IT Services Policy

DG25 – Configuration Management and Change Control

Prepared by: < Shelim Miah>
Version: 2.2
**Effective Date:** 02/02/2023  
**Status:** 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>1.11</td>
<td>Initial version.</td>
<td>William Mordaunt</td>
<td>12/05/2010</td>
</tr>
<tr>
<td>1.2</td>
<td>Annual Review – No change</td>
<td>Alan Hardy</td>
<td>14/07/2014</td>
</tr>
<tr>
<td>1.3</td>
<td>Annual Review – Some clarifications made and updated to closer alignment with ITIL V3 - 2011</td>
<td>Alan Hardy</td>
<td>18/09/2015</td>
</tr>
<tr>
<td>1.4</td>
<td>Review</td>
<td>David Nye</td>
<td>17/01/2018</td>
</tr>
<tr>
<td>2.0</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>28/05/2018</td>
</tr>
<tr>
<td>2.1</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>08/12/2021</td>
</tr>
<tr>
<td>2.2</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>02/02/2023</td>
</tr>
</tbody>
</table>

**Authorisation:**

<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>02.02.2023</td>
</tr>
</tbody>
</table>
# CONTENTS

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

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

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

   CONFIGURATION MANAGEMENT ............................................. 4
   CHANGE CONTROL ................................................................. 5

4 PROCESS AND PROCEDURES ................................................. 7

5 ROLES & RESPONSIBILITY ...................................................... 7

6 MONITORING ......................................................................... 7

7 EXCEPTIONS ........................................................................... 7

8 REFERENCES ........................................................................... 7

9 APPENDIX A – DEFINITIONS ................................................. 8

10 APPENDIX B - CHANGE TYPES ............................................ 9
1 Policy Statement

1.1 This Policy ensures that IT assets are logged, configured, and managed accordingly. This includes assets such as servers, datacentres, desktops etc. form the infrastructure that provides IT services to both staff and students across Queen Mary University of London (QM or QMUL).

1.2 Any revisions/iterations to systems, configuration or assets; must be assessed, planned, tested and managed to minimise disruptions to IT services.

1.3 The Policy aims to:
   - Outline the expectations of staff making changes to IT assets.
   - 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 all IT Services assets such as; network switches, desktops, servers etc and any Change to QM’s production / live environments managed by IT Services (ITS).

3 Policy Detail

Configuration Management

3.1 A repository of IT assets configuration items (CIs) must be established and maintained in the Service Management Tool (ITSM) for Central IT Services.

3.2 The repository/database also known as the Configuration Management Database, or CMDB for short, must include items throughout its lifecycle such as; servers, network devices and desktops.

3.3 Details or attributes of each CI also known as a Configuration Record are to be captured and maintained in the CMDB.

3.4 Configuration Records must be updated after changes are made to Cis in the production environment.

3.5 All CIs must have a status assigned that clearly marks what stage of the CI lifecycle that each CI is at. A status might typically be for example ‘in stock’, ‘awaiting build’, ‘awaiting installation’ or ‘installed’

3.6 Where possible the status, owner and location of the CI should also be captured in the CI record.

3.7 Each CI must have its own unique reference number that will help identify the CI record it refers to in the QMUL IT CMDB and where possible each CI is to be labelled Property of QMUL or QM” asset tag label with a unique reference number. Leased hardware will carry either a vendor’s
asset tag or one assigned by QM but without the “Property of QMUL or QM” wording where possible.

3.8 A Service Configuration Model must be developed and maintained by the Service Management team, to define the relationships and dependencies between CIs.

3.9 The QM IT CMDB must be audited periodically to ensure its accuracy and to monitor the efficiency and effectiveness of the Service Asset & Configuration Management (SACM) processes.

**Change Control**

3.10 A record of all changes to central production IT systems, must be captured, logged and maintained in the ITSM. This includes CI items that are part of or support these IT systems.

3.11 Formal change management procedures, including a method of categorisation based upon type, risk and urgency / severity levels.

3.12 Each change record must detail the proposed change ensuring that sufficient information is provided to enable a Change Assessor (Change Manager) to understand the need for the change, the impact on the business and any risks including mitigations associated to the change.

3.13 Before a Change is implemented, an impact and resource assessment must be carried out to consider:

- Impact the change will have on the Customer's business operations
- Effect on the infrastructure and service
- Impact on other services that run on the same infrastructure
- Impact of not implementing the change
- Resource considerations
- Impact on non-IT infrastructure e.g. helpdesk
- Current Change Schedule and Projected Service Outages
- Impact on other Service Management areas including continuity plans

3.14 Each change record is to be grouped, assessed, and approved based on its own merit i.e.

a) Standard – Changes of low risk to service and frequently occurring
b) Non-standard – do not frequently occur but may or may not impact services
c) Emergency change – Urgent fix to help get the service back up or prevent a service outage

3.15 Where complex business wide changes are proposed, these should be reviewed and assessed by a panel of experts (Change Advisory Board) who are able to advise and guide in the best way the change is to be implemented.

3.16 A formal Emergency change procedure must be in place for urgent changes to rectify a problem in an IT service that has a high negative impact on the business.
3.17 Each Change is to be tested and the outcome verified to ensure the expected outcome is achieved. Where the expected outcome is not achieved a process of rolling back to restore the system to its previous working state must be presented before any change is allowed to proceed.

3.18 Timescales must be agreed for all changes – based upon business need, budget and IT capability, including skills and resource availability of both IT staff and business staff (where necessary) for User Acceptance Testing.

3.19 As part of the process, customers and those who will be impacted by the change must be kept informed and updated throughout.

3.20 Changes or releases of significant impact need to be scheduled where possible to occur during a regular maintenance window in order to minimise impact on the service.

3.21 Any change that does not achieve the desired outcome or has an unexpected impact is known as a failed change. Failed Changes that cause impact to services beyond the allocated time (change Window) must be reviewed as part of a Post Implementation Review (PIR) to understand what went wrong and how, so that lessons can be learnt and incorporated into the change process.

3.22 During business critical periods such as Clearing and Enrolment, a freeze on proposed changes is to be assessed and a change schedule established listing the frozen services and freeze periods to prevent any adverse impact to critical activities during these periods.
4 Process and Procedures

4.1 The associated processes and guidance documents can be found by visiting the [ITS webpage](http://example.com), 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 All IT assets held under the control of IT Services must comply with the policy and any suspected unauthorised change must be reported to the Change Manager. 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 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 DG00 – Review and Update of Policies & Standard Operating Procedures
## 9 Appendix A – Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>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</td>
</tr>
<tr>
<td>Procedural Document</td>
<td>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.</td>
</tr>
<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 services.</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>PIR</td>
<td>Post Implementation Review – a review that takes place after a failed change to identify what went wrong, how and why.</td>
</tr>
<tr>
<td>Failed Change</td>
<td>A Change that exceeds the allotted time to complete and or does not provide the expected outcome (benefit) or has adverse impacts on the service</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database- contains the record of assets in IT Services</td>
</tr>
<tr>
<td>CI</td>
<td>Configuration Item, the service asset managed by IT, such as laptop, desktop, Network Switch, Application</td>
</tr>
<tr>
<td>CI record</td>
<td>A record in the CMDB that describes the attributes of a CI</td>
</tr>
<tr>
<td>Change window</td>
<td>Allocated time for a change to take place, during this time the system is agreed to be offline whilst the change is carried out.</td>
</tr>
<tr>
<td>Change Advisory Board</td>
<td>Change Advisory Board (CAB) – group of people who convene to discuss and approve changes.</td>
</tr>
<tr>
<td>Change Manager</td>
<td>Person responsible for change management and includes deputy</td>
</tr>
<tr>
<td>ITSM</td>
<td>IT Service Management - ITSM refers to the entirety of activities – directed by policies, organised and structured in processes and supporting procedures – that are performed by an organisation or part of an organisation to plan, deliver, operate and control IT services offered to customers.</td>
</tr>
</tbody>
</table>
## Appendix B - Change Types

The table below gives examples of changes described in this procedure. It is worth noting that **ALL** changes are subject to the change Management process.

<table>
<thead>
<tr>
<th>Standard Changes</th>
<th>Non-standard Changes (Normal Changes)</th>
<th>Emergency Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Standard Change is a pre-approved, relatively common, well known, documented, low risk Change. The change activity normally happens frequently and would not normally require any scheduling or communication beyond informing a user or small group. As such, it is quite common for a Standard Change (SC) to have previously been a Non-Standard Change (NSC) which has been approved by the appropriate Change Authority to become an SC and CAB notified. Standard Changes will be often implemented after being requested via the Request Fulfilment Process some of which might have been directly recorded and passed for action by the Service Desk.</td>
<td>A Non-Standard Change (Normal Change) is a change that is neither an Emergency Change nor a Standard Change. Normal changes follow the defined steps of the change management process. Simply put, an NSC is actually defined by what it is not. Since it is not a standard change nor an emergency change, it is simply every other change and must be authorised. An NSC requires additional information to Standard Changes.</td>
<td>The Emergency change procedure is reserved for changes intended to repair an error in an IT service that is negatively impacting the business to a high degree. Emergency changes should be designed carefully and, if possible, tested before use or the impact of the emergency change may be greater than the original incident. Emergency changes may document some details retrospectively. The number of emergency changes proposed should be kept to an absolute minimum, because they are generally more disruptive and prone to failure. All changes likely to be required should, in general, be foreseen and planned, bearing in mind the availability of resources to build and test the change. Nevertheless, occasions will occur when emergency changes are essential and so procedures should be devised to deal with them quickly, without sacrificing normal management controls.</td>
</tr>
</tbody>
</table>