Kingdom of Cambodia
Nation Religion King

Ministry of Health

National Institute of Public Health

Data Governance Policy
for
Data Sharing Platform in the DAC projects
(DRAFTED)

December 2025

Document Version

Version	Date	Author	Description
1.0	December 1, 2025	NIPH's DAC project team	This is the initial version which purposely: - To establish a comprehensive and concise policy for implementing data sharing platform with an ethical, secure, storage and sharing of health-related data within Cambodia via the DAC's project's implementation.

Table of Contents

Document Version i
Table of Contents ii
Introduction and Purpose 1
Scope 1
Governance Principles 1
Roles and Responsibilities 2
Core Policy Directives 3
Data Classification and Handling 3
Data Access and Sharing 4
Data Quality 4
Data Security and Privacy 4
Data Retention and Disposal 5
Ethical Data Stewardship Principles 5
Tools for Data Sharing 5
Data Sharing Models 6
Standardised Licensing Models 6
Data Management Requirements 7
Compliance and Enforcement 7
Policy Review and Amendment 7
ANNEX 1 – LIST OF CURRENT MEMBERS OF THE DATA GOVERNANCE COMMITTEE 8
ANNEX 2 – DATA ACCESS REQUEST FORM 9

Data Governance Policy
for Data Sharing Platform in the DAC project

Introduction and Purpose

Data is a powerful tool for health policy development globally, but in Cambodia, health-related data remains underutilized. Data is typically owned by donors, project teams, or research PIs, with no common mechanism for sharing with third parties.

The Strengthening Data Analytics Capacity for Health Policy and Systems (DAC) project, supported by the China Medical Board, aims to build data analytics capacity and establish a sharing platform, with the National Institute of Public Health coordinating these efforts.

In line with the goals of the Strengthening Data Analytics Capacity for Health Policy and Systems in Cambodia (DAC) project, this policy establishes the official rules for managing all health-related data within the DAC Data Sharing Platform. Cambodia's health data is often fragmented and underutilized. The DAC project, implemented by the National Institute of Public Health (NIPH), aims to solve this by creating a collaborative platform to support evidence-based health policy.

The purpose of this policy is to ensure that all data collected, stored, processed, and shared via the DAC Data Sharing Platform is managed securely, ethically, and effectively, thereby building trust among all participating agencies.

Scope

This policy applies to:

- **All data** housed within or accessed through the DAC Data Sharing Platform, including national surveys, disease surveillance data (e.g., Malaria, HIV, TB), anonymous hospital data, and other research study data.
- **All individuals and entities** involved with the DAC project, including **Data Owners**, **Data Consumers**, **Data Stewards**, and **Data Custodians**.

Governance Principles

All data management activities under this policy will adhere to the following core principles:

- **Accountability**: Each data asset has a designated owner accountable for its management and use.
- **Transparency**: All processes and decisions regarding data sharing will be clearly documented and understandable to all stakeholders.
- **Data Integrity**: Data must be accurate, consistent, and reliable from its source to its use, ensuring it is trustworthy for analysis and policymaking.
- **Security & Privacy**: Data shall be protected against unauthorised access or misuse through robust technical and procedural controls, with special attention to sensitive and personal information.
- **Compliance**: All data activities must comply with applicable Cambodian regulations and align with global best practices (e.g., GDPR and HIPAA principles) and adapt to new national laws as they are developed.

- **Purpose Limitation & Data Minimisation**: Data will be collected and shared only for specific, legitimate purposes, and only the minimum necessary to achieve those purposes will be shared.

Roles and Responsibilities

Clear roles are established to ensure effective governance. There are three major parties considering for implementing this policy such as owners, users/consumers and data sharing hub committee. The Figure 1 is shown these three parties are involved within this data sharing and will comply to the data governance policy.

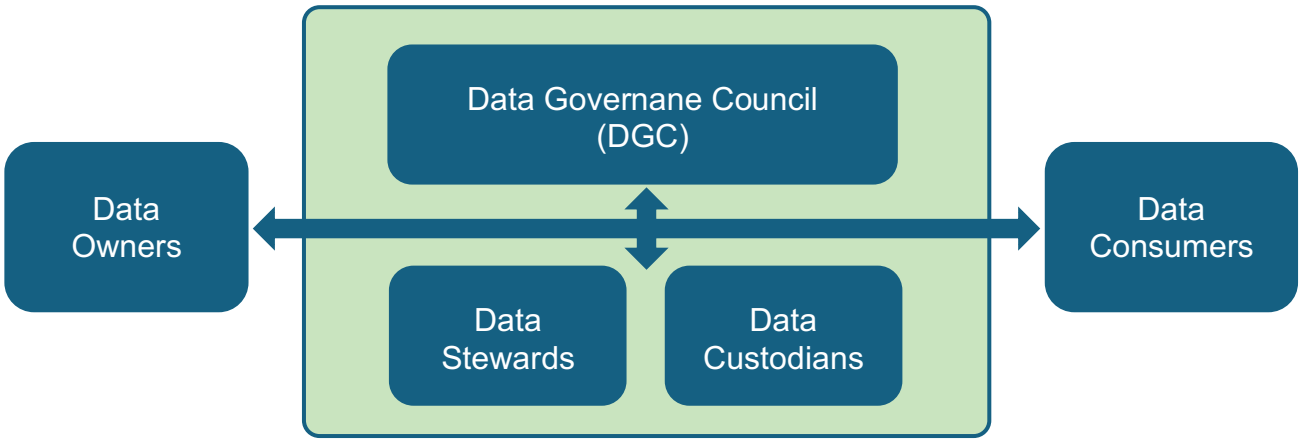

Figure 1. Three major parties are involving implementation of data governance.

- **Data Owners**: The institutions or individuals with ultimate accountability for a dataset (e.g., government agencies, research institutes, Principal Investigators). They are responsible for classifying their data and approving access requests. They must grant the authorisation of store and utilise their data by preparing and uploading their dataset for reuse under a designated license. The choice of license determines whether users need to be approved. The data owner involves the following activities:
    - Prepare and upload the dataset(s) along with supporting documents (e.g., questionnaires, protocols) to the platform.
    - Communicate with the platform's admin to finalise the documents and data-sharing
    - Approving data sharing agreements and data access requests if required.
- **Data Consumers**: Authorised users of the data, such as students, researchers, public health professionals, and policymakers. They are responsible for using the data ethically and in full compliance with data sharing agreements. The data consumer is involved in the following activities:
    - Adhering to data usage policies and data sharing agreements.
    - Submit the products generated from the dataset (e.g. technical report, manuscript, thesis) to the system.
    - Providing feedback on data usability and availability, if any.
- **Data Stewards**: The **DAC project's Data Analytics team and data curators**. They are responsible for operational management of data, including assessing and assisting with data uploads, managing data requests from data users, ensuring data quality and consistency, and ensuring compliance with policies established by Data Owners. They serve as intermediaries between data owners and technical teams:

- Receiving, assessing, and assisting data owners when uploading datasets.
- Receiving, assessing, and approving data requests from users.
- Monitoring the data to ensure it follows the request.

> ***Note:*** *For the current project, Data Steward team does not guarantee for the data quality. The data owners and data consumers are responsible in detecting any mistakes.*

- **Data Custodians**: The **technical IT team and platform administrators** responsible for the DAC Data Sharing Platform. They implement the technical security measures, manage the platform's infrastructure, and perform backups and recovery. They enforce policies and controls set by Data Owners and Data Stewards. The data owner is involved in the following activities:
  - Implementing data security measures (encryption, access controls).
  - Managing data infrastructure and storage.
  - Performing data backups and recovery.
  - Implementing data integration and transfer mechanisms.
  - Maintaining audit logs and monitoring data access.
  - Applying data masking or anonymisation techniques as required.

> ***Note:*** *Datasets are securely stored at NIPH's local sever which capacity have been upgraded to maximize the use up to 300 concurrent users.*

- **Data Governance Council (DGC)**: A committee of senior stakeholders or their representatives from NIPH, the Ministry of Health, legal teams, the Data Steward, the Data Owners, the Data Custodians and other key partners. It is responsible for strategic oversight, approving this policy, and resolving data-related conflicts. The DGC's activities involve:
  - Defining the overall data governance strategy and roadmap.
  - Approving major data policies and standards.
  - Resolving data-related conflicts or ambiguities.
  - Reviewing data governance performance and effectiveness.
  - Ensuring alignment with organisational objectives and regulatory changes.

  The list of current DGC members is in annex 1.

Core Policy Directives

Data Classification and Handling

All datasets onboarded to the DAC platform **must be classified** by the Data Owner according to their sensitivity (e.g., Public, Internal, Confidential, Restricted). The level of security, access control, and handling procedures will directly correspond to this classification.

Under the current policy, "health data" refers to datasets from surveys, public health surveillance, health services (routine data or medical records), and civil registration (e.g., births, deaths, and marriages). The Figure 2 is shown about type of health dataset.

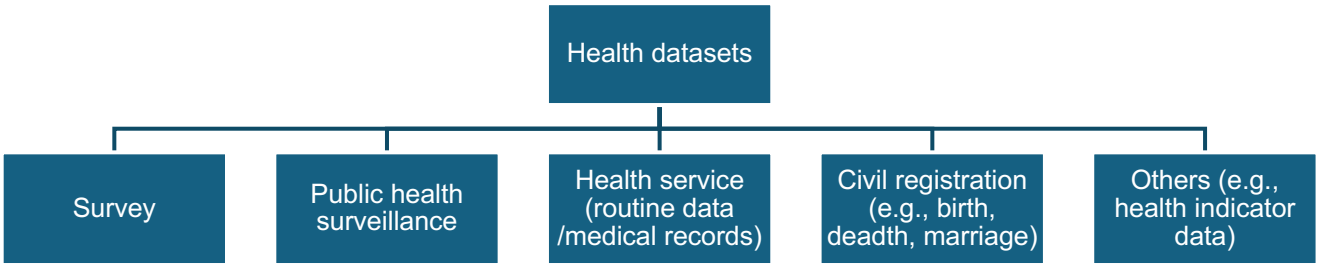

Figure 2. Type of health datasets

Data Access and Sharing

Access to data is granted based on the **"principle of least privilege,"** meaning users are granted access only to the data essential to their stated purpose.

- All requests for data access must be submitted through the formal process defined by the DGC. Please see annex 2 or visit this link to fill out the request form [link].
- All data sharing activities must be governed by a formal **Data Sharing Agreement (DSA)**, which specifies the purpose of use, limitations, and security requirements. DSAs must be approved by the Data Owner. The essential term of references (ToR) for the Data Sharing Agreement is in annex 3.
- In case of pending approval from the Data Owner within certain agreed period, which stated in Data Sharing Agreement (i.e. 40 days after requested date); the authority of approval will be automatically granted to Data Stewards or any designated individual or team by DGC.

Data Quality

Data Stewards **shall not guarantee** the quality of the data**;** they are responsible for ensuring that data owners and users check and clean the dataset**.** However, a feedback loop for reporting and resolving data quality issues is maintained to give knowledge to relevant stakeholders.

Data Security and Privacy

Data Custodians **shall implement** robust security measures, including encryption, role-based access control (RBAC), and secure data transfer mechanisms. The platform's architecture will follow the

"Privacy by Design" principle, embedding data protection into its core functionality. Where necessary, data masking or anonymisation techniques shall be applied before sharing.

We combine ethical procedure and technology (known as Privacy Enhanced Technologies – PETs) to implement privacy policies by altering or restricting the data view:

- **Data Masking and Anonymisation:** These methods protect sensitive information while still allowing it to be useful for the study. The platform achieves this by hiding certain columns, such as social security numbers or emails, from users who are not authorised to view the original data.
- **Row Filtering:** These rules control which records a user can see. Access is often based on the user's consent status or the approved purpose. This supports data minimisation and purpose specification.
- **Encryption:** A key method that converts data into a code to protect it from unauthorised access. The rules say that important data must be encrypted when stored and when being sent.

- **Using embedded data analytic tool – Jupiter Notebook:** Some datasets will be NOT allowed to download, store on user's local computer, and/or continue sharing to third-party without agreed or approved by authoriser. Therefore, the Data Users only accessible and use those datasets, they require to using the embedded data analytic tool – Jupiter Notebook on the data-sharing platform. The details instruction on how to utilisation of embedded this data analytic tool will be guided in Data Sharing Platform User guide / User manual.

Data Retention and Disposal

All data **shall be retained only as long as necessary** to fulfil its intended purpose or as required by regulations. After the retention period, data must be securely archived or permanently deleted in accordance with procedures approved by the DGC.

Ethical Data Stewardship Principles

Ethical data stewardship revolves around foundational tenets, guiding data professionals in their activities:

- Respect for Privacy and Consent: The Dataset uploaded to the platform must be anonymised, with no mechanism to link it and identify the individuals interviewed or who provided information.
- Transparency and Accountability: Organisations must clearly communicate how data is collected, used, and shared.
- Fairness and Non-Discrimination: Data systems and processes must be designed to be inclusive and unbiased.

Tools for Data Sharing

For the DAC project, the Data Sharing Platform is the tool for sharing the data. The Data Sharing Platform is a web-based application designed to store health data collected from or uploaded by stakeholders for reuse, ultimately benefiting human well-being. The platform will be processed as shown in Figure 3. This initiative is coordinated by NIPH.

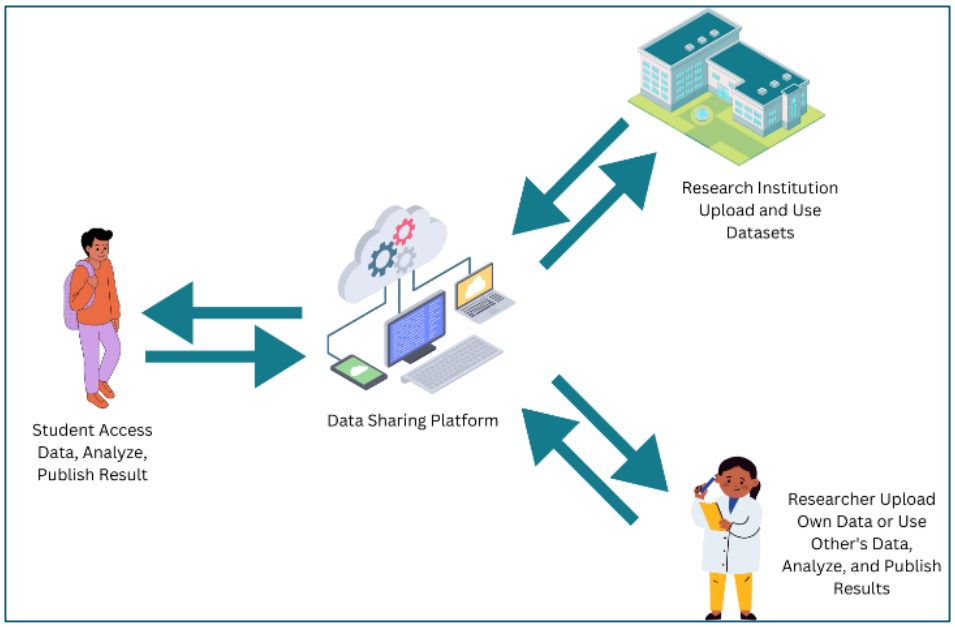

Figure 3. Data Sharing Platform's process

Data Sharing Models

The platform implements both Zero-Copy and ETL/API Models based on the licenses provided by the data owners.

- **Zero-Copy Models:** Some datasets cannot be downloaded but can be accessed by logging in to the data-sharing platform and analysing using the embedded data analytic tool – Jupiter Notebook, which is already installed and ready for use in the platform. The details instruction on how to utilisation of embedded this data analytic tool will be guided in Data Sharing Platform User guide / User manual.
- **ETL/API Models:** Some datasets can be downloaded, and users are free to copy them to their personal computers.

When uploading a dataset, the Data Owner could select one of the options: **make the data publicly available** OR **self-manage the request** (approve or deny) according to Data Sharing Agreement. The data sharing flow is shown in Figure 4 below.

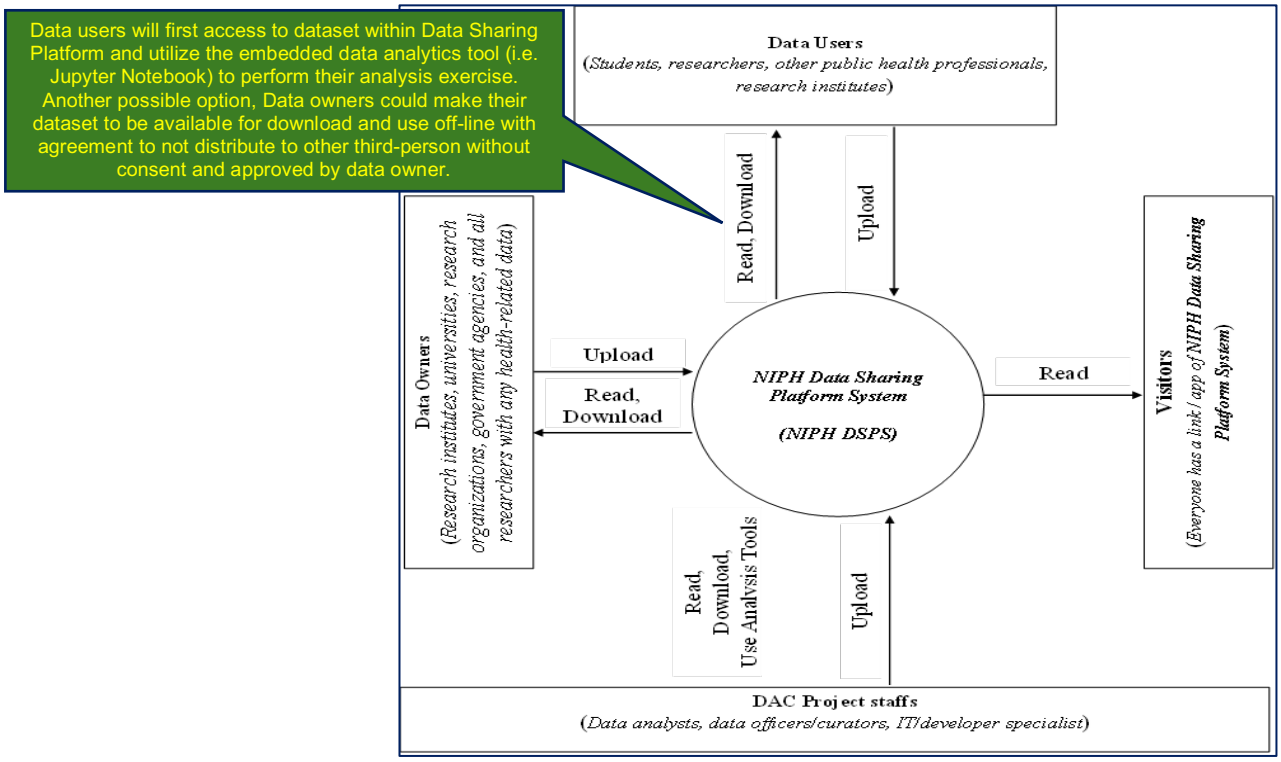

Figure 4. Data Sharing's Flow

Standardised Licensing Models

For datasets, **Creative Commons (CC) licenses** provide a standardised way to grant permission to use datasets and materials. **CC licenses** are composed of foundational elements that determine the scope of permissible use:

- **Attribution (BY):** The most permissive element, requiring users only to give credit to the creator.
- **ShareAlike (SA):** Mandates that any derivative works or adaptations must be licensed under the identical terms as the original work.
- **NonCommercial (NC):** Restricts use of the work exclusively to non-commercial purposes.

- **NoDerivatives (ND):** Requires that the work only be redistributed in its original, unaltered form.

Data Management Requirements

The platform will implement data auditing, lineage tracking, and monitoring of all processes. Those are **non-negotiable requirements** for security, compliance, and establishing accountability.

The platforms must generate detailed audit logs to answer key governance questions: "Who did what, where, and when?". These logs are generally categorised:

- Admin Activity audit logs record actions that modify configuration or metadata (e.g., changing Identity and Access Management permissions).
- Data Access audit logs record user-driven API calls that read resource configuration, metadata, or user-provided resource data.

For mature governance, audit focus must shift toward Data Access logs. While tracking administrative changes is important, compliance requires monitoring data content accessed and verifying the function of policy enforcement mechanisms. This connection between technical controls and metrics ensures accountability. Continuous monitoring helps detect anomalies and unauthorised use in real time, preventing security incidents.

Compliance and Enforcement

Compliance with this policy is mandatory for all participants in the DAC project and for all parties using the Data Sharing Platform.

- The **Data Governance Council (DGC)** is responsible for overseeing and enforcing this policy.
- The **NIPH** will conduct regular monitoring and evaluation of the project's implementation, including the framework, policy, and platform.
- Violation of this policy may result in the immediate revocation of data access privileges and other disciplinary actions as determined by the DGC.
- Regular audits will be conducted to assess adherence to this policy and report findings to the DGC.

Policy Review and Amendment

This policy is a living document. The Data Governance Council will review it annually or as needed to ensure it remains relevant and effective, taking into account new technologies, changing project needs, and the evolving legal landscape in Cambodia.

ANNEX 1 – LIST OF CURRENT MEMBERS OF THE DATA GOVERNANCE COMMITTEE

[List of current DGC's members]

ANNEX 2 – DATA ACCESS REQUEST FORM

1. Requestor Information

Field	Response
Requestor Name	
Department/Team	
Contact Email	
Contact Phone Number	
Date of Request	

2. Data and Purpose

Field	Response
Data Set Name(s) / Identifier(s) *(e.g., "Customer Transaction Log Q3 2025", "Employee Directory v2")*	
Data Owner *(If known. The individual or group responsible for the data)*	
Specific Data Fields / Elements Requested *(To ensure **least privilege**, list only the columns/fields you absolutely need.)*	
Justification & Purpose of Access *(Explain clearly and concisely why you need this data and what problem it will solve or what goal it will achieve.)*	
Anticipated Duration of Access *(e.g., 3 months, 1 year, ongoing project)*	
Please upload a support letter from your supervisor (if you will use it for thesis) or director if you will use it for your workplace. Note: It is not approved for personal use.	

3. Usage and Technical Requirements

Field	Response
Intended Use Location *(Where will the data be stored/processed? e.g., Approved Internal Server, Secure Cloud Environment)*	
Technical Format Required *(e.g., CSV, JSON, direct database connection)*	
Will the data be shared externally? *(If **Yes**, a formal **Data Sharing Agreement (DSA)** is mandatory. Please explain briefly.)*	1. Yes 2. No
If sharing externally, list the External Recipient(s) and Organization(s)	

4. Declaration and Agreement

I, the Requestor, understand and agree to the following:

- **Principle of Least Privilege:** Access will only be granted to the data elements essential for the stated purpose.
- **Formal Process:** This request must be approved by the **Data Owner** and/or the **Data Governance Committee (DGC)**.
- **Data Sharing Agreement (DSA):** If any data sharing activity is involved (internal or external), a formal DSA will be required, specifying the purpose of use, limitations, and security requirements.
- **Security:** I will adhere to all organizational security policies and treat the data with the highest level of confidentiality and care.

Field	Response
Requestor Signature	
Date	

---

5. DGC / Data Owner Approval

(To be completed by the approving authority)

Field	Response
Data Owner Name / DGC Representative	
Date of Review	
Decision	1. Approved 2. Denied
Conditions of Approval / Comments	
Signature of Approver	

ANNEX 3 – DATA SHARING AGREEMENT

TERM OF REFERENCES (ToR)
DATA SHARING AGREEMENT (DSA)
For the Data Sharing Platform in the DAC Project

This Data Sharing Agreement (the "Agreement") is made between:

1. **THE DATA OWNER: [Name of Data Owner Ministry/Institution/Organization]** (Hereinafter referred to as the "Data Owner")

AND

2. **THE DATA CONSUMER: [Name of Data Consumer Ministry/Institution/Organization]** (Hereinafter referred to as the "Data Consumer")

(The Data Owner and Data Consumer are hereinafter referred to individually as a "Party" and collectively as "the Parties")

RECITALS

WHEREAS:

A. The Parties are participants in the **Data Sharing Platform** in the DAC Project.
B. The Project utilizes a central **Data Sharing Platform** (the "Platform") as a secure hub for making data available and accessible.
C. The Data Owner granted an authorise to the Data Custodian of certain data ("the Data") made available via the Platform.
D. The Data Consumer wishes to access and use the Data via the Platform for a specific, approved purpose.

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the Parties agree as follows:

Article 1: Definitions

- **Data:** Refers to the specific dataset(s) provided by the Data Owner, to which the Data Consumer is granted access via the Platform under this Agreement.
- **Platform:** The central data hub/warehouse used for the Project, which manages data access and permissions.
- **Permitted Purpose:** The specific, pre-approved objective for which the Data Consumer is authorized to use the Data.

Article 2: Permitted Purpose

1. The Data Consumer shall only access and use the Data strictly for the following **Permitted Purpose**.
2. Any use of the Data outside of this Permitted Purpose is strictly prohibited without the prior, explicit written consent of the Data Owner.

Article 3: Data Access and Use

1. The Data Owner agrees to make the Data available to the Data Consumer via the Platform, subject to the terms of this Agreement.
2. Access to the Data is managed through the Platform. The Data Consumer shall request access through the Platform's established procedures.
3. The Data Owner (or their designated authorized team) shall review the Data Consumer's request and grant access permissions on the Platform according to the Permitted Purpose.
4. The Data Consumer shall only access the Data within the permission levels granted to them on the Platform.

Article 4: Data Consumer Obligations

The Data Consumer hereby agrees to:

1. **Use:** Use the Data *only* for the Permitted Purpose defined in Article 2.
2. **Confidentiality:** Treat the Data as confidential. The Data Consumer shall not disclose, share, publish, or disseminate the raw Data to any third party (including other departments within their own organization not covered by this Agreement) without the Data Owner's prior written consent.
3. **Security:** Implement reasonable administrative, technical, and physical safeguards to protect the Data from unauthorized access, use, or disclosure. This includes maintaining the security of their access credentials for the Platform.
4. **Re-Identification:** Not use the Data to re-identify any individual, in cases where the Data has been anonymized or de-identified.
5. **Destruction:** Upon completion of the Permitted Purpose, or upon termination of this Agreement, securely delete or destroy all copies of the Data (including derivatives) in its possession, and certify such destruction in writing to the Data Owner if requested.

Article 5: Data Owner Obligations

The Data Owner hereby agrees to:

1. **Access:** Provide the Data Consumer with access to the Data via the Platform, subject to approval as per Article 3. In case of pending approval from the Data Owner within certain agreed period, which stated in Data Sharing Agreement (i.e. 40 days after requested date); the authority of approval will be automatically granted to Data Stewards or any designated individual or team by DGC.
2. **Disclaimer:** Provide the Data on an "as-is" basis. The Data Owner makes no warranty as to the accuracy, completeness, or fitness for a particular purpose of the Data.

Article 6: Compliance with Law

1. Both Parties shall comply with all applicable laws and regulations of the Kingdom of Cambodia in relation to their activities under this Agreement.
2. This includes, but is not limited to, all relevant laws concerning data protection, privacy, intellectual property, and state secrets. If the Data includes Personal Data, it must be handled in strict accordance with Cambodia's personal data protection laws.

Article 7: Term and Termination

1. This Agreement shall commence on the date first written above and shall continue until the Permitted Purpose is fulfilled, or until terminated by either Party.
2. The Data Owner reserves the right to immediately revoke access to the Data via the Platform if the Data Consumer is in breach of any obligation under this Agreement.
3. The Data Consumer's obligations under Article 4 (Confidentiality, Security, Destruction) shall survive the termination of this Agreement.

Article 8: Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the Kingdom of Cambodia.

ACKNOWLEDGEMENT AND CONFIRMATION

The Parties, by their authorized signatories below, acknowledge that they have read, understood, and agree to be bound by the terms and conditions of this Data Sharing Agreement.

For the DATA OWNER:

[Name of Authorized Signatory] [Title of Authorized Signatory] [Ministry/Institution/Organization]

Signature: _____

Date: _____

For the DATA CONSUMER:

[Name of Authorized Signatory] [Title of Authorized Signatory] [Ministry/Institution/Organization]

Signature: _____

Date: _____