Data Backup Policy

Information Services

Centrally maintained University servers are scheduled to backup daily, with retention periods being dependent on data types.

1. Retention

Service	Retention period	Backup Location
University servers/ services	14 days	Cranfield Campus and replicated to the cloud
Test and development servers/services	14 days	Cranfield Campus only.
High Performance Computing	Temp and scratch areas are not backed up.	Not held.
File stores (personal and shared group drives)	User Recoverable Snapshots (Previous Versions) are taken every 4 hrs at 06:00, 10:00, 14:00… and held for 10 days. IS then provides further protection, recoverable via IT Service Desk: • 64 hourly backups (taken at 30 minutes past the hour) • 32 daily backups (taken at 19:00)	Cloud
CDS file store (personal and shared group areas)	User Recoverable Snapshots (Previous Versions) are taken 4 times a day and held for 10 days. IS then provides further protection, recoverable via IS Service Desk; • 31 daily backups (taken at 18:00)	Cloud
University databases including Finance, Human Resources and Registry services	7 days	Cranfield Campus and replicated to the cloud

Microsoft Office 365 (Email, OneDrive, SharePoint online)	1 year	Cloud

2. Archiving

Upon expiration of a user account any data stored within the personal file store or mailbox will be archived and available offline for maximum of 1 year.

If a permanent archive is required, then the Information Services Professional Service Unit (IS PSU) can transfer the data to DVD or similar media. However, authorisation must be obtained from the relevant Pro-Vice Chancellor of a School or Service Director of a Professional Services Unit. Once provided, the data will be the responsibility of the person making the request.

3. Local device storage

It is the responsibility of the data owner to ensure that any data temporarily stored on local PC hard disks is transferred to the network file store at the earliest opportunity. If using any removable media (CD/DVD or USB storage) then the Information Handling Procedures must be followed.

4. Business Continuity

Microsoft Azure public cloud services are used to store offsite copies of the University’s backups, for use in the event of disaster.

All cloud backups are transferred and stored encrypted for additional data protection.

Document control

Document title	Data Backup Policy
Originator name/document owner	Systems Manager
Professional Service Unit/Department	Information Services
Approval by and date	Director of Information Services; 01/10/2019
Date of last review and version number	September 2019 / V1.8
Date of next review	August 2020
Information categorisation	Confidential - Commercial

Document Review

Version	Amendment	By	Date
1.8	Minor change of wording for title of Section 3 and date/format changes	Information Security	September 2019