**Data Management Plan – Guidance regarding storage and access to research data collated by the University of Stirling**

We proposed the raw data is stored on a restricted SharePoint site which will be created and hosted by the University. The site will be restricted via access control and only those who need to view/edit data, will be given access. Access will be monitored. Access to the SharePoint site will be via Teams or web browser secured via HTTPS 443.

All University accounts are protected by MFA and use of a VPN is encouraged when accessing University resources including SharePoint.  We can add in a MFA prompt for external stakeholders accessing University resources as an additional security measure.

There will be restricted access to the SharePoint site with view only access of any data to maintain the integrity of the recordings but also the security of the data. Access to the site will be reviewed on a monthly basis to ensure prompt removal of those no longer requiring access.

Having a University account and using a University device, allows for MFA authentication and further security practices.

Additionally, the University utilises InTune which means if the device was lost or stolen, we can remotely wipe the device, minimising the possibility of a data breach.

The University account will have an expiry date, meaning access and level of access will be routinely reviewed.

Lastly, we operate on a least privilege basis, meaning users will have the minimum level of access rights possible to allow them to undertake their work.

|  |  |
| --- | --- |
|  | SharePoint |
| Licence Ownership | University of Stirling |
| File Transfer options | 443 – Direct Transfer via SHTTP |
| Physical location of data storage | Europe North Region: Microsoft are only able to specify that it will be in one or more of the following: Austria (Vienna), Finland (Helsinki), France (Paris, Marseille), Ireland (Dublin), Netherlands (Amsterdam) |
| Physical security measures in place | Please refer to the following MS document:  [Physical security of Azure datacenters - Microsoft Azure | Microsoft Docs](https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security) |
| Data retention timescales | Data deleted after end of study as per study data management plan. |
| Data backup details | 93 day deleted file retention.    Rubrik Backup solution for SharePoint and OneDrive (4 week retention) |
| Data Removal standards | Please refer to the following MS documents  [Microsoft 365 SharePoint Online Data Deletion - Microsoft Service Assurance | Microsoft Docs](https://docs.microsoft.com/en-us/compliance/assurance/assurance-sharepoint-online-data-deletion)  [Data destruction in Microsoft 365 - Microsoft Service Assurance | Microsoft Docs](https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-destruction) |
| System management | University of Stirling Infrastructure Team |
| 3rd party access? | Researchers involved in the project. |
| Security measures to protect data | Please refer to the following MS documents  [Security monitoring overview - Microsoft Service Assurance | Microsoft Docs](https://docs.microsoft.com/en-us/compliance/assurance/assurance-security-monitoring) |
| Access control management | Access will be restricted to specified individuals that will be determined by the research team. The actual granting of access with be performed by the University of Stirling Infrastructure Development Team after gaining approval through our Change Management process. This process is part of the University of Stirling Information Services Operating Policies    <https://www.stir.ac.uk/media/stirling/services/policy-and-planning/documents/08-Acceptable-Use-Policy.pdf>    <https://www.stir.ac.uk/media/stirling/services/policy-and-planning/documents/001-Electronic-Information-Security-Overarching-Policy.pdf> |
| Data access control | This is covered by the University policies above.    Please refer to the following MS documents  [Identity and access management overview - Microsoft Service Assurance | Microsoft Docs](https://docs.microsoft.com/en-us/compliance/assurance/assurance-identity-and-access-management) |
| Penetration Testing | We regularly undertake Penetration Testing by a third party company. |

**Data Flow:**

The following steps outline the method in which the data will be handled in a secure manner and stored to ensure no misuse.

1. Authorised agent will transfer data from an authorised device to the restricted Sharepoint/Teams site via SHTTP, using either their own University of Stirling account or partner University account.
2. Once transfer is complete, the data will be deleted from the laptop storage.
3. SharePoint/Teams site for data storage will be restricted via access control.
4. All access will be monitored.

**NB: The University does not recommend the use of OneDrive for research data storage.**