IT Services Policy/Policy Document

DG26 – System Backup and Recovery

Prepared by: <Shelim Miah>
Version: 2.3
**Review Date:** Aug 2020  
**Next Review:** Aug 2022

**Reviewers:**  
Kathy Whelan, IT Service Desk Manager  
David Pick, Network Security  
Thomas King, AD for Research  
Henrik Brogger, Head of Service Delivery  
Martin Evans, Head of Data Centre Services  
Terry Holland, Servers & Storage Manager  
Jason Bunning, Head of Application Delivery  
Ed Webb, Head of Application Solutions

**Policy Owner:**  
Name/Position: Rachel Bence – CIO IT Services

**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>1</td>
<td>Annual Review – No Change</td>
<td>Steve Wicks</td>
<td>08/07/2014</td>
</tr>
<tr>
<td>1.1</td>
<td>Added a sentence in step 2</td>
<td>Ian Douglas</td>
<td>29/05/2015</td>
</tr>
<tr>
<td>2.0</td>
<td>Annual review Template change</td>
<td>Shelim Miah</td>
<td>26/10/2016</td>
</tr>
<tr>
<td>2.1</td>
<td>Review</td>
<td>Shelim</td>
<td>22/01/2017</td>
</tr>
<tr>
<td>2.2</td>
<td>Review with AD Student &amp; Staff Services</td>
<td>Shelim Miah</td>
<td>13/03/2017</td>
</tr>
<tr>
<td>2.3</td>
<td>Update to exception 6 and removed section on processes, added 3.11,3.12,3.13</td>
<td>Shelim Miah</td>
<td>24/08/2020</td>
</tr>
</tbody>
</table>

**Authorisation:**

<table>
<thead>
<tr>
<th>Name / Position</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rachel Bence – CIO IT Services</td>
<td></td>
</tr>
</tbody>
</table>

**Signature**  
Rachel Bence

**Date**  
Aug 2020
Contents

1 POLICY STATEMENT ...........................................................................................................4
2 SCOPE ..................................................................................................................................4
3 POLICY DETAIL ..................................................................................................................4
4 ROLES & RESPONSIBILITIES ..........................................................................................5
5 MONITORING .....................................................................................................................5
6 EXCEPTIONS .......................................................................................................................5
7 RELATED DOCUMENTS .....................................................................................................6
8 REFERENCES .......................................................................................................................6
9 APPENDIX A – DEFINITIONS ..........................................................................................6
10 APPENDIX B – BACKUP EXCLUSION LIST ....................................................................7
11 APPENDIX C – BACKUP SCHEDULE/PLAN ....................................................................7
1 Policy Statement

1.1 This policy ensures that QMUL IT systems that are identified as requiring backup for example; server settings, operating systems, third party products and associated user data is backed-up and a process is available to recover server/user data as required/requested. It also ensures that the server and its associated user data is recoverable with minimal data loss in the event of system failure or corruption. This is also a prerequisite for disaster recovery and business continuity purposes.

1.2 The policy aims to:

- Outline the expectations of IT staff and stakeholders
- Ensure the security and protection of QMUL data
- Implement controls to recover from system failures
- Outline roles & responsibilities
- Enhance communications

2 Scope

2.1 This policy is applicable to all identified systems requiring backup run by IT Services for QMUL and maybe applicable to all IT Staff who manage or are responsible for running local systems.

3 Policy Detail

3.1 All identified systems under the control of QMUL IT are backed up and any exclusions system/server/user data areas are identified in the Appendix B. The level of data backup must be defined for each system (e.g. entire system, data partitions – which ones, etc.).

3.2 Each system/server/user data must be recoverable in the event of a failure or request, with indicative timescales and guidelines on how and when recovery will be completed.

3.3 A backup plan/schedule must exist that describes how the backup is completed see Appendix C.

3.4 The schedule and types of backups (e.g. full, differential or incremental) and frequency (e.g. daily or weekly) must reflect the business requirements of the organisation/department, the security requirements of the information involved, and the impact of the data loss to the continued operation of the organisation.

3.5 Business critical systems must have at least 3 months of backup information retained and be able to restore to any day within that time.

3.6 The status of back up jobs must be checked on a daily basis, any failed backup must be investigated where necessary and re-run as soon as possible.

3.7 Backups must be kept as far away as possible from the primary data preferably offsite.

3.8 Backup media should be encrypted at rest and must be kept in the same or greater physical and environmental conditions as the primary data.
3.9 Restoration procedures must be regularly tested at least once every 6 months to ensure that they are effective and that they can be completed within required timescales. Records of the testing must be kept.

3.10 Any associated documentation paper or electronic to enable the successful restoration must be kept secure and made available in the event of a partial or complete systems failure.

3.11 Back ups that are stored must align with the Records Retention Policy and Retention Schedule. Any Backup data held that conflicts with GDPR must be removed in accordance to the regulations.

3.12 Where Backup media such as tapes, CDs, removable hard drives etc. are no longer usable or required, they must be securely destroyed or blanked before disposal as per DG10 Disposal of IT Equipment and DG16 Disposal of Information.

3.13 The backup and recovery of cloud storage is the responsibility of the 3rd party supplier, their backup and recovery policy should be reviewed before agreeing to use their service to ensure that data is recoverable.

4 Roles & Responsibilities

4.1 System managers are responsible for developing and implementing backup procedures for the systems they manage.

4.2 They are also responsible for ensuring that backups are carried out, tested and recorded.

5 Monitoring

5.1 Compliance with the policies and procedures laid down in this document will be monitored by IT Services, together with independent reviews by both Internal and External Auditors on a periodic basis.

5.2 Where non-compliance is identified and the corrective actions have not been implemented, ITS will take appropriate action, which may result in escalation to senior management.

6 Exceptions

6.1 Where an exception to this policy is required, the matter should firstly be referred to the ITLT to assess the exception.

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

6.3 Where compliance to this policy is not possible due to technical, financial or regulative reasons, an exception must be raised to the appropriate group for approval so that it can be recorded as being granted exception to this policy.
7 Related Documents

7.1 Changes to this Policy will impact the:

• Backup Strategy
• Back up procedures
• Disaster Recovery plans

8 References

• SOP DG26 Systems Backup and Recovery Policy
• Retention Policy - http://www.arcs.qmul.ac.uk/media/arcs/policyzone/Records-Retention-Policy-2010-v01.2.pdf

9 Appendix A – 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>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>
<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>User Data</td>
<td>Files documents in MS Office; database files used for day to day operational activity</td>
</tr>
<tr>
<td>Server Data</td>
<td>Typically includes operating systems, configuration setting, and third party layered products for example ORACLE; MS SQL server.</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>
<tr>
<td>System manager</td>
<td>A person whose responsibility it is to maintain a system, ensure it is operational and rectify any bugs or issues.</td>
</tr>
</tbody>
</table>
Backup Media

Backup Media
A tape, CD, external hard drive or USB stick, essentially any piece of hardware that can be used to store data.

Recovery/Restore
Recovery/Restore
The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

Disaster Recovery Plan
Disaster Recovery Plan
The planning and implementation of a procedures to help recover from a total system failure.

Policy
Policy
A set of rules or framework that outlines the boundaries in which to operate.

Process
Process
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.

SOP
SOP
Standard Operating Procedure is a documented high level step-by-step sequence of Operational activities for adhering to policies that can be replicated across several departments and team.

Procedural Doc
Procedural Doc
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.

10 Appendix B – Backup Exclusion List

1. UAT systems
2. Dev Systems

11 Appendix C – Backup Schedule/Plan

The Backup schedule/plan must consist of the following:

How backs ups are to be carried out i.e. procedure for back ups

- When and how frequent backs are to be carried out i.e. every night
- Who is to be tasked with carrying out the back up
- What data is to be backed up
- What media is to be used to store the back up
- Frequency of testing and recording of the results
- Archiving of backup data and must be aligned to the retention policy/schedule
- How data is to be restored and what process are users to use to request this.
- Records of backup of when backup copies are taken and what has been backed up.