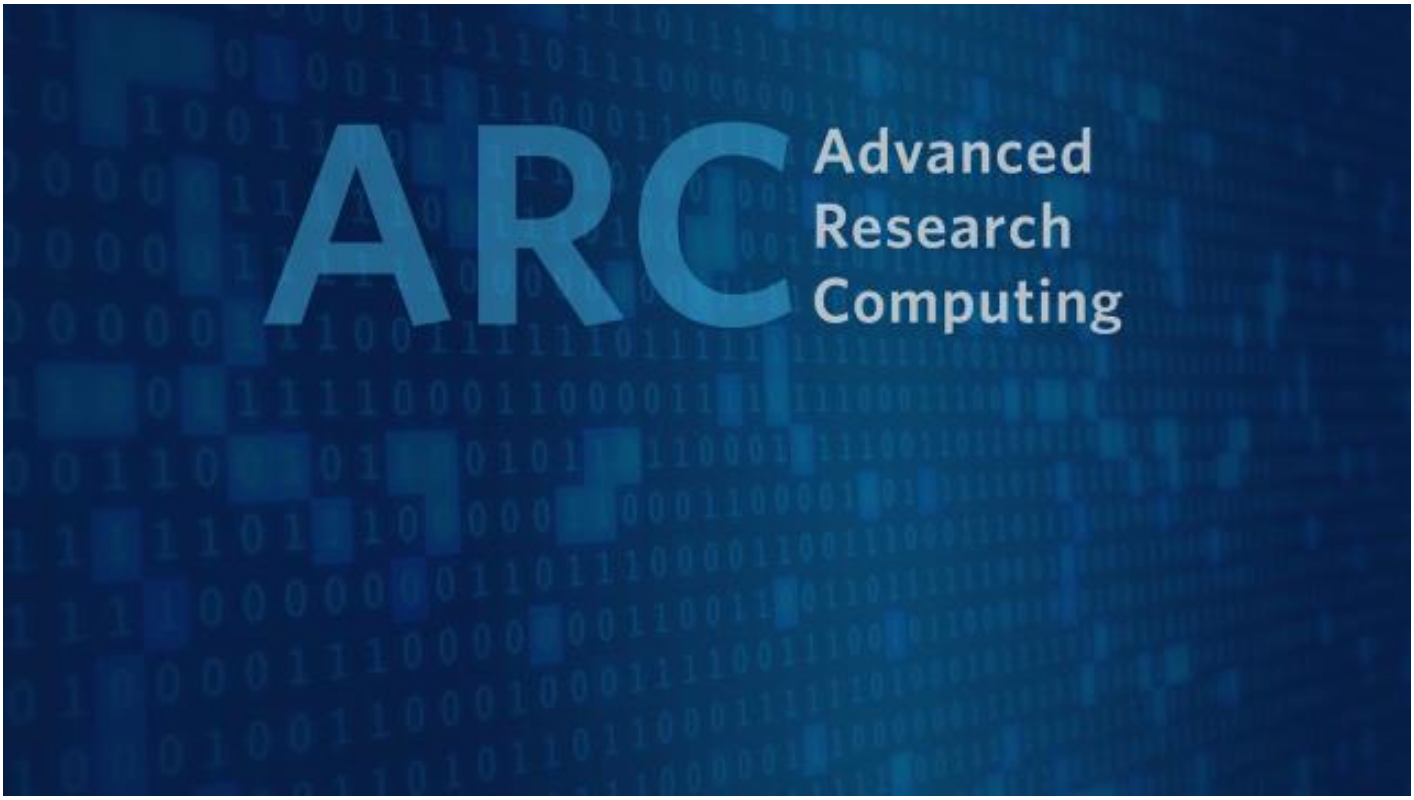
ARCS-22:
System Access Control

Version 1.2.0



THE UNIVERSITY OF BRITISH COLUMBIA

System Access Control

1. Introduction

1.1 Purpose

This standard defines access control requirements for UBC Advanced Research Computing (ARC) systems to manage access of **Users** and **ARC Systems Administrators**.

1.2 Scope

This standard applies to all **Users** and **ARC Systems Administrators** of ARC Managed Systems.

1.3 Governing Policy

UBC Policy SC14 Acceptable Use and Security of UBC Electronic Information and Systems and associated information security standards. For more information, please refer to: https://cio.ubc.ca/information-security/policy-and-standards/information-security-policy-standards-and-resources.

2. Standard

2.1 User Access

All systems must follow the principle of **Least Privilege** approach when granting **Users** access. Access must be integrated with UBC's **Campus Wide Login (CWL)** system except where specified in *Appendix A: ARC Managed Platforms*.

Users' authentication must require multi-factor authentication (e.g. **Enhanced CWL**) wherever possible.

Users access must be terminated from a system as specified in *Appendix A: ARC Managed Platforms*.

Users access must be suspended if they violate the associated *Terms of Service* (see *Appendix A: ARC Managed Platforms*) and as specified in section 2.4 of this standard.

2.2 Administrative Access

ARC Systems Administrators must not access any **Users** data, except for the purpose of maintaining system integrity or to the extent needed to provide support requested by **Users** through ARC Support.

2.3 Account Suspension and Reactivation

Accounts may be automatically suspended if:

- The **User's** CWL is no longer active or has been suspended.
- The account is no longer associated with an active allocation/project.

ARC Support has the ability to suspend, terminate, and reactivate accounts as necessary. Accounts must be suspended when:

- The **User's** credentials are compromised or suspected to have been compromised (see section 2.4).
- Requested by the **User**.
- Requested by the associated **Allocation Owner** or **Project Owner**.
- The user fails to comply with the associated Terms of Service (see *Appendix A: ARC Managed Platforms*) or based on any of the criteria in section 2.4 of this standard.

Users with accounts suspended due to one of the above measures may contact **ARC Support** to request reactivation.

All **Users** associated with an allocation/project must also be suspended if the owner of the allocation/project's user account has been suspended, and has not been reactivated within 90 days. The **Allocation Owner** or **Project Owner** must reactivate their account before any other **Users** account(s) will be reactivated by **ARC Support**.

Should the ownership of the allocation/project need to be changed, the service-specific procedures listed in *Appendix A: ARC Managed Platforms* must be followed.

2.4 Compromised Accounts

User accounts suspected or found to be compromised will be suspended until the account issue has been resolved. Compromised accounts include, but are not limited to:

- Credentials likely breached
- Credential sharing
- Known use of weak passwords
- Detection of associated malware activity
- Use of a shared email address

Users who suspect their accounts may be compromised must contact **ARC Support** immediately.

2.5 Securing User Accounts

All **User Accounts** must be secured in accordance with UBC's *Information Security Standard M4: Securing User Accounts*.

All **User Accounts** must follow the requirements in UBC's *Information Security Standard U2 Password and Passphrase Protection*.

3. Responsible, Accountable, and Consulted

Task	R	A	C
User Education, training and awareness of the access controls for the platform.	**ARC Support**	**ARC Service Owner**	**SRT**
Account Management, including provisioning and de-provisioning.	**ARC Service Owner**	**ARC Service Owner**	**SRT**

Suspension and Re-Activation of accounts as outline in section 2.5	**ARC Support**	**ARC Service Owner**	

3.1 All Users

- Must not share any access credentials with any other individual.
- Must notify **ARC Support** in addition to following regular institutional and associated procedures immediately in the event of any suspected information security or privacy breach, in the event their access credentials are compromised or believed to have been compromised, or any other security incident.
- Must read, understand, and agree to the associated Terms of Service (see *Appendix A: ARC Managed Platforms*) before using the service.

4. References

UBC ARC Glossary of Standards

UBC ARC Glossary of Terms

UBC Information Security Standard M4 Securing User Accounts

UBC Information Security Standard U2 Password and Passphrase Protection

Effective Date:	01-SEP-2020		
First Released:	01-SEP-2020		
Last Revised:	17-MAR-2023		
Last Reviewed:	22-MAR-2023		
Approved By:	ARC Management Team		
	22-MAR-2023		

Appendix A: ARC Managed Platforms

The following platforms are managed by ARC and their associated access control requirements are specified below.

1. UBC ARC REDCap

1.1 Scope

This includes the associated **UBC ARC REDCap Flex** production, pre-production, and development; application and database instances.

1.2 Terms of Service

The **UBC ARC REDCap** platform Terms of Service are published on the ARC web site and subject to change without notice:

https://arc.ubc.ca/sites/arc.ubc.ca/files/documents/TOS-REDCap-TermsOfService.pdf

1.3 Access Controls

All **Users** require an **Enhanced CWL** in order to access the platform.

If a **User** changes their **CWL** for any reason, they must notify **ARC REDCap Support** to ensure continued access.

1.4 Ownership Changes

If the **Project Owner** responsible for a project is no longer connected to that project or research group, ownership may be transferred to another eligible **User** by **ARC Support** as follows: If the project is part of a research study, the replacement **Project Owner** must be listed as part of the study team and approved by the **Principal Investigator** of that study. If the project is part of a non-research project (e.g. research lab), the new **Project Owner** must be a **Primary User** and approved by the **Administrative Head of Unit** for that project or research lab.

2. UBC ARC Sockeye

2.1 Scope

This includes the HPC platform and associated storage identified as **UBC ARC Sockeye**.

2.2 Terms of Service

The **UBC ARC Sockeye** platform Terms of Service are published on the ARC web site and subject to change without notice:

https://arc.ubc.ca/sites/arc.ubc.ca/files/documents/TOS-Sockeye-TermsOfService.pdf

2.3 Access Controls

All **Users** require an **Enhanced CWL** in order to access the platform.

If a **User** changes their **CWL** for any reason, they must notify **ARC Support** to ensure continued access.

2.4 Ownership Changes

If the **Allocation Owner** responsible for an allocation is no longer connected to that project or research group and has not already specified another **Eligible UBC Researcher** to become the new **Allocation Owner**; ownership may be transferred to another **Eligible UBC Researcher** by **ARC Support** when approved by the associated **Administrative Head of Unit**.

3. UBC ARC Chinook

3.1 Scope

This includes the object storage platform and identified as **UBC ARC Chinook**.

3.2 Terms of Service

The **UBC ARC Chinook** platform terms of service are published on the ARC web site and subject to change without notice:

https://arc.ubc.ca/sites/arc.ubc.ca/files/documents/TOS-Chinook-TermsOfService.pdf

3.3 Access Controls

At a minimum, the **Allocation Owner** and any delegated **Users** require an **Enhanced CWL** in order to access the platform.

Users accessing the **UBC ARC Chinook** platform using their **CWL** must notify **ARC Support** if they change their **CWL** for any reason, to ensure continued access.

3.3.1 Allocations with High or Very High Risk Information

In any case where High or Very High Risk information is to be stored as part of an allocation: All **Users** require an **Enhanced CWL** in order to access the platform. The **Allocation Owner** must not be granted permission to manage data sharing to users directly. The **Allocation Owner** must request **Users** to be added to the allocation by **ARC Support**.

3.3.2 Allocations with Low or Medium Risk Information

In cases where there is no possibility of High or Very High Risk information being stored as part of the allocation: the **Allocation Owner** may be granted permission to manage data sharing to **Users** directly. **Users** accessing the allocation are recommended to use **Enhanced CWL** in order to access the platform. (see 3.5 Data Classification Changes)

3.4 Ownership Changes

If the **Allocation Owner** responsible for an allocation is no longer connected to that project or research group and has not already specified another **Eligible UBC Researcher** to become the new **Allocation Owner**; ownership may be transferred to another **Eligible UBC Researcher** by **ARC Support** when approved by the associated **Administrative Head of Unit**.

3.5 Data Classification Changes

If, at any time, an allocation that previously had no possibility of including High or Very High-Risk information changes such that this possibility now exists. The **Allocation Owner** must immediately inform **ARC Support**. Before any High or Very High-Risk information is stored as part of the allocation, **ARC Support** must ensure that access controls are implemented as specified in section 3.3.1 above.