



IT Services Procedure

ITP04 – System Backup and Recovery Procedure

Prepared by: < Devopam Dasgupta, GRC Manager >

Version: 3.1

Last Review:	04/08/2026	Next Review:	03/08/2026
Reviewers:	Ambrose Neville (Chief Information Security Officer) Devopam Dasgupta (Governance, Risk and Compliance Manager) Geoffrey Providence (AD – Enterprise Systems & Technology Enhanced Learning)		
Procedure Owner:			
Name/Position	Geoffrey Providence (AD – Enterprise Systems & Technology Enhanced Learning)		
Revision History			
Version	Description	Author	Date
1	Initial version.	William Mordaunt	19 th April 2010
1	Annual Review –No Change	Steve Wicks	8 th July 2014
1.1	Added a sentence in step 2	Ian Douglas	29 th May 2015
2.0	Annual review Template change	Shelim Miah	26 th October 2016
2.1	Review	Shelim	22 nd January 2017
2.2	Review with AD Student & Staff Services	Shelim Miah	13 th March 2017
2.3	Update to exception 6 and removed section on processes, added 3.11,3.12,3.13	Shelim Miah	24 th August 2020
2.4	Update Retention Schedule link	Shelim Miah	02 nd August 2021
2.5	Review	Shelim Miah	02 nd February 2023
2.6	Review	Cathie Jayakumar-Hazra	10 th October 2025
3.0	Converted into a Procedure as a part of ISMS update for ISO 27001 audit	Devopam Dasgupta	13 th November 2025
3.1	Periodic review – minor change to terminology as per the Policy Writing Guidance	Devopam Dasgupta	8 th April 2026

3.2	Periodic review – minor updates in the titles of Head of Information Security to Chief Information Security Officer, and Head – Hybrid Platforms to AD – Enterprise Systems & Technology Enhanced Learning		
Authorisation:			
Name / Position	Geoffrey Providence (AD – Enterprise Systems & Technology Enhanced Learning)		
Signature	Geoffrey Providence		
Date	04/08/2026		

Contents

1	INTRODUCTION	5
2	SCOPE	5
3	PROCEDURE DETAIL	5
4	ROLES & RESPONSIBILITIES	6
5	MONITORING	6
6	EXCEPTIONS	7
7	RELATED DOCUMENTS	7
8	REFERENCES	7
9	APPENDIX A – BACKUP EXCLUSION LIST	8
10	APPENDIX B – BACKUP SCHEDULE/PLAN	8

1 Introduction

This procedure ensures that Queen Mary University (QMUL) critical IT systems and data are appropriately backed up (for example, server settings, operating systems, third party products and associated user data) 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.

1.1 The procedure 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 procedure 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 Procedure 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 A. 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 B.
- 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 Backups that are stored must align with the IS21 ITS Backup Policy, 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 IS29 Resue and Disposal of IT Equipment and DG09 Information Classification.
- 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 out in this document must be monitored by the Information Security Team as directed by the Chief Information Security Officer, along 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.
- 5.3 The Governance Risk and Compliance Manager, in conjunction with AD - Enterprise Systems & Technology Enhanced Learning, and the Chief Information Security Officer, is responsible for the monitoring, revision and updating of this document.
- 5.4 The effectiveness of this document must be evaluated at Infosec Monthly Meetings as well as the annual management review with Senior Management.

6 Exceptions

- 6.1 Where compliance to this procedure 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 procedure.
- 6.2 Any exception to this policy must be documented with business reasoning and signed off by the University's Chief Information Officer and the Chief Information Security Officer before implementation.

7 Related Documents

- 7.1 Changes to this Procedure will impact the:
 - Backup Strategy
 - Back up procedures
 - Disaster Recovery plans

8 References

- IS21 ITS Backup Policy
- IS29 Resue and Disposal of IT Equipment
- DG09 Information Classification.
- Retention Policy

9 Appendix A – Backup Exclusion List

1. UAT systems
2. Dev Systems

10 Appendix B – Backup Schedule/Plan

The Backup schedule/plan must consist of the following:

- 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.