Standard Operating Procedure (SOP) for Handling Ethical and Sensitive Data in Open Science at Universiti Malaysia Sarawak (UNIMAS)

1. Purpose

1.1 This Standard Operating Procedure (SOP) outlines guidelines and standard procedures for the management, sharing, and archiving of ethical and sensitive data in accordance with the principles of Open Science. The objective is to protect the privacy and data security of participants while simultaneously guaranteeing transparency, reproducibility, and ethical integrity.

1.2 The Open Science Research Data Management Policy of Universiti Malaysia Sarawak (UNIMAS) 2024 shall be read in conjunction with this SOP.

2. Scope

2.1 This SOP is intended for all personnel, data managers, and researchers who are engaged in the collection, analysis, storage, and dissemination of sensitive data in accordance with Open Science mandates.

3. Definitions and Interpretations

3.1 Anonymization

Anonymization means process of removing identifiable information from data sets to prevent traceability to the individual sources.

3.2 Open Access

Open Access means the access is freely availability on the public internet, permitting any users to read, download, copy, distribute, print, search or link to the full texts of these articles, crawl them for indexing,

pass them as data to software or use them for any other lawful purpose without financial, legal or technical barriers other than those inseparable from gaining access to the internet itself.

3.3 Personal Data

Personal Data means any information in respect of commercial transactions, which: (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; or (ii) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly, or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

3.4 Personal Data Protection Act 2010 (Act 709) (PDPA)

Personal Data Protection Act 2010 (Act 709) (PDPA) means an Act to regulate the processing of personal data in commercial transaction and to provide for matters connected therewith and incidental thereto. The Act was passed by the Malaysian Parliament on 2 June 2010 and came into force on 15 November 2013.

3.5 Sensitive Data

(a) "Sensitive Data" means data that can be used to identify an individual, species, object, process, or location that introduces a risk of discrimination, harm, or unwanted attention. Under law and the research ethics governance of most institutions, sensitive data cannot typically be shared in this form, with few exceptions.

(b) This refers to an information that could potentially harm an individual if disclosed. This includes, but is not limited to, personally identifiable information (PII), health records, financial information, and data related to ethnic, religious, or political backgrounds.

(c) Sensitive data is data that must be safeguarded from unauthorized disclosure. This may be the result of the nature of the research and/or data, the legislative requirement, or data that is pending for proprietary application, as illustrated in Table 1.

Table 1: Descriptions of Different Categories of Sensitive Data

Sensitive Data	**Descriptions**
Personal Data	Identification number, medical record, location (GPS)
Confidential Data	Trade secrets, investigations, security (passwords, financial information, national safety)
Restricted Data	Data that can only be shared with a certain group of people
Data with proprietary interest	Data that wants to be filed for any intellectual property rights to protect the novelty

(Source: Akademi Sains Malaysia)

3.6 Sensitive Personal Data

(a) Sensitive Personal Data means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission of any offense by him, or any other personal data data as the Minister of Communications and Multimedia Malaysia ('Minister') may determine by order published in the Gazette. Other than the categories of sensitive personal data listed above, the Minister has

not 'Gazetted' any other types of personal data to be sensitive personal data as of 29 December 2014.

4. **Ethical Considerations**

4.1. Informed Consent

(a) Ensure that participants are fully informed about the nature of the data being collected, how it will be stored, and the contexts in which it will be shared.

(b) Obtain explicit consent for data use in research, publication, and any future sharing in open repositories.

4.2. Data Minimization

(a) Collect only the data necessary for the research purposes.

(b) Avoid gathering excessive or irrelevant information.

4.3. Anonymization and Pseudonymization

(a) Prior to sharing data, ensure all identifiable information is removed or masked.

(b) Use pseudonyms or codes to replace identifying information where complete anonymization is not possible.

5. There is concern about violations of public dissemination of research findings which may be common, such as:

(a) Premature claims on findings or fabrications.

(b) Unfairness when giving credit to research colleagues, collaborators, students, funding agencies;

(c) Unprofessional conduct;

(d) Disclosure of sensitive information that violates “personal rights” or personal data protection or breach of confidentiality;

(e) Over-sensationalise findings or irresponsible media reporting;

(f) Withholding beneficial information;

(g) Non-sharing of public information or data funded by public funds;

(h) Use of an inappropriate medium that can reach an inappropriate audience, resulting in unwanted consequences, e.g. causing a panic situation amongst the general public; and

(i) Approval or permissions were not obtained, resulting in a situation as in (h) above.

6. Data Handling Procedures

6.1. Data Collection

(a) Utilize secure methods and tools for data collection to ensure initial protection of sensitive information.

(b) Store raw data in encrypted formats.

6.2. Data Storage

(a) Store sensitive data in encrypted databases with restricted access.

(b) Implement robust authentication mechanisms to ensure only authorized personnel can access the data.

6.3. Data Processing

(a) Use secure servers and encrypted channels for data processing.

(b) Implement access logs and regular audits to monitor data access and modifications.

7. Data Sharing

7.1. Ethical Sharing

(a) Ensure that shared datasets are devoid of any information that can lead to the identification of individuals.

(b) Accompany data releases with metadata explaining the levels of anonymization and any remaining risks.

7.2. Licensing and Restrictions

(a) Apply appropriate licenses that clarify permissible uses of the data.

(b) Set limitations based on the sensitivity of the data, ensuring compliance with ethical standards and participant consent.

8. Data Security

8.1. Encryption

(a) Encrypt sensitive data both in transit and at rest.

(b) Regularly update encryption protocols to the latest standards.

8.2. Access Control

(a) Implement role-based access controls (RBAC) to limit data access based on user roles and responsibilities.

(b) Conduct regular reviews of access controls and adjust as necessary.

8.3. Incident Response

Develop and maintain an incident response plan for data breaches, including immediate containment, mitigation, and notification procedures.

8.4. Research Data with National Security Risks

Sharing and re-using data containing information with national security risks is governed by several Acts in Malaysia, such as listed few in paragraph 10.

9. Training and Compliance

9.1. Training Programs

(a) Provide regular training on ethical data handling, security measures, and compliance with relevant regulations to all personnel.

(b) Ensure understanding and adherence to this SOP and related policies.

9.2. Compliance Monitoring

(a) Conduct periodic audits to ensure compliance with this SOP.

(b) Address non-compliance through corrective actions and, if necessary, disciplinary measures.

10. Documentation and Reporting

10.1. Documentation

(a) Maintain detailed records of consent forms, data processing activities, access logs, and audits.

(b) Ensure transparency in documenting the methodologies used for data anonymization and sharing.

10.2. Reporting

(a) Immediately report any incidents of data breaches or ethical violations to the designated authority.

(b) Submit regular compliance reports to oversight bodies.

11. Review and Updates

11.1 Conduct annual reviews of this SOP to incorporate improvements, updates to laws and regulations, and feedback from stakeholders. Update procedures as necessary to adapt to new challenges and technologies.

11.2 This SOP aims to balance the ideals of Open Science with the imperatives of ethical responsibility and data security, ensuring that sensitive data is handled with the utmost care and respect.

11.3 **Few Guidelines on Ethics and Data Protection as the main references to this SOP are as follows:**

(a) European Commission Ethics and Data Protection

(b) Personal Data Protection Act 2010

(c) Code of Research Ethics

(d) Guidelines for Ethical Review of Clinical Research or Research involving Human Subjects

(e) Malaysia Guidelines Good Clinical of Practise

(f) Intellectual Property Rights (Patents Act 1983, Trademarks Act 2019, Industrial Design Act 1996, Copyright Act 1987, Layout-designs of Integrated Circuits Act 2000

(g) Computer Crimes Act 1997

(h) Penal Code Act 574

(i) National Security Council Act 2016

(j) Official Secrets Act 1972

(k) Wildlife Conservation Act 2010

(l) National Biosafety Act 2007

(m) Sarawak Biodiversity Centre Ordinance (Amendment) 2003

(n) Sarawak Biodiversity Enactment 2000

(o) National Policy on Biological Diversity 2016-2025

(p) The Malaysian Code of Responsible Conduct in Research (MCRCR) by the National Committee on Research Integrity, Academy of Sciences Malaysia 2020.

12. Effective Date:

12.1 This Standard Operating Procedure (SOP) for Handling Ethical and Sensitive Data in Open Science at Universiti Malaysia Sarawak (UNIMAS) is fully effective commencing from the date of the approval by UNIMAS Executive Committee Meeting Bil. 05 2024 ke 90 on 26 July 2024.