IT Services Policy

DG06 – IT Incident (Malfunction) Reporting Policy

Previously Known as: IT Malfunction Reporting SOP
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>William Mordaunt</td>
<td>19/04/2010</td>
</tr>
<tr>
<td>2.0</td>
<td>Transferred onto a Policy Template</td>
<td>Shelim Miah</td>
<td>22/03/2016</td>
</tr>
<tr>
<td>2.0</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>10/07/2018</td>
</tr>
<tr>
<td>2.1</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>10/12/2021</td>
</tr>
<tr>
<td>2.3</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 & RESPONSIBILITY ....................................................................................................... 6
6 MONITORING ............................................................................................................................. 6
7 EXCEPTIONS .............................................................................................................................. 6
8 REFERENCES ............................................................................................................................... 6
9 APPENDIX A – DEFINITIONS .................................................................................................. 7
1 Policy Statement

1.1 This policy ensures that IT service malfunctions such as; faults, incidents, problems and issues are reported to IT services to be investigated and fixed in a timely manner. This will help in reducing downtime and impact on IT services.

1.2 The Policy aims to:

- Outline the expectations of all users of IT Services in reporting IT incidents.
- Outline the expectations of staff managing IT Services and systems.
- Ensure a consistent and central repository is used for reporting IT incidents.
- Outline roles & responsibilities
- Enhance Communications

2 Scope

2.1 The policy applies to all QM IT Services and system administrators and users of those services. Individuals, groups and organisations that work with QM and or provide services to QM must align with the policy to ensure that QM users are able to report incidents and have these resolved as soon as practicable.

3 Policy Detail

3.1 IT Service and system incidents must be logged and dealt with in the appropriate way to restore services and enable users to continue working with minimal disruption.

3.2 All reported incidents must be captured in a tool such as an IT Service Management Tool (ITSM) and allocated a unique reference number.

3.3 Response times and categories must be set to provide a structured approach to prioritising, fixing and reporting on incidents.

3.4 Individuals, Groups, Depts, Schools or Organisations within QM, responsible for providing services for users, must be prepared to receive, log and deal with incident reports relating to those services.

3.5 They must provide information to users about what level of support they can expect, the services that are offered, and how to contact the IT Service Desk to report and obtain advice on the services provided.

3.6 Users that detect or experience an incident must report this to the appropriate IT Service Desk using the documented or advertised method e.g. telephone, e-mail, Chat or via the self-service portal.

3.7 The IT Service Desk will attempt to resolve the incident at the time of reporting. If the incident cannot be immediately resolved, then users shall be advised of the reference number relating to the incident and ensuring the user is kept updated on the progress of the incident.

3.8 Where the IT Service Desk is unable to resolve a reported incident, the IT Service Desk will triage the incident to the team best suited to deal with the issue.
3.9 IT Service Desk or other IT Services staff must notify appropriate users when a reported incident has been resolved. In the event that the resolution of an incident takes an extended period, then periodic updates on the progress will be provided either via the ITS Status page or direct to the appropriate user depending on the scope and scale of the incident.

3.10 Staff working on an incident must log the actions taken to resolve an incident. This must include the outcome of any fault-finding investigation and any solution/workaround implemented, to the extent that a team member, from a different team would be able to understand:

- The cause of the incident,
- What actions were carried out to identify and remedy the incident,
- Who carried them out,
- For what reason, and the outcome of those actions.

3.11 Where the cause of an incident is unknown, requires further investigation or there are multiple instances of the same issue, this shall be logged in the ITSM as a problem ticket with a separate reference number.

3.12 Any temporary solution (workaround) in place whilst further investigations are taking place shall be recorded in a known error database, this will allow any similar faults to be fixed by the IT Service Desk on first contact, until a permanent solution is deployed.

3.13 The Service Desk manager or Service manager shall regularly review reported incidents to determine that incidents have been satisfactorily resolved and solutions are being progressed or if an investigation into an underlying issue is required (problem ticket).

3.14 The Service Desk manager or Service manager shall review corrective measures to ensure that information security controls have not been compromised and that action taken is fully authorised and not in breach of any relevant policy.

3.15 Where Faults or issues have not been satisfactorily resolved, an appeal or escalation process must be in place to allow the incident to be reviewed in its entirety (to include the handling of the incident).
4 Process and Procedures
4.1 The associated processes and guidance documents can be found by visiting the ITS webpage.

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 for anyone using and administering Services to QM 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 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 DG06 – IT Malfunction Reporting Policy
## 9 Appendix A – Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident</td>
<td>An unplanned interruption to an IT Service or reduction in the quality of an IT service. A <strong>Failure</strong> of a hardware that has not yet <strong>affected</strong> service is also an incident — for example, <strong>failure</strong> of one disk from a mirror set.</td>
</tr>
<tr>
<td>Problem</td>
<td>The underlying issue/root cause of one or more incidents.</td>
</tr>
<tr>
<td>ITSM</td>
<td>IT Service Management Tool, that allows IT Services to design, plan, deliver, operate and control information technology (IT) services offered to customers</td>
</tr>
<tr>
<td>Work Around</td>
<td>A temporary solution that restores the service or offers an alternative way of getting the user working/access to services until the fault is fixed</td>
</tr>
<tr>
<td>Known Error Database</td>
<td>A <strong>database</strong> that describes all of the known issues within the overall systems. It describes the situations in which these issues appear, and when possible, it offers a workaround that will get the user around the <strong>problem</strong> and back to productive work.</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 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>