Data Management Policy

1. Preamble 2

2. Definitions 3

3. Intent 5

4. Scope 5

5. Roles and Responsibilities 5

5.1. Researcher 5
5.2. Data Manager 5
5.3. Data Custodian 6
5.4. Executive Director, IMAS 6

6. Policy Matter 6

6.1. Data Storage and Organisation 6
6.2. Destruction of Data 6
6.3. Remote Access 6
6.4. Backups 6
6.5. Data Integrity 7
6.6. Access Control 7
6.7. Data Archiving and Sharing 7
6.8. Metadata 8
6.9. File formats 8
6.10. Data Management Plan 8
6.11. Intellectual Property 8
6.12. Confidentiality and Privacy 8
6.13. Design and Naming Conventions 9

7. Supporting Guidelines 9

7.1. IMAS Data Management Guidelines 9
7.2. Relevant Legislation 9
7.3. Relevant Policies and Other Documents 9

8. Policy Responsibilities 9

1. Preamble

- The Institute for Marine and Antarctic Studies (IMAS) collect, collate, maintain and store Data in the process of undertaking research.

- Data collected by IMAS is diverse in its format and content and may comprise small, experimental datasets confined to a single or short time period through to large multi-faceted datasets collected over a long term.

- The Data collected is, in the vast majority of cases, a high value asset. This valuation acknowledges:

    - the high cost involved in collecting the Data;

    - its value as an historical record and

    - its value in contributing to amalgamated Data (where the whole may present higher value than the sum of the parts).

- Future value of Data assets cannot be determined at the time of Data collection. Data deemed to be of low value may increase substantially in value with changes in social and political trends, scientific knowledge and environmental management requirements. All Data should be considered a high value, long term asset.

- Ensuring good curation practice and public availability of all IMAS Data (excluding Data limited by commercial potential, confidentiality or privacy) for use by colleagues worldwide:

    - adds significant potential for increased research outcomes through expanded use of the Data;

    - is frequently a requirement of funding organisation agreements entered into by IMAS and

    - may be required by legislation (eg. The Antarctic Treaty).

- Research Data collected by IMAS may be subject to various, and sometimes complex, Intellectual Property Rights. This may involve joint ownership, ownership retained by a funding organisation or overriding agreements made by State or Federal Government.

- In order to maximise the current and future value of Data collected, it is necessary to ensure all Data is:

    - securely stored and accessible for the long term;

    - documented to a standard that ensures the research community can re-use and have confidence in the Data and

    - published in a public and readily accessible format for all IMAS stakeholders and the wider research community with adequate protection of commercial interests, confidentiality, privacy and a researchers right to first publication as required.

2. Definitions

For the purpose of this Policy, the following definitions shall apply:

Data

Data means research outcomes that are collected by IMAS staff, students and honorary staff in the course of their employment or other contract or agreement with IMAS which are capable of being stored digitally (including data that can be converted to digital format) and includes:

- numerical or qualitative data;
- images, video or audio;
- documentation describing the data;
- documentation describing the data collection methodology or
- processed data or data derived from raw data considered to be a distinct and separate dataset from the raw data.

But does not include administrative data (such as financial and human resource data) or other data containing "personal information" as defined by the Personal Information Protection Act 2004.

Data Custodian

Means any person or entity having a contractual obligation to provide computer hardware, a data centre, an archiving facility or any other service involving access to Data.

Database File

A Database File is defined as a disk file containing Data that is accessed using specialised software capable of reading the file and normally supports a limited access security model and limited Data integrity support. Examples include a Microsoft Access database or Microsoft Excel Spreadsheet.

Data Management

Data Management includes activities such as:

- Creating databases and application software for accessing Data;
- collecting and organising Data;
- making digital copies (such as back-ups) of Data;
- archiving or making Data available to others;
- managing access to Data;
- ensuring systems and processes are used to maintain a high level of integrity in the Data and
- planning and/or designing any of the above activities.

Database Server

A Database Server is defined as a server that provides access to Data using network protocols; is capable of complex access security allowing selective access to specific components of the Data and can implement complex Data integrity rules. Examples include Microsoft SQL Server and Oracle Database.

Intellectual Property

For the purposes of this policy document, Intellectual Property means Intellectual Property as defined in the University of Tasmania Intellectual Property Policy.

Metadata

Metadata is information (or data) about Data. It describes the data, including how, where, when and by whom a particular set of Data was collected, and how the Data is formatted.

Researcher

A Researcher is defined as any member of IMAS staff, any person holding an honorary research position at IMAS or a student undertaking research at IMAS.

Restricted Data

Restricted Data is Data which has limited access for one or more of the following reasons:

- The Data includes Intellectual Property which may be commercially exploited.
- The Data is Confidential. Confidential information can arise by classification in contract or at common law by the circumstances in which information was divulged and received.
- The Data is subject to Federal or State Privacy laws.
- Results derived from the Data have not been published (a Researchers right to first publication).
- The Data contains information deemed to be of a secret, confidential or sensitive nature by the Director, IMAS but is not covered by the above points.

Secure Storage

For the purposes of this document, Secure Storage refers to digital storage media and systems that are:

- housed in a data centre or storage facility utilising redundant or backup power supplies, redundant data communications connections, environmental controls (such as air conditioning and fire suppression) and security devices and employing a Disaster Recovery Plan;
- housed in a data centre meeting the requirements for Tier 3 of the TIA-942 standard (Telecommunications Industry Association);
- physically secured against unauthorised access;
- at a minimum, backed up to secondary and offsite digital storage media on a regular basis not exceeding 24 hours and one week respectively.

3. Intent

The intent of this policy is to:

- ensure the long term security, availability and maximum usability of Data;
- ensure Data (excluding Restricted Data) is released and published in the public domain in a timely and accessible manner (where appropriate) and
- ensure the appropriate management of Intellectual Property Rights in Data.

4. Scope

This policy applies to:

- All IMAS Staff & Students
- All Data Custodians

In the event of inconsistency between this policy and a uniform University of Tasmania policy, the uniform University of Tasmania policy will prevail.

5. Roles and Responsibilities

5.1. Researcher

A Researcher must:

- provide a Data Management plan for all projects in consultation with the Data Manager as required;
- ensure Data is accurate and reliable and recorded and documented (see Metadata) in a format that is adequate for verification of research results;
- ensure all research contracts or agreements adequately address ownership and licensing of Data;
- ensure all research contracts or agreements allow use and storage of Data as contemplated by this Policy or otherwise provide the Data Manager with the details of the owner or licensor of the data and any restrictions on its access or use as well as any other conditions that would prevent the use and storage of data as contemplated by this Policy;
- not use or access Restricted Data without authorisation or allow another person to use or access Restricted Data without authorisation;
- unless otherwise prohibited by contractual obligations of IMAS, submit Data and associated metadata to the Data Manager at agreed project milestones and on project completion; and
- comply with all aspects of the IMAS Data Management Policy, associated standards and guidelines and other University policies where applicable.

5.2. Data Manager

The Data Manager will:

- ensure the availability to Secure Storage for all Data;
- ensure Data is managed to meet long term access requirements;

- receive requests to withhold Data;
- provide advice and services to meet the Data access requirements of all IMAS staff, stakeholders and the wider research community;
- provide advice and services to ensure the adequate funding of internal costs associated with Data Management for externally funded projects.
- ensure Data and metadata submitted by researchers is made publicly available (excluding Restricted Data as required);
- provide timely information, standards and guidelines to Researchers on Data Management and associated issues in accordance with this policy (contained within the The IMAS Data Management Guidelines).

5.3. Data Custodian

Researchers and the Data Manager must ensure that all Data Custodians have read and agree to the terms of this Policy.

5.4. Executive Director, IMAS

The Executive Director, IMAS will provide relevant approvals as required under this policy. This responsibility may be delegated to IMAS Centre Directors.

6. Policy Matter

6.1. Data Storage and Organisation

- All Data will be stored in a Secure Storage facility.
- Where Researchers are authorised to create Data on their own personal computer, or other media that is not defined as Secure Storage, they will ensure Data is backed up to secondary media on a regular basis and backed up to Secure Storage at the earliest opportunity.
- Large sets of empirical Data or empirical Data collected on an ongoing basis over periods exceeding two years will be stored and managed using a Database Server where authorised.
- The total number of Data Management technologies used to store, organise, retrieve Data will be limited and represent the minimum number to meet all Researcher requirements.
- Data will be maintained securely to prevent unauthorised access, alteration, destruction or breaches of access.

6.2. Destruction of Data

- Unless required through overriding legislation or policy, or by contractual agreement, Data should be kept indefinitely. Destruction of IMAS Data must be approved by the Executive Director, IMAS.

6.3. Remote Access

- Unless prevented by a contractual obligation of IMAS, Data may be accessed by Researchers remotely using secure, encrypted access to the University network.

6.4. Backups

- Data backups will be in accordance with the University of Tasmania Backup and Restoration Policy. In particular:

- All Data stored in a Secure Storage facility will be backed up daily.

- Copies of all research Data backups will be stored in an offsite storage facility (a secure, second storage location other than the location of the original backup or IMAS offices) and rotated on a weekly or shorter cycle.

6.5. Data Integrity

- Researchers will implement procedures to ensure Data is maintained with the highest possible levels of integrity and accuracy.

- Researchers must keep records of Data collection and processing methodologies.

6.6. Access Control

- Where Data is stored using a Database Server, the ability to create or alter Data will be password protected with only designated data entry or maintenance staff given write access.

- Where Data is stored using a Database File, access should be restricted as much as practicably possible using password protection and/or file server user access permissions.

6.7. Data Archiving and Sharing

- The Data Manager will ensure Data and metadata submitted by researchers is made publicly available (excluding Restricted Data as required);

- A Researcher may request that publication of Data (excluding Restricted Data) collected as part of a project where they are the Principal Investigator or Co-investigator is withheld for an agreed period not exceeding 12 months after completion of the project ("Withholding Period") for the purpose of ensuring the Researcher retains the right to first publication of results obtained through examination or analysis of the Data.

- Where a Principal Investigator, Co-Investigator, the Executive Director of IMAS or the Pro-Vice Chancellor (Research) considers that Data has commercial value, any of the afore mentioned may, by written request to the Data Manager, ask that Data remain or become Restricted Data for an additional period of up to 2 years.

- Where results obtained through examination or analysis of the Data have been published or following the expiration of any agreed Withholding Period or where Data has been collected for more than two years, and Data is not categorised as Restricted Data, the Data and associated Metadata will be made available publicly by submission to a high profile, data archiving facility providing Secure Storage.

- Where Data is categorised as Restricted Data, and results obtained through examination or analysis of the Restricted Data have been published or where the Restricted Data has been collected for more than two years, and public disclosure of Metadata is not prevented by an obligation of the University of Tasmania (contractual or otherwise), Metadata for the Data will be made available publicly by submission to a high profile, data archiving facility providing Secure Storage.

- Where only part of Data belonging to a set of Data is considered Restricted Data, the remainder of the non-Restricted Data may still be considered eligible for public availability.

- For the avoidance of doubt, any contractual obligation of the University of Tasmania owed to a funding body will prevail over the disclosure requirements contained in this part 6.7.

- All reasonable attempts will be made to ensure sharing of Data will include consultation with the Principal Investigator or a Co-investigator of the project for which the Data was collected to ensure background knowledge and idiosyncrasies of the Data are taken into account when new results are established.

6.8. Metadata

- Researchers will provide Metadata for their Data meeting or exceeding the mandatory requirement of the Marine Community Profile of ISO19115.

- Researchers will provide Metadata describing the structure of datasets (schema) as defined in the IMAS Data Management Guidelines.

6.9. File formats

- Where Data is stored in Database Files or other disk files, file formats used will be documented in the public domain, defined in the IMAS Data Management Guidelines and chosen to ensure likelihood of being readable in the future.

6.10. Data Management Plan

- New project proposals must include a Data Management Plan, including Data Management costs, as defined in the IMAS Data Management Guidelines.

- Externally funded projects must include a budget item for the recoupment of internal Data Management costs and should be formulated in consultation with the Data Manager and with the use of the UTas Budget Preparation Costing Tool.

6.11. Intellectual Property

- This Policy is not intended to alter ownership of any Intellectual Property rights.

- Intellectual Property rights in Data will be managed in accordance with the University of Tasmania Intellectual Property Policy.

- Students involved in the creation of Data will be requested to enter into a Deed of Assignment in accordance with the University of Tasmania Intellectual Property Policy.

- Students required to enter into a Deed of Assignment will be given the opportunity to seek their own legal advice.

- All Data published must include an appropriate acknowledgement of the owner of that Data.

6.12. Confidentiality and Privacy

- Where possible Researchers will not negotiate funding or other agreements that unnecessarily limit or restrict disclosure of Data.

- Researchers are responsible for ensuring that the Data Manager is fully informed of the details of any conditions regarding disclosure of Data.

- Researchers are responsible for ensuring that “personal information” (as defined in the Personal Information Protection Act 2004) is not included in Data.

6.13. Design and Naming Conventions

- Databases and other datasets and associated applications will be constructed using consistent design and naming conventions as defined in the IMAS Data Management Guidelines.

7. Supporting Guidelines

7.1. IMAS Data Management Guidelines

The IMAS Data Manager will maintain an IMAS Data Management Guidelines for practical implementation of this policy through its use by all IMAS staff and students.

7.2. Relevant Legislation

- Personal Information Protection Act 2004 (Tasmania)
- Freedom of Information Act 1991 (Tasmania)
- Archives Act 1983 (Tasmania)
- Antarctic Treaty

7.3. Relevant Policies and Other Documents

- Research Accountability (UTas, section 19)
- Intellectual Property Policy (UTas)
- Data Backup and Restoration Policy (UTas)
- The Australian Code for the Responsible Conduct of Research (NHMRC)
- TIA-942 Telecommunications Infrastructure Standard for Data Centers (TIA)

8. Policy Responsibilities

Implementation	**Executive Director, IMAS**
Compliance	**All IMAS Staff and Students** **All Custodians of IMAS Data**
Monitoring and Evaluation	**IMAS Data Manager**
Development and/or Review	**IMAS Data Manager** **Nominated Staff**
Interpretation and Advice	**IMAS Data Manager**