Research Data Management Plan

1. Overview

1.1 Applicant	
1.2 Project title [as on converis system]	
1.3 Project start and end dates	

2. Defining your data

2.1 Where does your data come from? Select an option:	
• Primary data (e.g., surveys, interviews, experiments)	
• Secondary data (e.g., existing datasets, public records)	
Describe (*Example:* "Data will be collected from interviews with 20 participants")	

2.2 What formats are your data in? Select an option: *Risk Management Tip: Some formats may pose security or accessibility risks. Ensure appropriate encryption or storage solutions are used.*	
• Text files (e.g., CSV, TXT, pdf)	
• Image files (e.g., JPEG, PNG)	
• Audio/video files (e.g., MP3, MP4)	
• Other (please specify)	

2.3 How often do you get new data? *Risk Management Tip: Data influx frequency can affect how data is managed and stored. High-frequency data collection might require more frequent backups or more robust storage systems.*	
• Daily	
• Weekly	
• Monthly	
• Once off	
• Other (please specify)	

2.4 How much data do you generate? *Risk Management Tip: Large volumes of data may increase the risk of data loss or corruption. Consider implementing automated backups and using appropriate storage solutions.*	
• Small-scale (e.g., under 1 GB) *Hard copy: small scale (1 file/ number of pages)*	
• Medium-scale (e.g., 1-10 GB)	
• Large-scale (e.g., over 10 GB)	

2.5 Who owns the data you generate? – Confirm CUT policy/ Degree purposes/ non-degree *Risk Management Tip: Ensure that data ownership is clearly defined to prevent disputes, and that intellectual property rights are respected.*	
• Researcher(s)	
• Institution (e.g., university or funding body)	
• Collaborating organizations	
• Sponsor/Funding organization	

3. Looking after your data

3.1 Where do you store your data? *Risk Management Tip: Consider the security and redundancy of your storage. For sensitive data, encrypted storage may be necessary.*	
• Local (e.g., external hard drives, USB drives) [include physical location]	
• Cloud storage (e.g., Google Drive, Dropbox)	
• Institutional storage (e.g., university servers, cut library, figshare	
Location/ address for hard copies	

3.2 How are your data backed up? *Risk Management Tip: Regular and off-site backups reduce the risk of data loss due to hardware failure or security breaches.*	
• Manual backups	
• Automated backups (e.g., cloud services)	
• Hard copies	

3.3 How do you structure and name your folders and files? *Example: "Data_Interview1_2025_01_30"* • *[Subtype]: The type of project document (i.e. "Form", "Draft" etc.)* • *[Project reference]: Project reference including the document and part number and the project id (i.e. "ISO/DIC 24495-1", "ISO/CD 21911")* • *[Document main topic]: A short description of what the main topic covered in the document (i.e. "Project limit extension request", "Revised proposal of Short Circuit test method", "Detailed observations and comments")* • *[Expected action if important]: If the expected action for the committee is important, you may reinforce it at the end of the document title (i.e. "For voting").* *Examples:* • *Comments - ISO/DIS 24495-1 - Detailed observations and comments from participants* *Risk Management Tip: Clear naming conventions help ensure data integrity and traceability, reducing the risk of misplacement or overwriting.*	
Description	

3.4 How do you manage different versions of your files? *Risk Management Tip: Version control is essential for maintaining the integrity of data and avoiding confusion with multiple iterations of the same file.*	
• Version control software	
• Manual versioning (e.g., "v1," "v2")	

3.5 What additional information is required to understand the data? *Risk Management Tip: Clear metadata reduces the risk of data misinterpretation and ensures compliance with ethical standards.*	
• Data dictionaries	
• Methodological details	
• Participant consent forms	
• Other (please specify)	

Research Data Management Plan

4. Archiving your data

4.1 What data should be kept or destroyed after the end of your project? *Risk Management Tip: Destruction of sensitive data is critical to mitigate privacy risks, while archiving ensures data preservation for future use.*	
• All data will be retained	
• Sensitive data will be destroyed after the project	
• Publicly shared datasets will be archived	

4.2 For how long should data be kept after the end of your project [minimum 3 years as per the CUT HREC policy]? *Risk Management Tip: Retaining data for an appropriate period is essential for compliance with institutional and legal requirements, as well as future research opportunities.*	
• 3 years	
• 5 years	
• 10 years	
• Indefinitely (for public datasets)	

4.3 Where will the data you keep be archived? *Risk Management Tip: Select an archival solution that ensures long-term preservation and compliance with data-sharing policies.*	
• Institutional repository [CUT library]	
• Public repository	
• Private cloud storage [consider future access]	

4.4 When will data be moved into the archive? *Risk Management Tip: Timing of archival ensures data availability and integrity while reducing the risk of losing valuable research findings.*	
• At the conclusion of the project	
• After data analysis is complete	

4.5 Who is responsible for moving data to the archive and maintaining them? *Example: "Data will be transferred to the institutional repository by the principal investigator (PI) and maintained by the university's research office."* *Risk Management Tip: Clearly assigning responsibility reduces the risk of oversight or data mismanagement.*	
Description	

5. Sharing your data

5.1 Who else has a right to see or use this data during the project?	
• Research team members	
• Collaborators	
• Funders	
• Supervisors	

5.2 What data should or shouldn't be shared openly and why? *Sensitive personal data should not be shared openly.* *Aggregated or anonymized data may be shared publicly.*	
Indicate specific project data	

5.3 Who should have access to the final dataset and under what conditions?	
Open access	
Restricted access (e.g., upon request, for approved researchers)	

5.4 How will you share your final dataset?	
• Publicly accessible database	
• Research publication as supplementary material	
• Upon request from the researcher or institution	
• Final dissertation/thesis available through CUT library	

6. Implementing your plan

6.1 Who is responsible for making sure this plan is followed?	
• Principal Investigator	
• Supervisors	

6.2 How often will this plan be reviewed and updated? *Risk Management Tip: Regular reviews ensure that any evolving risks, regulatory changes, or technological advancements are addressed.*	
• Annually	
• Every 3 months	
• Every 6 months	
• If changes are made to the proposal	

6.3 What actions have you identified from the rest of this plan? *Risk Management Tip: Identifying concrete actions helps ensure that any risks, including data breaches or legal violations, are minimized.*	
Description	

6.4 What policies are relevant to your project? [create drop down list of relevant CUT policies, POPIA act etc]	
Description	CUT Policies

6.5 What further information do you need to carry out these actions?	
• Training on ethical data management	
• Access to data management software	
• Library support	