# Computational Biology Division

## Data Access and Compute Resource Access/Usage Policy

[version 1.0.0.]

**Department:** Computational Biology Division

**Policy Owner:** Head of division

**Responsible for Update:** Head of division

**Review Cycle:** Yearly, or as required

**Prior update:** New policy formalizing departmental data and compute resource access usage

**Current update:** September 2024

**Approved by:** Computational Biology Division's head of division, September 2024

**Enquiries:** cbio-admin@uct.ac.za

# 1. Context

Computational Biology (CBIO) is a division of the Integrative Biomedical Sciences department located in the Faculty of Health Sciences, University of Cape Town (UCT). CBIO is committed to protecting the privacy and confidentiality of the human genetic and phenotypic data it manages. All staff students, and collaborators working with CBIO-controlled data must comply with this policy.

This policy's contents are defined by CBIO's leadership and are intended to drive the more detailed steps described in CBIO Data Processes and Procedures.

# 2. Objective

The purpose of this policy is to be the main point of reference for all CBIO data-related activities and procedures that are important for CBIO members and collaborators to follow and be made aware of. The policy also includes references to other external data policies (e.g. POPIA; UCT Data Policy), that may influence or dictate activities within the division. As such, this policy should help guide CBIO staff, students, and collaborators to understand and uphold best practices in data management and data protection; IT administration and security; ethical conduct when working with sensitive research data; and understand how to manage and report breaches in data security.

# 3. Applicable to

This policy applies to all CBIO staff, students, collaborators, and any other individual with access to CBIO-controlled data and compute resources.

# 4. Definitions

| Term | Definition |
|---|---|
| Breaches | Breaches include:<br>• Non-compliance with this policy and any procedures relating to it;<br>• Contraventions of any data protection legislation such as the POPIA.<br>• Disclosure of any sensitive data: personal or organizational |
| Compromise | Unintended deletion, exposure, corruption or misrepresentation of data |
| IT Security | Practices aimed at protecting data and systems from vulnerabilities, including the misuse of access privileges. |
| Ethical Conduct | Adherence to professional standards of integrity, confidentiality, and honesty in handling sensitive data. |
| POPIA | The Protection of Personal Information Act 4 of 2013 and its regulations. |
| Processing | Any operation or activity or any set of operations concerning personal information and data access, including:<br>• Collecting, receiving, recording, organising, collating, storing, updating or modifying, retrieving, altering, consulting, or using;<br>• Disseminating by means of transmission, distributing, or making available in any other form; or<br>• Merging, linking, restricting, degrading, erasing, or destroying personal information. |
| CBIO-controlled | Any datasets and information stored on CBIO owned infrastructure. |

| | |
|---|---|
| Data | Information collected or stored in all digital formats, used for research; administration; calculation; examination; processing and reasoning. |

# 5. Scope

This policy applies to all data accessed via CBIO systems, including administrative, human genetic, phenotypic, pathogen, microbiome and associated research data. It covers any action involving the collection, storage, processing, sharing, or destruction of data and includes project-specific guidelines and restrictions.

Access to CBIO-controlled data and compute resources is contingent upon signing the CBIO Data Protection and Ethical Conduct Declaration. This declaration must be signed annually.

# 6. Policy

*6.1. No individual will be given access to CBIO-controlled data unless they have signed the **Data Protection and Ethical Conduct Declaration** within the past 12 months. Failure to sign or renew the declaration within the given 12-month period could result in access to any CBIO-controlled data and compute resource being revoked.*

*6.2. Data and compute resource access is contingent upon a valid CBIO based **Data Management Plan** existing for the project related tasks to be undertaken.*

*6.3. Any individual granted access to CBIO-controlled data or compute resources, will take all reasonable measures to protect it from misuse and inappropriate access*

*6.4. Any individual that has access to any CBIO-controlled data or compute resources that were not explicitly granted access rights to these resources via the team lead or project owner, should refrain from accessing these resources and notify CBIO immediately (cbio-admin@uct.ac.za)*

*6.5. Users will ensure that all data access limitations and requirements as set out by the data owner are adhered to. This includes prompt deletion of datasets where time limitations have expired.*

*6.6. Will comply with this policy and all relevant policies relating to the access to data and compute resources. See section 7 Related Policies and Guidelines*

*6.7. Any suspected or known vulnerability and/or data / system breach is to be promptly reported to cbio-admin@uct.ac.za.*

# 7. Related Policies and Guidelines

This section provides reference to additional policies and guidelines that completement and support the objectives of this CBIO data access and compute resource access/usage policy. Adherence to these related documents is essential to ensure comprehensive compliance and alignment with organizational standards.

**University of Cape Town data protection policies**

https://uct.ac.za/administration/policies

**UCT Information and communication Technology Services**:

https://icts.uct.ac.za/about-icts/policies-and-guidelines

--end of policy--