Data Storage Policy

1. Introduction

1.1. This policy outlines the use of data storage within the organisation to protect data.
1.2. This policy describes how data shall be collected, accessed, secured, and used to meet organisation data protection standards as well as [legislative requirements and regulatory requirements]. This data storage policy complies with data protection law and follows best practices
Protects the rights of staff, customers, and partners
Is open about how it stores and processes individuals' data
Protects itself from the risks of a data breach

2. Scope

2.1. This policy covers all devices used to conduct organisation related business, and any file storage methods.
2.2. All contractors, suppliers and other people working on behalf of the organisation

3. Data Access

Only employees/users with a business necessity shall be granted access to data storage. Data shall not be shared informally. When access to confidential information is required, employees/users shall request it from their manager. Organisation will provide training to all employees/users to help them understand their responsibilities when handling data.

Employees/users should keep all data secure, by taking sensible precautions and following the guidelines below.

- Strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the organisation or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees/users should request help from their supervisor or Manager if they are unsure about any aspect of data protection.

4. Data Security

When working with private data, employees/users should ensure the screens of their computers are locked when left unattended. It should never be sent in clear text (e.g. email). Data must be encrypted before being transferred electronically. Managers and supervisors can explain how to send data to authorized external contacts. Employees/users should not save copies of personal data to their own computers. Always access and update the central copy of any data.

5. Data Use

Everyone who works for or with organisation has some responsibility for ensuring data is collected, stored, and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

6. Data Destruction

Organisation will only dispose of data and records in accordance with the requirements of the state and federal government legislative instruments. The destruction of data may be registered in the approved process and will be managed centrally through the Manager who will maintain a register of such. Data must not be destroyed if it is, or may be, the subject of a subpoena, or other formal request for access or relate to any ongoing action such as an appeal, regardless of whether the minimum statutory retention period has expired.

7. Data Storage

7.1. Local (SSD) disk drives

7.1.1 Local (SSD) disk drives on managed instances are for the primary purpose of storing the operating system and local profile settings for users. These should always be regarded as volatile – when a managed instance is imaged it **will** overwrite any data on it.
7.1.2. Local (SSD) disk drives **must not** be used for any storage of organisation or personal data. Organisation data should always be stored on approved organisation cloud storage services.
7.1.3. Local (SSD) disk drives should not be considered as secure.
7.1.4. IT Team for the organisation will reserve the right to refuse any request to attempt restoration of any organisation or personal data that has been lost by having been stored on local (SSD) disk drives.

7.2. Cloud storage

7.2.1. Only organisation approved cloud storage services should be used for the storing of University data. Details of approved and provided cloud storage services can be found on the cloud portal.
7.2.2. All approved cloud storage will be encrypted storage.
7.2.3. Most members/users are eligible for an approved cloud storage account. Details of eligibility can be found on the cloud portal.
7.2.4. Cloud storage allows for collaborative working. When sharing files, it is the responsibility of the storage area owner to check that the files are being shared with the intended collaborators.
7.2.5. Caution should always be exercised when sharing files through public links. These are not restricted to members/users and anyone who is in possession of the link can access the shared files. This may not always be the intended recipient. To mitigate the risks of unintended sharing of files in this way IT Teams have set the default expiry time of any shared public links to a period of 90 days.
7.2.6. If a member/user changes role or leaves the institution and are an owner of files that have been previously shared, it is the responsibility of that member to ensure that ownership of files is transferred to another appropriate member before they do so.
7.2.7. When a member/user leaves the organisation or changes to a role which no longer entitles them to a cloud storage account, their cloud storage account will be closed and then deleted after a period of 30 days.
7.2.8. Cloud storage is subject to quotas and must only be used for storing University data, and not for the purpose of personal information such as photos, music, or videos.

[Version Change Description] [Date] [Author]