ARCS-5:
Data Retention and Destruction

Version 1.0.1

THE UNIVERSITY OF BRITISH COLUMBIA

Data Retention and Destruction

1. Introduction

1.1 Purpose

UBC Advanced Research Computing (ARC) must implement appropriate data retention and destruction standards to safeguard data and backups stored on systems managed by ARC. This standard defines how data stored on **ARC Systems** is either retained or destroyed. It defines what protocols are to be employed in each case and what timelines must be followed when considering which data should be retained or destroyed.

1.2 Scope

This standard applies to all **ARC Systems**. This standard does not alter the responsibilities set out in *UBC Policy SC6 Scholarly Integrity* and *UBC Policy LR2: Research*.

1.3 Exceptions

Exceptions to this Standard are for approved purposes only. Approval is contingent upon information provided by a formal request and an assessment by ARC. Any approved exceptions must be re-evaluated regularly or whenever a material change to the control environment occurs.

2. Data Retention

2.1 Data Retention

Data on **ARC Systems** is only retained during the duration of allocated projects. This includes archival storage which must also be allocated. Once the allocation has ended, data must be deleted, sanitized, or destroyed within the time limit specified by the terms of service for that ARC system.

3. Data Deletion

3.1 Data Deletion – Active Storage

Data stored in **ARC Systems** may be deleted through the normal system tools provided by the client operating system. No additional measures are required to clear data from active storage as physical media is subject to additional sanitization (see section 4). If the **Data Owner** requires additional protections for data stored on **ARC Systems**, it is their responsibility to employ encryption at rest for this data.

3.2 Data Deletion – Backup Storage

No facility exists to request the deletion of specific data stored in backups of **ARC Systems**. Data stored on backup systems is deleted automatically, over time according to the applicable backup schedule, as new backups overwrite the old information.

4. Data Destruction

4.1 Media Sanitization

Any physical media components of **ARC Systems** to be repurposed or reused must be sanitized prior to reuse. Sanitization should follow either US DoD 5220.22-M (7 passes) or RCMP TSSIT OPS-II (7 passes).

4.2 Media Destruction

All physical media components of **ARC Systems** that are to be removed from ARC control, or decommissioned; and that cannot be sanitized and reused; must be physically destroyed to render the media unreadable. Refer to *UBC Information Security Standard #08 Destruction of UBC Electronic Information*.

4.3 Documentation

ARC must maintain a record of any media that has been repurposed or destroyed, including the system from which it was last in service, and the method of destruction for a period of at least one (1) year from the date of destruction.

5. Responsibility

5.1 Data Owner

The **Data Owner** is responsible for the complete lifecycle of their data. The **Data Owner** is responsible to ensure that storage of this data on **ARC Systems**, in compliance with this standard, is consistent and remains in compliance with all applicable institutional policies, regulations, laws, ethics requirements, and agreements.

5.2 ARC Systems Team

The **ARC Systems Team** is responsible for ensuring **ARC Systems** are managed in compliance with this standard.

5.3 UBC IT

UBC IT is responsible for the security of some backup storage systems where data from **ARC Systems** may be retained in accordance with all UBC information security standards including *UBC Information Security Standard #08 Destruction of UBC Electronic Information*.

Effective Date:	28-AUG-2019		
First Released:	28-AUG-2019		
Last Revised:	17-MAR-2023		
Last Reviewed:	22-MAR-2023		
Approved By:	ARC Management Team		
	22-MAR-2023		