BACKUP MANAGEMENT POLICY (ISP016)

1. OVERVIEW AND PURPOSE

1.1. As a knowledge-based institution, University of Sussex holds much data and information system of great value, both in financial and impact of loss terms. The backing up of data and other files is an essential practice to insure against the loss of this valuable information.

1.2. The purpose of backing up is to allow the restoration of a system to a current or recent state in the event of system failure. Backup media is not intended to serve as a form of short- or long-term storage of information.

1.3. The purpose of this policy is to describe the University of Sussex data backup and recovery procedures and standards. This policy covers the data backup schedule, backup retention and data recovery.

1.4. This policy covers all systems managed by IT Services. Data held and managed locally in departments is excluded unless departments have entered into specific arrangements with IT.

1.5. Users are individually responsible for data held locally on their computer or any other device, and all critical data must be stored on the network drives or centrally managed cloud storage services provided.

1.6. The objectives of this policy are:

1.6.1. To describe the University of Sussex data backup and recovery procedures, protocols and standards.

1.6.2. To establish a limit on the length of time backups are maintained.

1.6.3. To encourage staff and researchers to distinguish between the purposes and practices of backing-up data versus retrieval or archive storage of data.

2. SCOPE

2.1. This policy applies to all use of University computing facilities including software, computers and/or networks, whether on-campus or via remote connections.

2.2. The policy covers the approach to data backup and recovery for systems on-campus in Brighton. Third party provided systems, including cloud-hosted, will require additional measures to be put in place.

2.3. IT Services are responsible for the backup and protection of data in systems fully managed by them on behalf of the University.

2.4. Where systems are not fully managed by IT Services, or an agreement has not reached specifically around backup, it is the responsibility of the Head of School or Professional Service to ensure data is adequately protected.

2.5. This policy does NOT cover data retention or compliance requirements.

3. RESPONSIBILITIES

3.1. Director of IT Services

3.1.1. Overall accountability of the implementation of this policy.

3.1.2. Ensure that the duties associated with this policy are resourced and carried out appropriately.

3.1.3. Periodically review the risks associated with data storage, backup and retention and ensure that appropriate mitigations are in place.

3.1.4. Ensure that all systems fully managed by IT Services have an adequate level of backup and data protection.

3.2. Head of Technical Operations

3.2.1. Ensure that the operational tasks associated with this policy are resourced and carried out appropriately.

3.2.2. Ensure that test recovery activities are carried out on a periodic basis.

3.2.3. Ensure that backup equipment and software is fit-for-purpose, operational and appropriately licensed and supported.

3.2.4. Agree and periodically review Service Level Agreements to ensure appropriate operation of the tasks associated with this policy.

3.2.5. Ensure that those systems fully managed by IT Services are adequately backed up and data protected.

3.3. IT Services Staff Members

3.3.1. Carry out backup and recovery tasks as required and in line with agreement Service Level Agreements.

3.3.2. Identify requirements for additional backups as they arise.

3.3.3. Ensure that any recovery activities result in a stable outcome.

3.4. University Officers, Heads of Schools (and the Dean of BSMS), Directors of Professional Services Divisions and Section Heads

3.4.1. Ensure that all information in their area is protected in conformance with this policy.

3.4.2. Make people in their area of responsibility aware of this policy.

3.4.3. For systems that are not fully managed by IT Services, or an agreement has not reached specifically around backup, it is the responsibility of the Head of School or Professional Service to ensure data is adequately protected.

3.5. Researchers and Assistants

3.5.1. Ensure that appropriate backup and recovery plans are in place and are conformant with this policy.

3.5.2. Ensure that any associated archival requirements are identified and addressed in line with University data retention policies.

3.5.3. In the event of a data loss incident, raise a support ticket with IT via the IT Service Management system as soon as possible to start the recovery process.

3.5.4. Report any Information Security incidents or risks to the Director of IT Services via an appropriate channel.

4. POLICY

4.1. It is the policy of the University of Sussex that all information it manages shall be appropriately secured to protect the institution from the impact of loss or irreparable damage to valued information.

4.2. Data backup is purely to allow the Institution to continue its activity after a data loss incident, by retrieving some or all of the data lost. All data should be backed up according to its value to the Institution, the cost of recreating the data, any financial costs or penalties which might be incurred because of data loss or corruption and the risk of data loss or corruption.

4.3. There are two key parameters that must be identified to ensure appropriate protection of any data or system:

4.3.1. Recovery Point Objective (RPO) - the maximum acceptable age (in minutes, hours or days) of backup which could be restored in the event of a data loss incident. This will determine the possible scale of data loss arising from the incident. For example, a set of hundreds of financial transactions into a system with an RPO of 24 hours could result in a large amount of re-keying or possibly even complete financial loss.

4.3.2. Recovery Time Objective (RTO) – the maximum time it would take to recover from the data loss incident. This will be affected by the type of media (disk, tape, etc.) used to backup the data and the volume of data being recovered. For example, a single 10TB data set could take a very long time to recover from tape, whereas a single 100KB file on disk make take seconds.

4.4. Data backup is not archiving (the practice of storing data which is no longer required for reference purposes only) and must not be used as a cheap substitute for appropriate archive management.

4.5. All backup systems and media must be physically located somewhere different (at least in another building) to the original data.

4.6. Any removal backup media (e.g. LTO tapes) will be withdrawn from the backup system and transferred to an appropriate place of safe storage; typically, this will be a fire safe.

4.7. Any backup solution will be tested fully at the point it is implemented, and thereafter at least annually to ensure that it is operational and can fulfil its objectives in the event of a data loss incident.

4.8. Data backup solutions should be reviewed at least every two years to ensure that they continue to meet the Institution's requirements and the solution is modified if appropriate.

4.9. Requests for recovery of data must be submitted to IT via the IT Service Management as soon as possible following a data loss incident. Upon receipt of the request, IT will start the recovery process as soon as possible, in line with agreed Service Levels.

4.10. Backups schedules are listed in Appendix One – Backup Schedule and represent the current operational requirements of the University. As such they are subject to change on occasion.

4.11. All tapes are transferred to a fire safe for off-line storage. The fire safe is in a different location to the data centre. Full backup tapes will be moved to the fire safe immediately. Incremental tapes will be moved at regular intervals.

4.12. Tapes will be recycled until up to 95% of manufacturers service window. In all cases tapes should be replaced before failure.

4.13. Disk backups are kept for two months before being overwritten.

4.14. Where third-parties are contracted to provide backup services, they should comply with this policy as a minimum expectation. Requirements to deviate outside of the minimum expectation should be discussed with IT Services and, if necessary, flagged as a risk.

5. LEGISLATION AND GOOD PRACTICE

Review / Contacts / References	
Policy title:	BACKUP MANAGEMENT POLICY (ISP016)
Date approved:	5th Sept 2019
Approving body:	Information Governance Committee
Last review date:	New policy
Revision history:	1.1
Next review date:	12 months from approval date
Related internal policies, procedures, guidance:	http://www.sussex.ac.uk/infosec/policies
Policy owner:	*IT Services*
Lead contact / author:	*Pete Collier, Assistant Director, Strategy and Architecture*

SUPPORTING DOCUMENTS

Data Protection policy and guidance -
http://www.sussex.ac.uk/ogs/policies/information/dpa/dataprotectionpolicy

Knowledge and Research Exchange policies - http://www.sussex.ac.uk/staff/research/rqi/rqi_information_and_support/rqi_strategy_policy/research-policies

Records Management Guidance - http://www.sussex.ac.uk/ogs/policies/information/recordsmanagementguidance

Appendix One – Backup Schedule

The current backup schedule is listed below. It is subject to change in accordance with operational requirements without re-approval of the Policy itself.

There are three general categories of backup to fit with generic University requirements:

Critical (RPO = 24 hours, retention 12 months)

- Clients backup to disk backup initially and then cloned to LTO tape
- Monthly full backup
- Following the Monthly backup, nightly level backups
- 12 months of backups retained

Standard (RPO = 24 hours, retention 6 months)

- Clients backup to disk backup initially and then cloned to LTO tape
- Monthly full backup
- Following the Monthly backup, nightly level backups
- 6 months of backups retained

Research + Large Volumes (RPO = 24 hours, retention 8 months)

- Clients backup directly to LTO tape
- Full backups every 4 months
- Nightly, weekly or monthly level incremental backups, as appropriate for the specific requirement
- 8 months of backup retained

This section last updated: July 2019