



Republic of the Philippines
Department of Science and Technology
ADVANCED SCIENCE AND TECHNOLOGY INSTITUTE



Data Policy

This Data Policy is implemented by the COARE Team, in conjunction with COARE's [Service Level Agreement \(SLA\)](#) and [Acceptable Use Policy \(AUP\)](#)

Postal Address	: Asti Bldg. UP Technology Park Complex, CP Garcia Ave., Diliman, Quezon City 1101	Tel no. : +632 8249-8500 +632 8246-9755;
Website	: www.asti.dost.gov.ph	Fax no. : +832 8246-9764
Email	Info@asti.dost.gov.ph	

Document version:
Version 9.1/ 28 April 2026

Version History

Version	Date	Description	Authors
0	22 November 2018	Draft Document	COARE Team
1	10 December 2018	Final Document	COARE Team
1.1	24 April 2019	Draft Document	COARE Team
1.2	24 May 2019	Draft Document	COARE Team
2	5 August 2019	Final Document	COARE Team
2.1	20 February 2020	Draft Document	COARE Team
2.2	2 June 2020	Draft Document	COARE Team
2.3	24 June 2020	Draft Document	COARE Team
3	7 August 2020	Final Document	COARE Team
3.1	25 May 2021	Draft Document	COARE Team
3.2	7 June 2021	Draft Document	COARE Team
4	14 June 2021	Final Document	COARE Team
4.1	15 June 2022	Draft Document	COARE Team
4.2	11 July 2022	Draft Document	COARE Team
5	22 July 2022	Final Document	COARE Team
6	8 August 2023	Final Document	COARE Team
7	19 March 2024	Draft Document	COARE Team
7.1	30 April 2024	Final Document	COARE Team
8	18 March 2025	Draft Document	COARE Team
8.1	1 July 2025	Final Document	COARE Team
9	21 April 2026	Draft Document	COARE Team
9.1	28 April 2026	Final Document	COARE Team

Contents

1. About this Document.....	4
2. Definition of Terms	4
3. Scope and Applicability	7
4. COARE Data Policy.....	7

1. About this Document

The Computing and Archiving Research Environment (COARE) is one of the services offered by the Department of Science and Technology – Advanced Science and Technology Institute (DOST-ASTI) that provides computational and storage resources for research initiatives that address or contribute to the thematic areas under DOST's Harmonized National Research and Development Agenda (HNRDA) 2022-2028. COARE serves as a national-level supercomputing facility that provides platforms for data storage, analysis, and sharing through the following services: High-Performance Computing (HPC), Science Cloud, and Data Archiving.

This document outlines all the data-related policies and procedures concerning COARE and is implemented to ensure that all data generated, analyzed, processed, and stored in and through COARE will only be related to research and other scientific studies. These data should comply with the existing policies implemented by the DOST and other applicable laws and regulations of the Republic of the Philippines. This document also discusses the responsibilities of the COARE Team in managing all data stored through COARE services.

2. Definition of Terms

The following terms will be relevant as reference in understanding this SLA:

- 2.1 Accounts:** This comprises the credentials and/or other applicable requirements that enable a COARE user to access COARE services. Account credentials include a unique username (following the format: "firstname.lastname"), password (if necessary), and other relevant information.
- 2.2 Active User:** Unexpired COARE Account
- 2.3 COARE:** An encompassing term that refers to the services, team, end users, IT infrastructure, facility, etc.
- 2.4 COARE Services:** This refers to the standard services that COARE offers, namely: High-Performance Computing (HPC), Science Cloud, and Data Archiving.
- 2.5 COARE Service Level:** The group of people that maintains COARE's operations, handles the provision of COARE services and provides support to COARE Users. The COARE Team is composed of four (4) levels of support:
 - 2.5.1 1st Level – L1 Support:** Service Desk
 - 2.5.2 2nd Level – L2 Support:** Technical Operations Team and Software Development Team
 - 2.5.3 3rd Level – L3 Support:** Technical Operations Team Lead and Software Development Team Lead

2.5.4 4th Level – L4 Support: COARE Management

- 2.6 COARE Users:** Users who have been given access to COARE, have been provided with COARE resources, and/or use the COARE Services (HPC, Science Cloud and Data Archiving).
- 2.7 [COARE Wiki](#):** A platform for COARE users as their reference to any pertinent information related to COARE and any COARE services. Information such as the COARE Service Catalog, procedures in availing COARE services, Frequently Asked Questions (FAQs), templates, forms, and other relevant guides can be found in COARE Wiki.
- 2.8 Confidential Data:** Data classified as Confidential is not shared and is not included in the list of datasets that can be accessed by End Users. Confidential Data will not be covered by the [COARE End Users License Agreement \(EULA\)](#).
- 2.9 Data Access Request:** The process of granting or denying access to the Internal and Private dataset published in the [COARE Data Catalog](#). Data Access Request may be executed by filling-out the Data Access Request Form (which will be displayed upon clicking the “Download” button.)
- 2.10 Data Archiving:** A COARE service that provides a repository with redundancy that aims to accommodate various storage requirements of COARE users and to enable storing of data on a short-term or long-term basis. This does not include storage used in HPC (home and scratch) and Science Cloud (cloud disk storage).
- 2.11 Data Archiving via [Data Catalog](#):** A web-based research repository under COARE’s Data Archiving service that provides access to a collection of scientific datasets produced by various research findings.
- 2.12 Data Catalog Data Owner:** A COARE User who is the rightful owner of a specific dataset in the COARE Data Catalog. Data Owners have the right to approve or reject Data Access Requests from End Users.
- 2.13 Data Catalog End User:** A COARE user who has authorized access to datasets published in the COARE Data Catalog.
- 2.14 Data Classification:** This refers to the Data Catalog’s data classification categories/levels: Public, Private, Confidential.
- 2.15 Data Protection Officer (DPO):** A DPO is/are individual(s) designated to ensure an organization’s compliance with the [Data Privacy Act of 2012](#), its IRR, issuances by the National Privacy Commission (NPC), and other applicable laws and regulations relating to privacy and data protection.
- 2.16 [Data Purging](#):** Deletion of COARE user data stored in either or both the home or scratch directories or other location(s) within the applicable COARE service(s).
- 2.17 Data Subject:** A user whose personal information is processed.

- 2.18 HPC:** The COARE HPC Service consists of a cluster of compute and storage servers to allow high-speed and resource-intensive computations and processing of large datasets.
- 2.19 Home Directory (/home):** The storage option recommended for storage of application source codes, user program binaries, user directories, user directories, user directories, modules directories, and small-sized active datasets.
- 2.20 Internal Data:** All data classified as Internal belongs exclusively to Data Owner from DOST-ASTI and is made available in a “View Only” mode, by default, to all DOST-ASTI personnel. Access to datasets in this classification requires a request for data access submitted to the rightful DOST-ASTI Data Owner/s.
- 2.21 Job:** A job is an allocation of resources assigned to a COARE HPC user for a specified amount of time.
- 2.22 Job Script:** This is a script created by users to submit jobs to the HPC. It contains job information and instructions on how the job will run in COARE.
- 2.23 Long term data storage in HPC:** Storage of HPC data within the timeframe of the HPC user’s account validity.
- 2.24 Metadata:** The metadata contains the information (i.e., title, description, organization details, etc.) pertaining to the dataset.
- 2.25 Personal Information:** Any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
- 2.26 Public Data:** All data classified as Public are accessible and are available for download to anyone who has a registered account in the Data Catalog.
- 2.27 Private Data:** All data classified as Private belongs to the rightful Data Owner who chooses to share their data with only a select few. End Users are only able to download Private datasets if they have a registered account, and their data access request has been approved.
- 2.28 Science Cloud:** A COARE service that enables the provision of virtual machines (VM) for cloud-based applications and computing.
- 2.29 Science Cloud Dashboard (OpenStack):** A web-based interface to manage virtualized resources in the Science Cloud.
- 2.30 Science Cloud Project:** A foundational, organized container in Science Cloud used to isolate compute resources (CPU, memory, disk and object storage, network, user/user-group access, etc.) for a user or resource partner.
- 2.31 Scratch Directories (/scratch):** These directories are intended for the storage of the user’s running jobs, especially for execution of heavy I/O operations.
- 2.32 User Portal:** The main platform that the COARE Team uses to carry out service request management and incident management processes. All

service requests and incidents concerning any COARE services must be logged through a ticket in the [COARE User Portal](#).

3. Scope and Applicability

The COARE Data Policy applies to all COARE Users (both active and inactive).

4. COARE Data Policy

Data Related Policies for COARE HPC Service

- a. All HPC clusters (home & scratch directory) should only contain data on research and development (R&D) work and other scientific research.
- b. Both the home and scratch directories should not be used for long-term storage.
- c. The storage offered through COARE Services should not be intended as the users' sole storage of their files/data. Users are strongly encouraged to maintain an external copy of all their data and to refrain from using COARE as their only repository for the files critical to their research.
- d. Users should be responsible when deleting their files. The COARE Team does not guarantee recovery of files that have already been deleted.
- e. The COARE Team may forego obtaining permission from users to access users' files if accessing is crucial to troubleshooting an error, debugging jobs, or resolving incidents that are tagged with a Critical or High priority level. At the same time, the COARE Team ensures non-disclosure/privacy or integrity of the affected user's data.
- f. Information on users' jobs (CPU, memory, disk I/O, job script, job runtime, etc.) will be regularly collected by the COARE Team as reference in preparing capacity, availability, upgrade, and maintenance plans for COARE services.
- g. The COARE Team will conduct storage audit activities regularly to maintain an efficient shared environment, based on COARE's resource utilization threshold.
- h. Once a user's account has expired, the COARE Team will issue a notice of purging of files upon the account's expiry. Users with expired accounts will be given ninety (90) days to back up their files upon expiry of their account. On the 90-day mark, the COARE Team will proceed with the deletion of ALL files of expired accounts.
- i. Users have the sole responsibility for all actions that they perform involving their HPC account. If contents stored through the COARE have been proven to be malicious, illegal, and/or is in violation of existing laws and policies, the COARE Team will not be, in any way or form, required to be subject to investigation.

Data Related Policies for COARE Science Cloud Service

- a. COARE Team may forego obtaining permission from users to access provisioned Science Cloud resources if access is crucial to troubleshooting an error, debugging jobs, or resolving incidents that are tagged with a Critical or High priority level. At the same time, the COARE Team ensures non-disclosure/privacy or integrity of the affected user's data.
- b. Users are encouraged to [secure their own backup](#) through their dashboard on the Science Cloud, performing volume snapshots and volume backups regularly to secure their data.
- c. The COARE Team will not be liable for retrieving files or data that have been deleted due to users' negligence (e.g., weak passwords, insecure SSH authentication methods, etc.) and/or compromised through hacking, worms, etc.
- d. The COARE Team will be conducting storage audit activities regularly as part of COARE's maintenance activities to manage the capacity and maintain the availability of COARE's resources. Data purging may be performed guided by the [Purging Guidelines](#) implemented by the COARE Team.
- e. Users have the sole responsibility for all actions that they perform involving the Science Cloud resources provided to them. If content published through the COARE has been proven to be malicious, illegal, and/or is in violation of existing laws and policies, the COARE Team will not be, in any way or form, required to be subject to investigation.

Data Related Policies on the usage of the COARE Data Archiving Service

- I. The COARE Data Archiving service is intended for long-term data storage and distribution. Users are encouraged to treat Data Archiving Services as one of their alternative storage options and to be responsible for securing a copy of their data regularly.
- II. **Specific data-related policies concerning the Data Catalog**
 - a. Only datasets that are under the Public and Private data classification levels are publicly searchable and viewable, and the metadata of these data classification levels are indexed in the Data Catalog and presented at the [Data Classification Guidelines](#).
 - b. Metadata of datasets tagged as Confidential are not shared and are not included in the COARE Data Catalog's list of datasets that can be accessed by End Users.
- III. **Specific Data-related policies concerning the Data Catalog (Data Owners)**
 - a. Prior to uploading and storing their datasets in the Data Catalog, Data Owners should categorize their datasets according to the appropriate data classification levels: Public, Private, or Confidential. The COARE's Data

Classification Guidelines will be the main reference for Data Owners in identifying the distinctions among each data classification level.

- b. Data Owners who intend to protect datasets, modify permission levels for shared databases, or publish datasets without making them publicly accessible may refer to the [Data Classification Guidelines](#) for appropriate options on securing and storing their data.
- c. Data Owners are required to submit the metadata of their dataset and must refer to the metadata format provided by the COARE Team for describing dataset information and files within the dataset. Metadata will be used in populating Metadata management and searching features of the Data Catalog. Submission of a preview of the Data Owner's dataset is optional.
- d. Data Owners are only allowed to upload datasets that are appropriate for research and development (R&D) work and other scientific studies. Storing data that is unrelated to research (e.g., documents, viruses, and media files such as movies, music, and photos that are not related to research) is not allowed.
- e. Data Owners, who have uploaded specific datasets in the Data Catalog, must regularly check their e-mail for Data Access Requests submitted for their approval. Data Owners hold exclusive rights over specific datasets in the Data Catalog. Thus, it is their duty to grant or deny Data Access Request Forms accomplished and submitted by end users.

IV. Specific data-related policies concerning the Data Catalog (End User)

- a. End Users who want to download any dataset published in the Data Catalog must first register for an account. To start accessing and downloading datasets, End Users must be logged in with their registered Data Catalog account.
- b. End Users are eligible to download public datasets in the Data Catalog without the need to accomplish the Data Catalog Data Access Request Form.
- c. End Users who want to download datasets classified as Private may accomplish and submit the Data Access Request Form.
- d. End Users, prior to downloading any dataset from the Data Catalog, must duly comply with and agree to the [End User License Agreement \(EULA\)](#) provided by the COARE Team, as well as with any additional license agreements provided by the Data Owners.
- e. Access to private datasets in the Data Catalog is only available for seven (7) days. After access to these datasets has expired, the End User must complete the Data Catalog Access Request Form to obtain access to the datasets again.

Other Data Related Policies

I. Data Sharing

- a. While users can utilize COARE services and choose to store their data privately, the COARE Team encourages users to engage in data sharing by publishing their data publicly through the Data Catalog.
- b. All datasets tagged as “Public” will be shared and made available through the Data Catalog.
- c. Datasets with Private data classification levels may be shared following permission levels set by Data Owners.
- d. Users may choose to share their data with other COARE users through access and permission privileges.
- e. While selected datasets have been approved for sharing, these datasets downloaded from the Data Catalog cannot be modified, reproduced, distributed, commercially exploited, or re-uploaded in other data platforms, since these datasets are the exclusive property of rightful Data Owners (See Section 5 in [COARE End User License Agreement](#)).

II. Data Citation

- a. All datasets in the Data Catalog have ownership and intellectual property rights that belong to rightful Data Owners. Thus, all datasets downloaded shall reflect the Data Catalog and the rightful Data Owner as dataset sources (See Section 4.2 in [COARE End User License Agreement](#)).
- b. Any utilization (i.e., in theses, research, journal articles or any academic paper/s) of any datasets downloaded from the Data Catalog requires attribution of the rightful Data Owner through proper citations. (See Section 4.3 in [COARE End User License Agreement](#)).
- c. A COARE user, upon the utilization of any of the COARE Services and the data results, analyses, and processes generated from these services, must attribute the DOST-ASTI and the COARE in theses, research, journal articles, academic paper/s, or any related content.

III. Data Privacy

- a. Personal information including full name and contact details (email address) will be collected from anyone who wants to access COARE services. All personal information submitted to the COARE Team will be used for the provision of COARE services and for reports submitted to DOST and other monitoring agencies.
- b. All COARE users are data subjects whose personal information are protected by [Republic Act 10173 \(Data Privacy Act of 2012\)](#). The processing (collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction) of all

personal information of all COARE users (whether potential, active, or inactive) will only be conducted in adherence to [R.A. 10173](#).

- c. All personal information of users should be submitted to and updated with the COARE Team only through official platforms: e-mail (gridops@asti.dost.gov.ph, coareservicedesk@asti.dost.gov.ph, the [COARE User Portal](#), the [COARE Data Catalog](#), and/or official forms.
- d. Other personal information not belonging to the COARE user (such as, but not limited to, full name of immediate supervisor and their contact details, full name of colleagues and their contact details) will also be processed according to the provisions of the [R.A. 10173](#).
- e. The COARE Team shall coordinate closely with the DOST-ASTI's designated Data Protection Officer (DPO) to implement data privacy measures in compliance with [R.A. 10173](#).