td>Queen Mary University of London</td>
</tr>
<tr>
<td>JANET</td>
<td>Joint Academic Network, the organisation the provides QMUL with Internet connectivity</td>
</tr>
<tr>
<td>ITS</td>
<td>IT Services</td>
</tr>
<tr>
<td>Users:</td>
<td>All Students, Staff or otherwise authorised users of QMUL IT Systems and Services</td>
</tr>
<tr>
<td>BYOD</td>
<td>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.</td>
</tr>
</tbody>
</table>