POLICY TITLE:	Data Classification Policy

1. Purpose

The purpose of this policy is to define how data is identified, classified, labelled, and properly handled and protected in accordance with its importance and potential impact to COBLH. Data must be properly handled throughout its entire lifecycle, from creation to disposal. The importance of such information varies and therefore requires different levels of protection.

2. Scope

This policy applies to all COBLH employees, contactors, volunteers, and any other users authorised to access data stores, information in any medium, and/or information systems. In addition, third parties may be subject to this policy through contractual obligations to COBLH.

COBLH is performing its due diligence to ensure proper data classification in accordance with the following legal, regulatory, and compliance obligations:

Mandatory Obligations
Health Records and Information Privacy Act 2002 (NSW)
State Records Act 1998 (NSW)
Australian Privacy Act 1988
Voluntary Obligations
Australian Privacy Principles
Australian Protective Security Policy Framework (Policy 8)

3. Definitions and Roles

Data: For the purposes of this policy, 'Data' refers to all quantitative and qualitative pieces of information that are created, gathered, and used by COBLH to conduct its business operations. This encompasses a wide array of formats and media types, including but not limited to:

- **Electronic data:** Stored digitally on servers, computers, mobile devices, or cloud systems.
- **Physical data:** Printed or written information contained in reports, memos, notebooks, and other physical documents.
- **Intellectual data:** Knowledge embedded in the company's practices, procedures, intellectual property, and the collective expertise of its employees.

Data User: Individuals who access data at any point during its lifecycle. Anyone within the organisation can be a data user.

Data Creator: Individuals who create new data and are responsible for classifying it as it is created. The creator should assess the severity of the organisational impact if that data was compromised to efficiently decide on the classification. Anyone within the organisation can be a data creator.

Data Owner: Individuals, often department heads (or a similar role), who have direct responsibility for the data that resides and/or is primarily used within their department. The owner is accountable for classifying the data and reviewing the classification.

Data Steward: Individual responsible for data governance, practices, and requirements – essentially responsible for the entire data classification program.

Data Custodian: Individuals responsible for implementing the policies and standards (procedures) established by the data steward, including physical data storage, backup and recovery, and the operation of security and data management systems.

Data Auditor: Individual responsible for reviewing data owner's classification to determine if it aligns with regulatory or other corporate requirements and business objectives. The data auditor is also responsible for reviewing the data users' effective handling of data in accordance with the appropriate policies and procedures. Often a risk/compliance/privacy officer or similar role.

PII (Personally Identifiable Information): PII refers to any information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual.

4. Classification Levels

Level 5 Classification [Top Secret]: Applies to data that is highly sensitive and its use should be limited on a need-to-know basis. Restricted information includes trade secrets, potentially identifiable information (PII), cardholder data (credit cards), or health information. If disclosed, there would be a significant financial, legal and/or reputational damage to the organisation.

Level 4 Classification [Secret]: Applies to data that if compromised could negatively impact operations, including harming the organisation, its patients, partners, or employees. Examples include vendor contracts, employee reviews and salaries.

Level 3 Classification [Protected]: Applies to data that is intended for use within the organisation. Unauthorised external disclosure could adversely affect the organisation, its patients, employees, and business partners.

Level 2 Classification [Official: Sensitive]: Applies to data that is not openly published but can be made available via open record requests. Direct access to this data is restricted to authenticated and authorised employees. Limited data may contain redactions to protect confidential material.

Level 1 Classification [Official]: Applies to data that is readily available to the public with anonymous access.

Level 0 Classification [Unofficial]: Applies to data that is not associated with an official duty or business activity.

5. Policy

5.1 A Data Classification Steering Committee (DCSC) will be established to oversee the data classification initiative in accordance with the DCSC Charter.

5.2 Data owners (often based on departments) shall identify a data custodian, who will work with the information technology (IT) department and the DCSC to establish and enforce a Data Classification (DC) Standard for adoption by the organisation.

5.3 Each department shall identify and classify their information systems and data stores and manage access to those systems and stores in compliance with the adopted DC Standard.

5.4 Data classification will indicate the level of impact to COBLH if the confidentiality, integrity, and/or availability of the information is compromised. If the appropriate classification of an asset is not obvious (i.e. not dictated by specific laws and regulations), use the following table as a guide to effectively classify the asset. The higher the impact on the organisation, the more restrictive the classification should be.

Security Objective	**Potential Impact**		
	Low	**Moderate**	**High**
Confidentiality **Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.**	The unauthorised disclosure of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.
Integrity **Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.**	The unauthorised modification or destruction of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.
Availability **Ensuring timely and reliable access to, and use of, information.**	The disruption of access to, or use of, information or an information system could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	The disruption of access to, or use of, information or an information system could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The disruption of access to, or use of, information or an information system could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.

5.5 Departments will ensure that all non-public data is appropriately identified, including restrictions on redistributions when transmitted via email or physical mail, which are to be adopted using the DC Standard.

5.6 Data steward (with assistance from data custodians as needed) will work to establish a organisation-wide data handling training curriculum.

5.7 Data custodians will review the department's progress annually. Metrics will be presented to the steering committee, including the total number of data stores and systems identified and their associated classification status.

5.8 Data custodians will work with IT to ensure appropriate asset protection measures are in place relative to the data's classification.

5.9 The data auditor will review data classifications once per year to determine if previous data classifications can be safely downgraded to a lower classification level.

COBLH employees, contractors, volunteers, and any other users authorised to access data stores, information in any medium, and/or information systems will comply with the information asset handling standards established in the DC Standard.

6. Policy Compliance

6.1 Any exception to this policy must be approved by the DCSC in writing.

6.2 Any COBLH employees, contractors, volunteers, or authorised user discovered to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Unauthorised disclosure of regulated data, such as personally identifiable information, may lead to legal repercussions.

7. Related Documents

7.1 Information Security Policy Charter

7.2 Data Classification Standard