DATA SENSITIVITY, SECURITY & STORAGE ADVICE

Version: 15 April 2020

Research Data may contain information of a personal or sensitive nature which must be protected against unwarranted disclosure. Sensitive information may include but is not limited to; health-related data; personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; financial information; genetic data or biometric data processed solely to identify a human being. Sensitive information may also relate to information which may pose a risk to cultural resources, the environment or animals (such as the location of endangered species) or to national security.

Research Data at Macquarie University can be broadly grouped into three categories depending upon the sensitivity of its information. The categories are: General, Sensitive, and Highly Sensitive.

This schedule outlines:

1. a guide for assessing and classifying data as highly sensitive, sensitive or general
2. appropriate security measures and storage options for active data according to its sensitivity classification

Data sensitivity indicators

Data is generally considered either Sensitive or Highly Sensitive if it contains Identifiable “personal information” or identifiable health information. This includes:

1. ''[Information or an opinion] about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.' (PPIPA 1998 section 4.1; HRIPA 2002 section 5.1)
2. See also: ''...information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.' (Australian Privacy Act 1998).

The type of “personal information” contained in the data will largely help determine if it should be classified as “Highly Sensitive” or “Sensitive”, as follows.

Highly sensitive data

Research Data is considered highly sensitive when:

1. it contains the following types of “personal information” (adapted from the Australian Privacy Principles, Privacy Act of 1988, schedule 1; see APP B.138 for more information), is identifiable, and could put someone at risk if made available:

   - racial or ethnic origin
   - political opinions
   - membership of a political association
   - religious beliefs or affiliations
• philosophical beliefs
• membership of a professional or trade association
• membership of a trade union
• sexual orientation or practices
• criminal record
• health information about an individual
• genetic information
• biometric information
• financial information

a. it contains information that is subject to regulatory controls (or poses a risk to national security, refer to Defence Trade Controls Act).

**Sensitive data**
Data might be considered **sensitive** when:

• It is identifiable and contains personal information / human subject data but does not concern the sensitivity indicators listed above (in section 4.2)

• it does concern a sensitivity indicator listed above and is anonymised but could potentially be re-identified if combined with other, publicly available, data.

• it contains cultural heritage location information or other heritage data where community consent for release is lacking (standards and procedures vary in different countries)

• it contains ecological or environmental data concerning rare, threatened or endangered species

• it contains data governed by IP / commercialisation agreements

• Data where one or more investigators on the project do not consent to its release (agreement should be reached before a project is launched)

• It contains non-work-related contact information, location information, or other information deemed ‘private’, ‘confidential’, or ‘sensitive’ by any MQ policy

This list is not exhaustive; if you think that your data may be sensitive and have queries relating to this checklist contact a Data Officer/Data Steward.

**General Data**
Data might be classified **general** when it is:

• Publicly available third-party data

• Open data

• It is not sensitive or highly sensitive
Data protection and security practices for management of active data

Security practices must be applied to all data to prevent unauthorized access.

The sensitivity level of the data determines the security practices that must be applied during data management. Researchers are expected to obtain assistance from IT (if needed) to meet the following requirements:

1. **The standard security practices which should be applied to research data which isn’t classed as either sensitive or highly sensitive are:**
   - You must back up your data (e.g., using OneDrive or AWS’s backup mechanisms). All backups must be automated.
   - You should back up your data to a second storage location (e.g. if you use OneDrive, backup to Cloudstor).
   - You should encrypt all personal or work devices from which the data will be accessed.
   - You should use the enterprise password manager and ensure unique, strong passwords for all services related to the data. The master password to the manager must be strong.
   - You should use two-factor authentication with an authenticator app or hardware token (preferred).

2. **If your data is classed as sensitive the following security practices are expected:**
   - You must back up your data to a second storage location. All backups must be automated.
   - You must encrypt all personal or work devices or drives used store the data locally (including devices synchronised with online storage).
   - You must use two-factor authentication with an authenticator app or hardware token (preferred).
   - You should use the enterprise password manager and ensure unique, strong passwords for all services related to the data. The master password to the manager must be strong.

3. **If your data is highly sensitive the following security measures must be applied:**
   - You must back up your data. All backups must be automated.
   - You must use only MQ-issued devices and drives to access or locally store the data.
   - You must encrypt all devices or drives used to store the data locally (including devices synchronised with online storage).
   - You must use two-factor authentication with an authenticator app or hardware token (preferred). Use of two-factor must be required each time the services are accessed.
• You **must** use the enterprise password manager and ensure unique, strong passwords for all services related to the data. The master password to the manager must be strong.

**Table 1: Security Requirements according to Data Sensitivity Classification**

<table>
<thead>
<tr>
<th>Security measures</th>
<th>General</th>
<th>Sensitive</th>
<th>Highly sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated backup</td>
<td>Must</td>
<td>Must</td>
<td>Must</td>
</tr>
<tr>
<td>Backup to secondary storage location</td>
<td>Should</td>
<td>Must</td>
<td>Must</td>
</tr>
<tr>
<td>Personal devices can be used</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Devices (MQ or personal) encrypted</td>
<td>Should</td>
<td>Must</td>
<td>Must</td>
</tr>
<tr>
<td>Enterprise password manager</td>
<td>Should</td>
<td>Should</td>
<td>Must</td>
</tr>
<tr>
<td>Two-factor authentication</td>
<td>Should</td>
<td>Must</td>
<td>Must</td>
</tr>
</tbody>
</table>

**Storage of 'active' data**

1. As long as the appropriate security measures are followed (as in Table 1), the Macquarie University pre-approved storage options data (NOT for Highly Sensitive data) includes: Office365 OneDrive, Cloudstor, and Open Science Framework native storage (if 'Australia' is selected as the project location)

2. Custom storage solutions using Australia-based Amazon Web Services or other web services may also be acceptable but will require approval by a Research Data Officer/Data Steward via a Data Management Plan.

3. Bespoke on-site storage devices or other arrangements could be possible with the support of your Faculty IT and will require approval by a Research Data Officer/Data Steward via a Data Management Plan.

4. For highly sensitive data, contact your Data Steward or a Research Data Officer. Highly sensitive data will require client-side encryption or a bespoke storage solution arranged by your Faculty IT group (for example, OneDrive can be configured for this purpose).

**Table 2: Storage Options according to Data Sensitivity Classification**

<table>
<thead>
<tr>
<th>Storage options</th>
<th>General</th>
<th>Sensitive</th>
<th>Highly sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Macquarie SharePoint</td>
<td>Preferred</td>
<td>Preferred</td>
<td>Yes (properly configured)</td>
</tr>
<tr>
<td>Macquarie OneDrive</td>
<td>Preferred</td>
<td>Preferred</td>
<td>No</td>
</tr>
<tr>
<td>Cloudstor</td>
<td>Preferred</td>
<td>Preferred</td>
<td>No</td>
</tr>
<tr>
<td>Open Science Framework native storage</td>
<td>Yes</td>
<td>Yes (if Australian data location specified on project creation)</td>
<td>No</td>
</tr>
<tr>
<td>Commercial cloud (if locally supported and AU storage location)</td>
<td>Yes</td>
<td>Yes (if data Australian data location specified)</td>
<td>Yes (properly configured)</td>
</tr>
<tr>
<td>Peak Facility (NCI, Pawsey)</td>
<td>Yes</td>
<td>Yes</td>
<td>TBC</td>
</tr>
<tr>
<td>On-premise (bespoke) (If institutionally approved)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>