Is the Data Archive suitable for sensitive data?

Your research data might warrant special security controls if its unauthorised release could:

- Cause distress to individuals or private entities,
- Breach undertakings to maintain confidentiality, or
- Negatively impact on the reputation of the University.

If your data is sensitive in any way, you must carefully assess any service you use to store and share it. At a minimum, you should:

Review the

- UNSW Research Code of Conduct.
- UNSW Procedure for Handling Research Material & Data.
- UNSW Retention periods for records relating to research.
- UNSW IT Policies & Guidelines.

You may also need to review:

- Guidelines, legislation & UNSW policies for human research.
- AIATSIS Managing research: use, storage and access.
- Values and Ethics - Guidelines for Ethical Conduct in Aboriginal and Torres Strait Islander Health Research.

You can also seek advice from the UNSW Human Research Ethics Home and visit the Australian National Data Service Publishing and Sharing Sensitive Data page.

Most research data does not require security controls above and beyond the University's standard practices. The Data Archive has been designed with UNSW policies and procedures in mind and so:

- Stores information on local servers (not overseas, which could be in breach of the Privacy Act).
- Is monitored for malicious attacks and security breaches.
- Has complete audit logs of user activity.
- Does not permit deletion of uploaded files.
- Provides granular access controls.

You can also adopt good security practices as an individual and within your research team, such as:

- Choosing a good password for your UNSW zID account and not sharing it.
- Ensuring that only authorised team members have access to data, by setting appropriate permissions (see the RDMP and Data Archive page for more information on setting permissions).

- Keeping computers secure (e.g. making sure operating systems and apps are up to date, and having a password or pin number on your device).
- Keeping copies of very important files in multiple locations.

Note: deletion of data from the Data Archive requires UNSW IT intervention. Contact your local IT support or the UNSW IT Service Centre (**9385 1333**) to discuss management of mandatory retention and deletion requirements.

Help and further information:

- To learn more about the Data Archive:
  - go to the Start here page
  - see all Help Topics
  - see all Frequently Asked Questions (FAQs)
  - browse through the carousel on the homepage to view all available videos
- To access the Data Archive Web application, use this link, or, go to the Home page for other access options
- To create, or update, a Research Data Management Plan go to the ResData service
- **Note**: the Data Archive service is also available over SFTP, see the SFTP client guide for more information