IT Services Policy/Policy Document

DG26 – System Backup and Recovery

Prepared by: < Shelim Miah>

Version: 2.2

Effective Date:	**17/03/17**	Review Date:	**17/03/18**

Reviewers:	**Steve Wicks, Servers & Storage Manager** **David Boakes, Assistant Director Student & Staff Services** **Ian Douglas, Head of Information Security** **Henrick Brogger, Head of Student & Staff Support Services** **Amit Patel, Head of Service Management** **Martin Evans, Head of Data Centre Services** **David Cooper, Interim Head of Technical Applications**
Policy Owner:	
Name/Position	Katie Friis, Interim Deputy Director of IT Services

Revision History

Version	Description	Author	Date
1	Initial version.	William Mordaunt	19/04/2010
1	Annual Review –No Change	Steve Wicks	08/07/2014
1.1	Added a sentence in step 2	Ian Douglas	29/05/2015
2.0	Annual review Template change	Shelim Miah	26/10/2016
2.1	Review	Shelim	22/01/2017
2.2	Review with AD Student & Staff Services	Shelim Miah	13/03/2017

Authorisation:	
Name / Position	**Katie Friis, Interim Deputy Director of IT Services**
Signature	**Katie Friis**
Date	**TBD**

Contents

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 must be kept in the same 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.

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 Process and Procedures

5.1 The associated processes and guidance documents can be found by visiting the IT webpage, some pages maybe restricted to IT Staff only.

6 Monitoring

6.1 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 Audit on a periodic basis.

6.2 The Assistant Director of Student & Staff Services, in conjunction with the Risk & Governance Manager, is responsible for the monitoring, revision and updating of this document.

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 IT Lead Team (ITLT) for a decision via the Assistant Director for Student & Staff Services.

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

7.3 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.

8 Related Documents

8.1 Changes to this Policy will impact the:

- Backup Strategy
- Back up procedures
- Disaster Recovery plans

9 References

- SOP DG26 Systems Backup and Recovery Policy

10 Appendix A – Definitions

Term	Meaning
QMUL	Queen Mary University of London
JANET	Joint Academic Network, the organisation the provides QMUL with Internet connectivity
ITS	IT Services
BYOD	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.
User	A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL's systems.
User Data	Files documents in MS Office; database files used for day to day operational activity
Server Data	Typically includes operating systems, configuration setting, and third party layered products for example ORACLE; MS SQL server.
ITLT	IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.
ITSB	IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.
System manager	A person whose responsibility it is to maintain a system, ensure it is operational and rectify any bugs or issues.
Backup	The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
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	The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.
Disaster Recovery Plan	The planning and implementation of a procedures to help recover from a total system failure.
Policy	A set of rules or framework that outlines the boundaries in which to operate.
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	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	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.

11 Appendix B – Backup Exclusion List

1. UAT systems
2. Dev Systems

12 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.