IT Services Policy/Policy Document

DG08 Implementing IT Systems

Prepared by: <Shelim Miah>
Version: 2.2
Effective Date: 02/02/2023  Review Date: 02/02/2024

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

Policy Owner:
Name/Position  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>Saul Freeman</td>
<td>23/04/2010</td>
</tr>
<tr>
<td>1</td>
<td>Annual Review – No Change</td>
<td>David Nye</td>
<td>15/04/2014</td>
</tr>
<tr>
<td>1.1</td>
<td>Paragraph 14 added</td>
<td>Ian Douglas</td>
<td>28/11/2014</td>
</tr>
<tr>
<td>1.2</td>
<td>Additional Clauses added</td>
<td>Ian Douglas</td>
<td>29/05/2015</td>
</tr>
<tr>
<td>1.3</td>
<td>Review</td>
<td>D.Nye</td>
<td>05/10/2018</td>
</tr>
<tr>
<td>1.4</td>
<td>Review</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>16/12/2021</td>
</tr>
<tr>
<td>2.2</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>02/02/2023</td>
</tr>
</tbody>
</table>

Authorisation:
Name / Position  IT Lead Team
Signature        IT lead Team
Date             02/02/2023
Contents

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

1.1. The commissioning of a new IT system/s and major revisions/iterations of existing systems must be assessed, planned and managed in accordance with Queen Mary University of London (QM or QMUL) policy and are in line with industry best practice.

1.2. The Policy aims to:
   - Outline the expectations of those implementing or carrying out changes to IT systems
   - Ensure the security and protection of QM data
   - Implement controls to safeguard against adverse effects
   - Outline roles & responsibilities
   - Enhance Communications

2. Scope

2.1. This policy applies to anyone, including third parties, implementing QM ITS systems or making any changes, revisions or updates to existing QM systems.

3. Policy Detail

3.1. All new IT services and systems, and changes to existing IT services and systems are triggered only by an approved request for change brought forward by an authorised QM member of staff.

3.2. Any Project that includes the implementation or release of an IT service/system as part of the project delivery must adhere to this policy and follow the release, transition and change process.

3.3. The business need and business impact of changes must be clearly documented and communicated so that all stakeholders are aware and understand the impact.

3.4. Stakeholders impacted by a change must be given the opportunity to thoroughly analyse the change before implementing.

3.5. Changes must not be made to the production systems without the approval of the IT and user representatives responsible for the service.

3.6. Non-IT business units are not to implement changes that affect IT services without proper IT notification and approval through standardised procedures.

3.7. All requests for new IT systems and major changes must provide a documented service design document (SDD) identifying the value and warranty of the service, including a comprehensive risk analysis against a standardised set of criteria.

3.8. IT Security must be given the opportunity to perform a Security Risk Assessment at the design phase of any new IT Service and/or System. Before any new systems are introduced, a risk assessment process will be carried out which will include an assessment of the legal obligations that may arise from the use of the system. These legal obligations will be documented and a named system controller/owner, with responsibility for updating that information, will be identified.

3.9. All service design specifications must include a service support model and architectural design.
3.10. All changes must be evaluated by the relevant QM IT change control body and must follow an agreed escalation process for handling decision and conflicts.

3.11. All new services targeted for production will be subject to a standard and formalised service transition process that provides criteria that must be met before the service can be transitioned into production.

3.12. Where possible, all releases are to be tested prior to production implementation and post-production implementation.

3.13. All releases must utilise a standard set of test processes and tools for IT applications and infrastructure changes.

3.14. All testing strategies shall be based on business risks to QM not just technical risks.

3.15. Where required, Testware (environment settings, code, test data, transaction scenarios, test tool scripts and results data) are to be archived and maintained as application and track release baselines.

3.16. Unused Plugins, themes, sample code, modules, functions etc. must be disabled and/or removed from IT Systems prior to them being used for production purposes or made accessible from the Internet.

3.17. Using live data for testing purposes is considered bad practice. QM does not permit testing using live data as it’s use for testing purposes would not be compliant with GDPR.

3.18. Dummy data should be used where possible, if this is not possible then the testing environment must have the same security controls in place as a production environment.

3.19. Personal identifiable information must be avoided in live data for testing. If there are exceptions to this, please contact the Information Security Team.

3.20. As part of the release and Change plan a back out or roll back strategy is to be included or documented why this cannot be achieved.

3.21. All new and revised IT systems are to be documented and added to the relevant QM configuration management database. Standardised methods must be used for the efficient and prompt handling and recording of all changes. With the overall aim of minimising risk to the service and business.

3.22. Access to QM configuration management databases must be limited to authorised QMUL staff.

3.23. All production releases of IT systems must be signed off against a standardised set of service acceptance criteria before exiting Early Life Support.

3.24. All relevant information regarding new or changed services shall be available to all necessary QM IT staff.

3.25. Servers that host core infrastructure services. E.g. Domain Controllers, DNS etc. must not be used for other purposes such as hosting business applications.

3.26. Servers must not host multiple applications that have different data confidentiality classifications.

3.27. Where a system hosts data of different confidentiality classifications then the security level must be set for the most sensitive data held.

3.28. The Head of Service is responsible for creating an appropriate baseline configuration.

3.29. All systems must be configured to meet a defined baseline that includes security configuration, mandatory agents (e.g. Anti-Virus, CMDB reporting etc.)
3.30. Every information system must have a designated system controller/owner who is ultimately accountable for that system. The accountability for ensuring the protection of information systems and ensuring that specific security processes are carried out shall lie with the controller/owner although the day to day responsibilities may be delegated.

4. Process and Procedures

5.1 The associated processes and guidance documents can be found by visiting the ITS webpage.

5. Roles & Responsibilities

5.1. The Risk and Governance Manager will be responsible for initiating the review cycle for the policy, process document owner to carry out the review. The Document owner will assess and incorporate any comments or feedback received.

5.2. Once the document has been updated, the Risk and Governance Manager will take the document to the appropriate board for approval. All approved documentation are to be stored in a central repository and uploaded to the web where applicable.

6. Monitoring

6.1. It is mandatory for anyone including third party suppliers who are responsible for implementing, changing or upgrading QM ITS systems/services to comply with this IT Policy and any associated procedure. Where non-compliance is identified, ITS will take appropriate action, which may result in escalation to senior management for action to be taken.

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. 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.

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 DG25 – Configuration Management & Change Control
9. Appendix A

9.1. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDD</td>
<td>The Service Design Document (SDD) is the document that provide context around a Service or IT system. Essentially providing the who, what, where, when, and why of a new or changed IT Service</td>
</tr>
<tr>
<td>Acceptance Criteria</td>
<td>Acceptance Criteria are conditions which an IT System, software or application must satisfy to be accepted by a user or customer</td>
</tr>
<tr>
<td>Roll Back/Back out plan</td>
<td>A Plan or procedure that specifies the required steps and or actions to restore a system to its original or earlier state, in the event of failed or aborted implementation</td>
</tr>
<tr>
<td>Service Support Model</td>
<td>Support processes necessary to ensure service quality. These processes manage problems and changes in the IT Infrastructure</td>
</tr>
</tbody>
</table>