IT Services Policy

DG22 – Maintenance of System Security Logs

Prepared by: <Shelim Miah>
Version: 2.0
Effective Date: 22/03/2018  Review Date: 28/03/2018

Reviewers: Kathy Whelan, IT Service Desk Manager
Henrik Brogger, Head of Service Delivery
Amit Patel, Head of Service Management
Martin Evans, Head of Data Centre Services
David Boakes, Assistant Director IT Operations

Policy Owner:
Name/Position Rhys Davies

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</td>
<td>Annual Review – No Change</td>
<td>Ian Douglas</td>
<td>21/07/2015</td>
</tr>
<tr>
<td>1.1</td>
<td>Transferred onto a Policy Template</td>
<td>Shelim Miah</td>
<td>22/03/2016</td>
</tr>
</tbody>
</table>

Authorisation:
Name / Position Rhys Davies
Signature R.Davies
Date
## CONTENTS

1 POLICY STATEMENT ........................................................................................................... 4

2 SCOPE .................................................................................................................................. 4

3 POLICY DETAIL .................................................................................................................... 4

4 PROCESS AND PROCEDURES ............................................................................................. 5

5 ROLES & RESPONSIBILITY ................................................................................................ 5

6 MONITORING ...................................................................................................................... ERROR! BOOKMARK NOT DEFINED.

7 EXCEPTIONS ....................................................................................................................... ERROR! BOOKMARK NOT DEFINED.

8 REFERENCES ....................................................................................................................... 5

9 APPENDIX A ........................................................................................................................ 6
1 Policy Statement

1.1 This policy ensures that all unauthorised information-processing activities are recorded for evidence and so that trends and patterns can be analysed to help implement corrective actions.

1.2 The Policy aims to:

- Outline the expectations of system managers.
- Ensure a consistent approach to capturing and storing security incidents.
- Introduce a more security aware culture
- Outline roles & responsibilities
- Enhance Communications

2 Scope

2.1 The policy applies to all IT systems that connect to the core QMUL network including third party QMUL systems/services.

3 Policy Detail

3.1 QMUL systems shall produce and store system (audit) logs of user activities, system errors and information security events for an agreed period as defined in the Records Retention Schedule to assist in future investigations and for access control monitoring.

3.2 Audit logs must include:

- User IDs
- Dates, times, and details of key events, e.g. log-on, log-off, task, job, action
- Workstation identity or location where possible
- any network addresses available, especially IP or MAC addresses

3.3 Measures must be in place to protect facilities that log information and the information itself against tampering and unauthorised access.

3.4 When implementing the Auditing facility, the following must be taken into account;

- The risk of exceeding the storage capacity of the log file media,
- Failure of events being recorded or over-writing of past-recorded events.

3.5 The clocks of all relevant information-processing systems must be synchronised with an accurate time source to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.

3.6 Audit logs shall be reviewed periodically and corrective measures taken where necessary.
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 Roles & Responsibility

5.1 The Risk and Governance Manager will be responsible for initiating the review cycle for the document owner to carry out the review. The document owner will assess and incorporate appropriate comments/feedback received.

5.2 Once the document has been updated, the Risk and Governance Manager will request approval from the appropriate approval body. All approved documents are to be stored in a central repository and uploaded to the web where applicable.

6 Monitoring

6.1 It is mandatory to comply with this policy. Where non-compliance is identified, ITS will take appropriate action.

6.2 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.

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

7 Exceptions

7.1 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.

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

8 References

SOP DG22 – Maintenance of Security Logs Standard Operating Procedures
QMUL Records Retention Policy and Schedule
## Appendix A

### 9.1 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL’s systems.</td>
</tr>
<tr>
<td>ITLT</td>
<td>IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.</td>
</tr>
<tr>
<td>ITSB</td>
<td>IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.</td>
</tr>
</tbody>
</table>