 Information Assurance Services

**University Data Classification Decision Matrix**

**Decision Matrix**

Different types of data fit within different security levels, each of which has a level of risk attached should this data be lost, leaked or misused. The matrix shows the University data and risk classifications, with examples of data that fit into each classification.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Public/ Unrestricted** | | | | |
| **Classification** | **Description** | **Impact of unauthorised disclosure** | **Types of data** | **Appropriate IT facilities might include** |
| **Public** | Publicly available information | **None:**  No confidentiality issues, must still be accurate and protected from unauthorised change | - Website/internet content    - Marketing/publicity  - Research activity details | - Well-managed University and personally- owned PCs, mobile devices and removable media (external storage).  - University managed email services.  - Appropriately secured web-servers.  - LAMP service. |
| **Unrestricted** | Information that is not in the public domain but would cause minimal harm should unauthorised disclosure occur. | **Low:**  No sensitive data.  No compliance restrictions.  Disclosure might be inappropriate but of little significance. | - Internal correspondence  - Data which would be released as part of Freedom of Information request.  - Data which is not subject to legal, regulatory, commercial, contractual embargo.  - Data not yet prepared for formal publication. Policies and procedures. | - Well-managed University and personally- owned PCs, mobile devices and removable media (external storage).  - University managed email services, Appropriately secured web-servers  - LAMP service.  - Research R:drives,  - Alice (HPC),  -Specialist IT facilities (e.g. MRI).  VPN from fully managed laptop |
| **Restricted** | | | | |
| **Classification** | **Description** | **Impact of unauthorised disclosure** | **Types of data** | **Appropriate IT facilities might include** |
| **Restricted** | Information which could cause harm or distress, to individuals or the University, should unauthorised disclosure occur. | - Distress or embarrassment to small numbers of individuals.  - A degree of damage to the University’s reputation or operations.  - Breach of legislation, regulation or contract with possibility of some financial penalty.  - Potential to prevent specific current or future research activity. | - Data subject to legal, regulatory, contractual embargo (unless a higher degree of restriction is specified).  - Data with ethical/moral/confidentiality implications e.g. identifiable deceased data subjects.  - Identifiable Personal Data\* covered by Data Protection Act 2018 and Article 6 GDPR | - IT services for which the University has the *Cyber Essentials* certification:  - Fully-managed Windows 10/Linux desktops (no local admin rights)  - Fully- managed laptops if permitted  - Enhanced security Research Filestore (R:drive) - Enhanced security HPC (Alice)  - Filedrop. Encrypted  - Specialist IT facilities (e.g. MRI) with approved and agreed Standard Operating Procedure.  - Appropriate University system e.g. Student Record System. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Highly Restricted** | | | | |
| **Classification** | **Description** | **Impact of unauthorised disclosure** | **Types of data** | **Appropriate IT facilities might include** |
| **Highly Restricted** | Information which is likely to cause serious harm to individuals or the University should unauthorised disclosure occur | - Risk to safety or well-being of individuals.  - Significant distress to individuals  - Substantial legal consequence to individuals or the University.  - Substantial financial penalties.  - Substantial damage to University reputation or operations.  - Institutional damage, may cause a wide block on research, funding, data sharing or collaboration | - Data which poses risk to personal safety.\*\*  - Patient identifiable data\*\*.  - Sensitive personal data\*\*  Protected characteristics defined by Equalities Act 2010\*\*  - Special Category Data under DP Act 2018 and Article 9 of GDPR\*\*.  - Data subject to legal, regulatory, contractual restrictions.  - Data subject to embargo for which highest degree of restriction is specified | - Appropriate University system e.g. Student Records System, HR System, SAP.  - Specific, access controlled folder within Departmental Shared Area (X: drive)  Filedrop – documents containing this data must be encrypted before being place in Filedrop and any password provided to the recipient by a different method.  - Enhanced Security Research Filestore (R: drive)  - *Cyber Essentials+* Secure Computer and Storage Service for Research (contact IT Business Partner for information) |

**Notes:**

#If the PI still needs access to the R:Drive remotely and their data is higher than ‘Unrestricted’, it is assessed on a case-by-case basis involving Information Assurance Services and RED.

\*All require Combined ROPA (Register of Processing Activities) and Threshold DPIA (Data Privacy Impact Assessment) before processing commences.

\*\*All require Combined ROPA (Register of Processing Activities) and Threshold DPIA and likely to require a Full DPIA before processing commences.

For any data you need to process or otherwise use, please also refer to the Data Classification Guidance Notes and Data Classification Decision Tree.

As a rule of thumb, anything not covered in this document defaults to highly restricted. .