The Babraham Institute

BI-BICS-004 IT BACKUP AND RETENTION POLICY

Document reference			
Policy number:	BI-BICS-004		
Policy Owner:	Cass Flowers, CIO		
Date:	04 Aug 2022		
Version:	1.0		
Status:	Draft		
EIA number:	BI-BICS-EIA-004		
Review Period:	1 Year		
Last reviewed:	09 December 2022	Next review:	August 2023

Version control			
Date	Version	Status	Summary of Changes
04 Aug 2022	0.1	Draft	Wording draft
09 December 2022	1.0	Live	Final amendments following BEC comment and approval

Document approval			
Define the approval authorities for the document			
Document version	Document approved by	Position	Date
1.0	BEC	N/A	09 December 2022

Distribution		
Name or Group	Date of issue	Version
All staff and associates	12 December 2022	1.0

Associated policies, procedures and guidance
This policy should be read in conjunction with:
BI-BICS-001 IT Security & Usage Policy
BI-IM-003 Information Classification and Security Policy
BI-IM-002 Data Protection Policy
BI-KEC-001 Intellectual Property Policy
BI-HR-001 Code of Conduct
BI-COM-002 Use of Social Media & Related Online Platforms Policy
BI-HR-005 Disciplinary Policy
BI-HAS-003 Safeguarding Policy

Contents

1. Definitions

1.1. Group Data

"Group data"	Data typically owned and administered by group/department/facility heads and accessed by their group/department members.
"Group file share"	Network shares on Institute enterprise storage owned by group/department/facility heads. These shares are often accessible to group members or facility users for storing and collaborating on work. Commonly referred to as "N Drive" or "O Drive".
"ELN notebook"	Electronic Lab Notebooks stored within a group/department head's designated area in OneNote notebook files. These are stored in Microsoft 365 cloud-based services.
"Scientific cluster data"	Data from scientific analysis, experimentation, or facility use stored on the Institute's enterprise storage systems. Commonly referred to as "Isilon storage".

1.2. User Data

"User data"	Data typically created, owned and accessed by a single user.
"User file share"	An individual file share on Institute enterprise storage associated with a named user account. Commonly referred to as "M Drive".
"User mailbox"	Email mailbox associated with a user's domain account stored either on Institute email servers or Exchange Online within Microsoft 365 cloud-based services.
"User OneDrive"	The OneDrive service within Microsoft 365 cloud-based services (https://onedrive.live.com) associated with a named user account.

1.3. Other definitions

"Archive"	Long-term storage of data that will be rarely accessed.
"Default quota"	The maximum amount of data that can be stored by default, unless agreed otherwise.
"Device"	Physical computer hardware such as a laptop, desktop, mobile, tablet or a computer connected to scientific equipment.

"Employee"	Institute employees on Institute or Babraham Institute Enterprise Ltd (BIE) terms and conditions, Institute employees on BBSRC or other terms and conditions, and Research Fellows on Institute terms and conditions.
"Institute data"	Any electronic data belonging to the Institute. For example, emails, office documents, database data, financial data.
"Institute managed / owned device"	Any device that is configured or managed by BICS and connects to the main Babraham Institute network. This includes devices used by BRC Ltd. that are managed by BICS.
"IT service data"	Data owned and administered by BICS which is essential to run IT servers and services, including: • Virtual/physical server storage containing server data • Server and service configuration data • Network equipment configuration data.
"Named user account"	The individual account assigned to an employee and used to access Institute IT services. The username for this account often includes an individual's surname.
"Retention"	The length of time data is kept for, and therefore the period that a backup or archive of data can be restored back to.
"Shared mailbox"	Email mailbox associated with a group/shared email account stored either on Institute email servers or Exchange Online within Microsoft 365 cloud-based services.
"Snapshot"	A copy of data at a specific moment in time.
"Staff"	Employees and Babraham Institute registered PhD students.
"User"	Anyone accessing an Institute IT service.

2. Commitment statement

2.1. At the Babraham Institute our mission is to be an international leader in research focusing on basic cell and molecular biology with an emphasis on healthy ageing through the human lifecycle.

2.2. Babraham Institute Computing Service (BICS) is committed to providing an efficient, flexible, and secure service that will meet the changing needs of the science at the Institute, whilst working within the regulations, policies and requirements of the Institute, Janet, and the Cyber Essentials Scheme.

3. Purpose

3.1. The purpose of this policy is to provide a high-level outline of backup, retention and recovery measures in place to protect the integrity and availability of Institute data and services.

4. Scope

4.1. This policy applies to:

- Institute employees on Institute or Babraham Institute Enterprise Ltd (BIE) terms and conditions
- Institute employees on BBSRC or other terms and conditions
- BRC Ltd. employees
- Research Fellows on Institute terms and conditions
- Research Fellows (honorary)
- Honorary Members of Faculty
- Babraham Institute registered PhD students
- Visiting students
- Visiting researchers and workers, including consultants and secondees
- Workers provided by a third party / contractors
- Visitors
- Trustees

4.2. This policy applies to Institute data stored on:

- Institute enterprise storage, i.e. user/group file shares and scientific cluster data
- Institute archiving systems, e.g. Research Data Archiving Repository (RADAR)
- Institute servers providing IT services
- Microsoft 365 cloud-based services, e.g. Microsoft OneDrive, Teams, SharePoint Online, and Exchange Online.

4.3. **Institute data must be stored using the storage services detailed above (4.2) and not stored locally on Institute managed devices.**

5. Storage allocation

5.1. When new data storage areas are provisioned, they are allocated with default quotas.

5.2. Default quotas are provisioned as follows:

- 10GB for user file shares (M drive)
- 20GB for standard group file shares (N/O drive)
- 1TB for OneDrive storage
- 20GB for user mailboxes on the Institute email server.

5.3. Larger group shares, particularly those exceeding 1TB, are provisioned on the Scientific cluster data storage (Isilon) with allocations set based on group or facility requirements and provisioning managed on a “fair use” basis.

5.4. Increases to default quotas must first be discussed with the CIO having first ensured that all data stored is necessary. Any unnecessary data must be removed or archived (e.g. using

Research Data Archiving Repository (RADAR)). Increase requests are subject to capacity, availability, and fair use. Requests for large increases to storage space may require the purchase of additional storage equipment by the group/department.

6. Backup and retention of user/group data

6.1. User/group file shares and scientific cluster

6.1.1. User/group file share and scientific cluster backups are created daily and overwritten each day.

6.1.2. Snapshots for user and standard group file shares (i.e. M, N, O drive) are created daily and recoverable by users on a Windows system via 'Properties' > 'Previous Versions' of Files and Folders. Snapshots are retained for 28 days.

6.1.3. Due to storage limitations, snapshots are not enabled by default on the scientific cluster data. Data owners should discuss with BICS if this becomes a requirement.

6.2. Data archiving

6.2.1. Research Data Archiving Repository (RADAR) is a manual data archiving repository for unused/inactive research data requiring long retention due to funder requirements. It is available on request to all researchers.

6.2.2. All data for archiving must be appropriately organised to aid identification in accordance with the Research Data Management Policy (BI-RES-008). Retention periods must be defined to ensure archived data is stored only for as long as necessary. Any personal data within the archive must be identified and recorded to ensure the Institute meets its responsibilities as defined in the Data Protection Policy (BI-IM-002).

6.2.3. Data archived to RADAR is copied to two physical storage systems in different data centres at the Institute to ensure redundancy.

6.3. User email mailboxes

6.3.1. Email mailboxes are either stored on the Institute email server, or in Exchange Online.

6.3.2. Deleted items on the Institute email server, or in Exchange online, are retained for 30 days and recoverable by users via the 'Deleted Items' folder.

6.3.3. The Institute email server is backed up daily and retained for 30 days. Backups are taken for service disaster recovery purposes only and users are not able to restore this data themselves.

6.3.4. No additional backups are performed for the Exchange Online email service beyond that provided by Microsoft 365 cloud-based services. Microsoft replicate Exchange Online mailboxes across Microsoft datacentres for service disaster recovery purposes only and users are not able to restore this data themselves.

6.4. Electronic lab notebooks (ELN)

6.4.1. Backups of ELN Notebooks stored on SharePoint Online in Microsoft OneNote format are taken daily and retained perpetually. Backups are taken for business continuity purposes only and users are not able to restore this data themselves.

6.4.2. Users can restore deleted pages or recover previous page versions using functionality built into OneNote and SharePoint Online.

6.4.3. Deleted pages and page version retention use Microsoft's default retention settings.

6.5. OneDrive

6.5.1. No additional backup services are provided for data stored in Microsoft OneDrive as this is a resilient Microsoft 365 cloud-based service. Users should use OneDrive in-built functionality to restore previous versions of files as necessary.

6.5.2. If the owner/user of data stored in OneDrive leaves the institute, an archive process is triggered within 2 months of their leave date. The user's line manager is then notified of the pending deletion and given access permissions. The line manager has up to 30 days to copy any required data before it is deleted.

7. IT Service Data

7.1. Servers running Institute services are backed up on a regular basis for the purposes of disaster recovery. This process is managed through BICS policies and procedures.

7.2. Retention periods and backup frequency of IT servers varies depending on the server role and criticality. This ranges from non-critical server backups being retained for 7 days to critical server backups being retained for 40 days.

7.3. Immutable (read-only) backups are configured for IT servers to protect against corruption from a major cyber-attack. Read-only backups of critical business systems are retained for longer durations for disaster recovery purposes.

7.4. Network equipment configuration is backed up daily for the purposes of disaster recovery. There is no generic retention period for network device configuration, and older backups are manually purged as necessary.

8. Further information

8.1. This policy will be reviewed regularly to incorporate any changes, legislative or otherwise. The next review date is specified on the cover sheet.

8.2. Associated policies, procedures and guidance are listed on the cover sheet. The Policy Owner named on the cover sheet can be contacted with any queries.

8.3. This policy may be varied, withdrawn, or replaced at any time by the Institute at its absolute discretion.